



Improving Cyber Risk Communication: Mental Models of VPN in a professional services firm in the Netherlands

Improving Cyber Risk Communication: Mental Models of VPN in a professional services firm in the Netherlands

Master thesis submitted to Delft University of Technology
in partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE

in **Complex Systems Engineering and Management**

Faculty of Technology, Policy and Management

by

Veroniek Binkhorst

Student number: 4276620

To be defended in public on November 23rd 2020

Graduation committee

Chairperson & First Supervisor	: Dr. ir. W. Pieters, section organisation and governance
Second Supervisor	: Dr.-Ing. T. Fiebig, section ICT
Advisor	: Dr. K. Labunets, section organisation and governance
External Supervisor	: R. Laarabi, EY

Preface

Dear reader,

In my perception, it feels like quite a while ago that I started to look for a Master thesis research topic. When I started, I first tried to grasp what a mental model was, then how it could be used and on which abstraction level research should be performed.

Now, months later, a complete research has been done on the mental models of experts and laypeople of VPN in a professional services firm in the Netherlands. Eighteen interviews have been completed, accumulating to 792 minutes, or 13,2 hours, a little over 150 pages of transcriptions and drawings, which equals to around 96.000 words that have been analyzed.

All this data has been brought together in this report and interesting findings have emerged. The process has not always been easy, but I am proud of the result. I had the pleasure to perform an internship at EY while I executed this research, and they have been very helpful in facilitating the interviews. I want to thank my supervisor at EY for her suggestions and feedback on this work.

Additionally, I want to thank the members of my graduation committee for their time, involvement, constructive feedback, and input. All this definitely had a valuable contribution to the quality of this research.

Lastly, I want to thank my family, friends, and loved ones for their support during the last few months, for their willingness to think along with me, and for distracting me when necessary.

Hopefully you enjoy reading this report.

Kind regards,

Veroniek Binkhorst
Delft, November 2020

Executive summary

In order for people to become more resilient and able to act in a secure manner when interacting with IT-systems, more effective and efficient risk communication is needed. One way to improve risk communication is to design it around the risk perception of the audience, or in other words, a person's view on a risk.

This study focuses on the perception of how a Virtual Private Network (VPN) works and the changes that occur in the threat landscape when a VPN is used. To study this perception a mental model approach is used. The working definition of a mental model in this thesis is the representation in an individual's mind of how a system works.

This study contributes new academic insights by adding to the knowledge base in this research area. Two knowledge gaps are addressed. The first knowledge gap is the lack of a clear, established method to capture and elicit mental models. This knowledge gap is partly addressed by performing a limited review of methods used to explicate mental models. The second addressed knowledge gap is that limited research has been done on the mental models of different cyber mechanisms. This is the first study of perceptions and practices regarding VPN and therefore this knowledge gap has been addressed.

This research is of societal relevance, because one out of nine persons were victim of cybercrime in 2017 (National Coordinator for Security and Counterterrorism [NCSC], 2019). Studies on the effectivity of cyber risk communication on a user's security behavior are essential in the current world (NCSC, 2019), and ensuring that people are aware of the cyber situation is one the three most important challenges to reach adequate cybersecurity levels (Van den Berg, 2019). Mental models have been useful in other fields, like environmental (Camp, 2009; Morgan et al., 2002), health (Morgan et al., 2002), and drug risks (Camp, 2009), and are therefore thought to be also useful to design cyber risk communication (Nurse et al., 2011).

Furthermore, mental models of VPN are an important topic to research, because this mechanism offers people the capability to cope with threats and increase their self-efficacy. Coping and self-efficacy has been found to be a reliable, moderately strong predictor for cybersecurity intention and behavior (European Union Agency for Network and Information Security [ENISA], 2018).

Additionally, cybercrime is becoming more mature and is shifting its focus to larger and more profitable targets (Europol & EC3, 2019). This research is focused on employees in a professional services firm in the Netherlands. The professional services firm selected is representative for other multinational professional services firms. Therefore, it is expected that the results found in this research will be applicable to similar firms as well. The main research question of this study is:

“What are the similarities and differences between the mental models of experts and laypeople of VPN in a professional services firm in the Netherlands?”

To answer this question, a qualitative and case study approach was used. Data was collected via semi-structured, online interviews and a three part scenario-based drawing task. The interviews consisted of three parts. The first part focused on how a VPN works. The second part focused on the current threat landscape. The third and final part focused on changes in the threat landscape that occur do to use of a VPN.

The target group consisted of experts and laypeople. Experts were employees that work in an information technology department at the firm for a minimum of two years and/or employees that are in the possession of a relevant degree or certificate (e.g. EMITA, CISA, CISSP). Laypeople were employees that work in a department that was considered non-technical, for example the departments legal, finance, and HR. Purposive sampling for maximum variation was used, based on the key characteristics educational qualifications, education area, role in the firm, and years active in the firm.

The collected data consisted of the transcriptions of the interviews, drawings made during the interviews, and the notes of the interviewer. Data was analyzed according to the Grounded Theory method. This method consists of open coding, axial coding, selective coding, and theory generation. During coding, memoing was performed to keep track of the thought process and theory development. A round of closed coding was done using existing frameworks to describe the current threat landscape. The results have been used to design a framework that illustrates the mental models of experts and laypeople of VPN in a professional services firm in the Netherlands. The concepts in the framework explain *when, where, why, how, or with what consequences* a VPN is used. The accuracy of this framework has been evaluated, by comparing it with a real-world model of a VPN. To evaluate the accuracy of the perceptions of the current threat landscape, the answers were compared with the Cyber Security Assessment Netherlands (NCSC, 2019).

Ethical considerations were taken into account for recruitment, data collection, data analysis, data publication, and data deletion. This research was reviewed and approved by the Human Research Ethics Committee of Delft University of Technology.

In total eleven interviews were held with experts and seven with laypeople. The average duration of an interview was 44 minutes, with a range between 13 and 88 minutes. Theoretical saturation was reached in the expert group, but not in the laypeople group separately. However, no new concepts were identified in the laypeople interviews compared with the expert interviews. Therefore, when combining the results, theoretical saturation has been reached.

The results on the perception of experts and laypeople in this sample of the current threat landscape is not completely accurate. However, the perception is deemed acceptable and it can be concluded that a distorted view on the current threat landscape will not be the cause of a potentially distorted view on the changes in the threat landscape due to VPN usage.

The designed framework that illustrates the mental models of experts and laypeople of VPN in a professional services firm in the Netherlands is depicted in figure 1. Indicated in framework are the theory elements known, which were determined at the outset of this research. At the center of the framework the selective code, or core category, is depicted. The framework has been divided into three core elements, namely the user element, the technology element, and the security element. It is indicated whether a concept was mentioned by only experts or by both groups.

The user element, the technology element and the security aspect from the security element, together form the perception of how a VPN works. The other concept groups in the security element, 'threats mitigated' and 'new threats', form the perception of the changes in the threat landscape when a VPN is used.

The framework shows that many similarities, but also important differences exist between the mental models of experts and laypeople. For example, in the user element many similarities can be identified. On the other hand, in the technology and security element many differences can also be identified. Since almost all concepts in the technology element that are only named by experts are also accurate, this indicates a less complete mental model for laypeople than experts on the technology element.

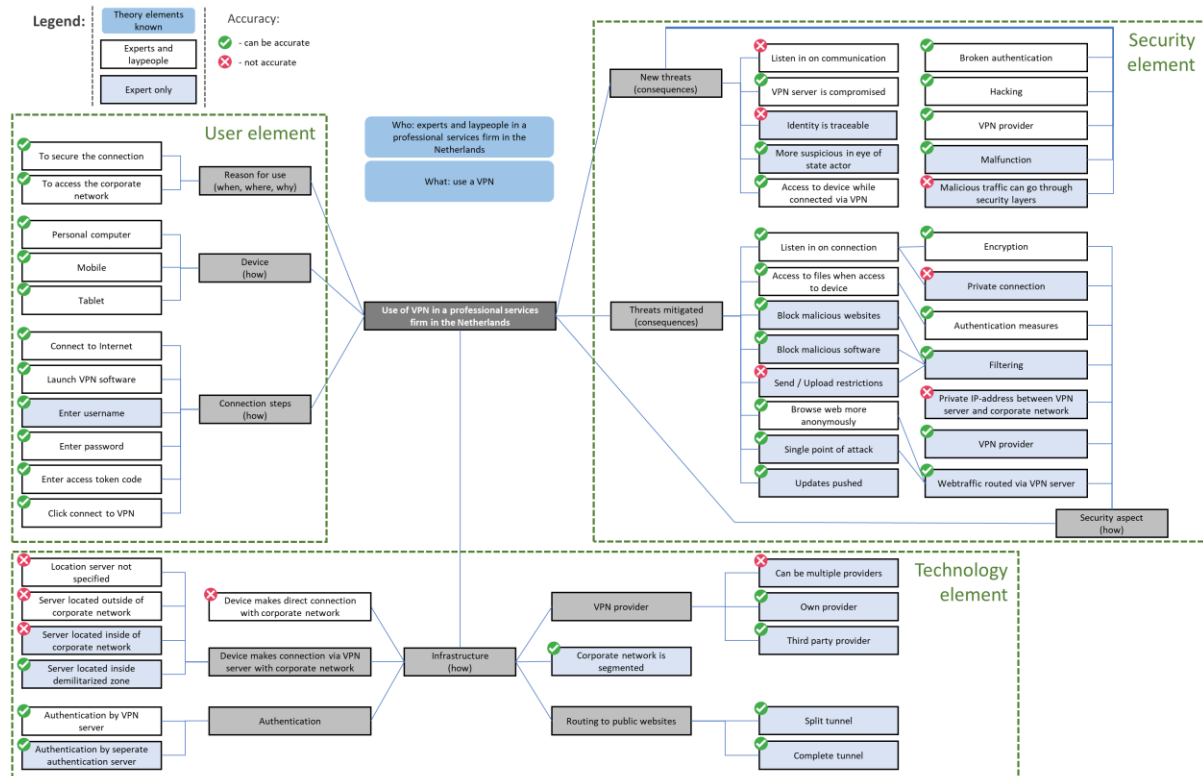


Figure 1: Framework illustrating the mental models of experts and laypeople

The framework also shows that the perceptions of both groups contain accurate and mistaken beliefs. Interesting to notice is that the inaccurate concepts in the security aspect group do not relate to additional inaccurate threats mitigated. The one inaccurate threat mitigated comes forth from an accurate concept, namely filtering. Another interesting fact to notice is that all inaccurate concepts in the groups security aspect and threats mitigated are named by only experts. On the other hand, experts do also name more accurate concepts than laypeople.

How the connection is secured in reality, and therefore what threats are mitigated, depends on the network configuration of the professional services firm and could be limited by the use of a split VPN. Mistaken beliefs and accurate perceptions that might not be in place in reality, depending on the network configuration, could result in an important consequence. This consequence can be that people think they are safer than they actually are, and therefore are either less watchful for threats or take more risks than they would otherwise. Since the mistaken belief in the concept group 'threats mitigated' is only mentioned by experts, and the other, more complicated, but accurate perceptions are only mentioned by experts as well, it can be expected that mainly experts in this target group overestimate the security of a VPN.

On the other hand, the inaccurate threats identified indicate a different result. Inaccurate threats, in the concept group 'new threats', could actually result in an underestimation of the security of a VPN and to more secure behavior than necessary. For example, because some experts and laypeople think a VPN does not protect against someone listening in on the communication, it was identified that they would sometimes choose to not establish a VPN connection when they use an unsecured network. Experts indicated they would use a mobile network instead as a precaution, which is a good solution, but laypeople did not mention this. The result of this inaccurate perceived threat could be that an unsecured network is used, but without creating a VPN connection. Since this would create a threat, this would ultimately result in an unnecessary risk due to a mistaken belief.

To conclude, many similarities, but also important differences exist between the mental models of experts and laypeople. The perceptions of both groups contain accurate and mistaken beliefs. The mistaken beliefs could

result in more or less secure behavior than necessary in reality, and therefore create unnecessary precautions and risks.

The results of this study contribute to the design of cyber risk communication in three ways. First, the results show what language is used by the audience and what certain terms mean to different persons in the audience. These results can be used to adjust the language in the communication to accommodate the information needs of the audience.

Second, the identified mistaken beliefs in the mental models can be used to improve the clarity of the message to the audience. Mistaken beliefs can cause confusion among the audience and the communication message to be understood incorrectly by the audience, because in their mental model something works in a different way than what's being told to them. The results of this study can help to adjust the communication to improve the clarity of the message to the audience.

Third and final, the mistaken beliefs can be used to focus the communication on what the audience needs to know, instead of repeating what the audience already knows. Additionally, by taking into account the results on when, where, and why a VPN is used and what changes in the behavior occur due to new threats that arise because a VPN is used, the risk communication message can be adjusted to maximize the impact on the resulting behavior.

Contents

Preface	iv
Executive summary	vi
List of Tables	xiv
List of Figures	xv
1. Introduction	1
1.1 Research topic.....	1
1.2 Theoretical relevance.....	1
1.3 Societal relevance	2
1.4 Report outline	2
2. Background	3
2.1 Core concepts	3
2.1.1 Cyberspace.....	3
2.1.2 Cybersecurity	3
2.1.3 Risk	3
2.1.4 Risk communication.....	3
2.1.5 Risk perception	3
2.1.6 Mental model.....	4
2.2 Virtual Private Networks	4
2.2.1 Corporate Virtual Private Network	4
2.2.2 End-User Virtual Private Network.....	6
2.3 Literature review.....	6
2.3.1 Mental models as metaphors	6
2.3.2 Mental models in response scenarios	7
2.3.3 Expert mental models	7
2.3.4 Expert and laypeople mental models	8
2.3.5 Laypeople mental models of malware.....	8
2.3.6 Other laypeople mental models	9
2.4 Discussion of the literature and identification of knowledge gaps	10
2.5 Main research question	12
3. Study design.....	13
3.1 Subquestions.....	13
3.2 Research approach.....	14
3.3 Data collection method.....	14

3.3.1 Interview design.....	14
3.3.2 Drawing task design	15
3.3.3 The platform: Big Blue Button	16
3.3.4 Validation of the interview protocol.....	17
3.4 Target group.....	17
3.4.1 Experts and Laypeople	17
3.4.2 Sampling method	18
3.4.3 Sample size.....	18
3.4.4 Recruitment method.....	18
3.5 Data analysis method.....	19
3.5.1 The data: transcriptions, drawings and notes of the interviewer	19
3.5.2 Grounded Theory	20
3.5.3 Closed coding: the current threat landscape.....	21
3.5.4 Inter Coder Agreement	23
3.5.5 Accuracy of the mental models	24
3.6 Ethical considerations	24
4. Results.....	26
4.1 Statistics interviews and participants	26
4.2 Perception of how a VPN works	27
4.2.1 Reason for use.....	27
4.2.2 Device on which the VPN can be used.....	29
4.2.3 User steps to establish a connection	29
4.2.4 Infrastructure	29
4.3 Perception of the current threat landscape	35
4.3.1 Threats	35
4.3.2 Threat actor.....	36
4.3.3 Threat actor motivation	37
4.3.4 Threat actor capability	37
4.3.5 Threat impact.....	37
4.4 Perception of changes in the threat landscape when using a VPN	37
4.4.1 Mitigation of threats due to VPN usage	37
4.4.2 New threats due to VPN usage	39
4.4.3 Change in human behavior to deal with new threats.....	42
5. The mental models of experts and laypeople.....	43

5.1 Framework illustrating the mental models.....	43
5.2 Accuracy of the mental models	44
5.1.1 Accuracy perception of how a VPN works	44
5.1.2 Accuracy perception of the current threat landscape	45
5.1.3 Accuracy perception of changes in the threat landscape when using a VPN.....	46
6. Discussion and Conclusion	47
6.1 Similarities and differences between the mental models	47
6.1.1 Answers to the subquestions.....	47
6.1.2 Answer to the main research question.....	47
6.1.3 Comparison of the results to related work.....	48
6.2 Scientific and societal implications	49
6.2.1 Scientific implications	49
6.2.2 Societal implications	50
6.3 Limitations of the study	51
6.4 Further research possibilities.....	52
6.5 Embedding in CoSEM curriculum, I&C track, and cybersecurity specialization	52
Reference list	54
Appendix A: Interview protocol.....	59
A.1: English interview introduction.....	59
A.2: Dutch interview introduction	59
A.3: Interview protocol	59
Appendix B: Recruitment Text and Informed Consent Form	62
B.1: Recruitment text for contact persons experts Dutch	62
B.2: Recruitment text for contact persons experts English	62
B.3: Recruitment text for contact persons laypeople Dutch	63
B.4: Recruitment text for possible participants English.....	63
B.5: Recruitment text for possible participants Dutch	64
B.8: Informed consent form via e-mail.....	65
Appendix C: Interview transcripts.....	68
C.1: Transcript Expert 1.....	68
C.2: Transcript Expert 2.....	89
C.3: Transcript Expert 3.....	95
C.4: Transcript Expert 4.....	106
C.5: Transcript Expert 5.....	121

C.6: Transcript Expert 6.....	135
C.7: Transcript Expert 7.....	141
C.8: Transcript Expert 8.....	150
C.9: Transcript Expert 9.....	157
C.10: Transcript Expert 10.....	165
C.11: Transcript Expert 11.....	172
C.12: Transcript Laypeople 1.....	186
C.13: Transcript Laypeople 2.....	192
C.14: Transcript Laypeople 3.....	200
C.15: Transcript Laypeople 4.....	202
C.16: Transcript Laypeople 5.....	204
C.17: Transcript Laypeople 6.....	210
C.18: Transcript Laypeople 7.....	217
Appendix D: Code book and Frequency Distribution Codes.....	226
D.1: Code book perception of how a VPN works.....	226
D.2: Code book perception of the current threat landscape.....	235
D.3: Code book perception of changes in the threat landscape when using a VPN.....	242
Appendix E: Overview of ICA coefficients per semantic domain.....	247

List of Tables

Table 1: Overview of papers included in literature review.....	10
Table 2: Closed coding framework for threats	21
Table 3: Closed coding framework for threat actors	22
Table 4: Closed coding framework for the motivation of a threat actor.....	22
Table 5: Closed coding framework for the capability of a threat actor.....	23
Table 6: Closed coding framework of the impact of a possible threat.....	23
Table 7: Statistics of the interviews	26
Table 8: Demographic information of the participants	26

List of Figures

Figure 1: Framework illustrating the mental models of experts and laypeople.....	viii
Figure 2: Real-world model of a VPN	5
Figure 3: Conceptual model of the study design	13
Figure 4: The landing page of the conferencing platform	16
Figure 5: The whiteboard of the online conferencing platform	17
Figure 6: Overview of the recruitment process	19
Figure 7: Axial coding with the use of post-its	20
Figure 8: First and second basic configuration of the infrastructure	30
Figure 9: Third and fourth basic configuration of the infrastructure	30
Figure 10: First and second additional specification of the infrastructure.....	31
Figure 11: Drawing made by expert 9.....	33
Figure 12: Drawing made by expert 6.....	35
Figure 13: Drawing made by layperson 5	35
Figure 14: Drawing made by layperson 2	35
Figure 15: Framework of the mental models of experts and laypeople.....	43
Figure 16: Framework of the mental models of experts and laypeople evaluated for accuracy.....	44

1. Introduction

The field of cyber risk communication is relatively new and questions exist on how to effectively communicate risks in the cyber domain (ENISA, 2018). The goal of cyber risk communication is to help people to be resilient and able to act in a secure manner when interacting with IT systems. To design effective and efficient risk communication, it is necessary to determine the risk perception of the audience (International Organization for Standardization [ISO], 2018b; Rohrmann, 1992). A person's risk perception is that person's view on the risk (ISO, 2009).

The following subsections introduce the research topic, describe the theoretical and societal relevance, and present the outline of this report.

1.1 Research topic

This study focuses on the perception of how a Virtual Private Network (VPN) works and the changes that occur in the threat landscape when a VPN is used. A VPN is a means used by organizations to let employees access the corporate network via the Internet from a remote location. When the corporate network is accessed, resources become available to the employee as if directly connected to the corporate local area network. Another use case of VPN is to secure the connection with encryption, so it becomes impossible to eavesdrop.

Two elements of the perception are researched to answer the main research question. First is what the perception is of how a VPN works, for which is looked into the reason for use, on which devices a VPN is used, which steps are taken by users to establish a connection, and what the infrastructure looks like. Second is researched what the perception is of changes in the threat landscape when a VPN is used, for which is looked into the perception of threats mitigated by a VPN, the perception of new threats that arise due to the use of a VPN, and what changes occur in a user's behavior to deal with these new threats.

To study this perception a mental models approach is used. The working definition of a mental model in this thesis is the representation in an individual's mind of how a system works. Additionally, a case study approach is used. The case consists of a professional services firm in the Netherlands. The subjects of the study are employees in the professional services firm and the target group is split into experts and laypeople.

The objective for this research is to develop a substantive theory on the similarities and differences between the mental models of experts and laypeople of VPN in a professional services firm in the Netherlands.

1.2 Theoretical relevance

Research on risk perception in the field of cybersecurity is necessary because this area of research is relatively new and has been said numerous times to be critical to research in literature. In 2009 Camp mentioned that the use of mental models as a tool for risk communication had not yet been embraced by computer security experts (Camp, 2009). In the eleven years since the article of Camp, some research in this field has been done (e.g. Furman et al., 2012; Krombholz et al., 2019; Wash & Rader, 2011). But research on mental models in the cyber field is still young and developing. According to Nurse et al. (2011), research should focus on the perception of security risks and decision-making regarding these risks. Wash & Rader (2011) propose the same in their research agenda, stating that research should focus on understanding how users make security decisions and the problems that arise due to these decisions.

This study contributes by adding to the knowledge base in this research area. This is the first study of perceptions and practices regarding VPN. The professional services firm selected is representative for other multinational professional services firms. Therefore, it is expected that the results found in this research will be applicable to similar firms as well. By studying both expert and laypeople perceptions, it was possible to explicate perceptions

of both groups and differences between the groups. Mistaken beliefs in these perceptions have been identified and the consequences of these mistaken beliefs on behavior and its possible implications are described.

1.3 Societal relevance

This research topic is of societal relevance because more effective and efficient risk communication must be designed. According to NCSC (2019), one out of nine persons were victim of cybercrime in 2017 and research on the effectivity of awareness campaigns on a user's security behavior is currently very important. Van den Berg (2019) describes the creation of cyber situation awareness as one the three key challenges to reach adequate cybersecurity levels. It is of importance to consider the information needs and the variety of these needs among the audience in cyber risk communication (Stewart & Lacey, 2012). Communication should focus on what people need to know and the mental model approach can help to design this (Fischhoff, 1995). Mental models are thought to be a valuable source of information to design cyber risk communication, because the use of mental models has been very successful in different fields (Nurse et al., 2011). These fields are for example environmental (Camp, 2009; Morgan et al., 2002), health (Morgan et al., 2002), and drug risks (Camp, 2009). Additionally, more and more research indicates that people use mental models to understand, evaluate, and act on risks (Jones et al., 2011).

Furthermore, cybercrime is becoming more mature and is shifting its focus to larger and more profitable targets (Europol & EC3, 2019). According to a large survey, 59% of organizations experienced a significant or material breach in 2019 (EY, 2020). This shows the need for research into risk perceptions in organizations to improve the cyber risk communication for employees of these organizations.

The professional services firm in this research, like similar other professional services firms, handles highly confidential and personally identifiable information. Effective risk communication aids in protecting the confidentiality, integrity, and availability of this information. As such this research both helps directly the professional services firm and similar firms as indirectly the general population by protecting those that could be affected by an undesirable event.

Finally, research into mental models of VPN is important because through this mechanism people can protect themselves against certain threats. Because users decide when and where they use a VPN connection, their decisions can have important consequences. This research can eventually help people to cope with threats and increase their self-efficacy. Coping and self-efficacy are a reliable and moderately strong predictor for cybersecurity intention and behavior, which indicates that the center of attention of measures should be on increasing the user's ability to respond to cyber threats rather than only focusing on the threat itself (ENISA, 2018).

1.4 Report outline

In section 2 the core concepts are defined, an overview is provided of what a VPN is, knowledge gaps are identified based on a literature review, and the main research question is identified based on the identified knowledge gaps. Section 3 presents the study design and contains the subquestions formulated to answer the main research question and discusses the research approach and methodology. Section 4 presents the results. In section 5 the results are used to design a framework that illustrates the mental models and the accuracy of the mental models are evaluated. In section 6 the results are discussed and the main research question is answered.

2. Background

This section describes and defines the core concepts and demarcate the research field (section 2.1), describes a representation of a VPN in the real world (section 2.2), presents a literature review (section 2.3), identifies a knowledge gap based on a discussion of the literature review (section 2.4), and formulates the main research question based on the identified knowledge gap (section 2.5).

2.1 Core concepts

This section describes six core concepts. We start on the highest abstraction level with cyberspace, dive into subdomains, and conclude with mental models.

2.1.1 Cyberspace

We define cyberspace using the definition of the ISO (2012), which defines cyberspace as “a complex environment resulting from the interaction of people, software and services on the Internet, supported by worldwide distributed physical information and communications technology (ICT) devices and connected networks”.

2.1.2 Cybersecurity

The cybersecurity domain tries to secure cyberspace. No universally accepted definition of cybersecurity has been defined, and it is, therefore, fitting to determine a contextual definition (ENISA, 2016). In this thesis we use the definition of Van den Berg (2018), who defines cybersecurity as “the multidisciplinary (cyber) risk management challenge of securing cyberspace”. With the challenge of securing cyberspace three domains, being technology, human, and process, are encompassed.

2.1.3 Risk

Cybersecurity is a risk management challenge, and therefore we need to define risk. Risk can be defined as “a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence” (National Institute of Standards and Technology, 2012).

2.1.4 Risk communication

The product of this study can be used to design communication on risks. Morgan et al. (2002) define risk communication as “communication intended to supply laypeople with the information they need to make informed, independent judgments about risks to health, safety and the environment” (p. 4).

To design effective risk communication we need to determine the risk perception of the target audience (ISO, 2018b; Rohrmann, 1992).

2.1.5 Risk perception

Risk perception considers the way people view the risk and what factors affect their perspective (Nurse et al., 2011). ISO (2009) defines risk perception as the “stakeholder’s view on a risk”, in which a stakeholder is defined as a “person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity”.

Many factors influence someone’s behavior and many different theories exist describing these factors, for example the Theory of Planned Behavior (Ajzen, 1991) or the Fogg Behavioral Model (Fogg, 2009). One important factor that influences behavior is the risk perception of a person (Fischhoff, 2013).

Risk perception consists of multiple elements. For example what the possible outcomes of a decision are perceived to be, how these possible outcomes are valued, the perceptions about those outcomes, how big the risk is perceived to be, what factors are considered to be important to influence the risk, and the emotional state of the decision maker (Fischhoff & Kadvany, 2011).

In this study we focus on the perception of how a VPN works and the perception of the changes in the threat landscape when using a VPN. To explicate the risk perception of the target group, a mental models approach is used.

2.1.6 Mental model

We can find different definitions of mental models in literature. Johnson-Laird (1986) and Garg et al. (2012) define mental models as internalized representations of external reality. In Wash (2010) and Wash & Rader (2011) a mental model is defined as a model in the person's mind of how things work. Camp (2009) does not provide a definition for mental models, but communicates them as being metaphors that can be used to communicate risks. Wash & Rader (2015) define mental models as a set of causal beliefs that a person possesses that he or she uses to guide decisions and behavior. Märki et al. (2016) performed a literature review on the definition of mental models. In this review the most frequently described attributes of mental models were that mental models are mostly wrong, are representations, and that they change over time. In this study the following working definition of a mental model is used: *"A mental model is the representation in an individual's mind of how a system works"*.

2.2 Virtual Private Networks

In this section is explained how a VPN works and what changes in the threat landscape can occur when using a VPN. This overview is not meant to be complete and is based on what choices are made in general by organizations. The information for this section is provided by Dr.-Ing. Tobias Fiebig. In figure 2 a visual representation of the information in this section is presented. In the text numbers are added that refer to a part of the figure.

In general a VPN is used in two different settings. The first setting is in an organization and is described in section 2.2.1. The second setting is in a personal setting, which is described in section 2.2.2.

2.2.1 Corporate Virtual Private Network

A Virtual Private Network (VPN) is a means used by organizations to let employees access the corporate network via the Internet from a remote location. When the corporate network is accessed, resources become available to the employee as if directly connected to the corporate local area network. Network administrators can impose restrictions on what resources and services a remote access VPN client can use.

The corporate network consists of at least two segments. The first segment is the internal network (1), which is not accessible from the public Internet and contains the resources and private webpages from the organization. The internal network is only accessible if connected directly to the local area network, or if connected via a VPN connection. The second segment is a demilitarized zone (DMZ)(2), which is a segment of the corporate network that is publicly accessible via the Internet. When a VPN connection is established, Internet traffic is routed via a VPN server in the DMZ to the internal network (3). To protect the corporate network, all webtraffic that enters the DMZ is filtered by a firewall (4).

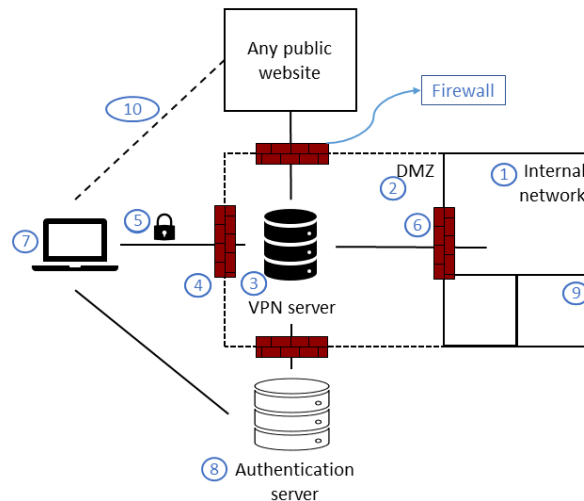


Figure 2: Real-world model of a VPN

The VPN connection is secured with encryption (5). By using encryption, the plaintext message is transformed into cyphertext. At the endpoint of the secured connection, the message is decrypted, which transforms the message back into plaintext. Encryption protects confidentiality by ensuring that no one other than the original sender and the receiver of the message know what is written in this message. Additionally, encryption protects integrity by ensuring that the message is not manipulated in transit.

When employees need to send confidential information over the Internet, encryption thus ensures that no third party can eavesdrop or manipulate the message. This is especially important when employees connect to a publicly available Internet connection in for example a café, hotel lobby, or random Wi-Fi hotspot. The encryption must be properly configured and using a proven protocol in order to be secure.

When encryption is used, traffic cannot be inspected on whether it complies with the firewall's filtering rules. Because of this reason, it is important to consider if the encryption is terminated before, at, or after a firewall. In most cases, the encryption is terminated at the VPN server inside the DMZ. This means that malicious webtraffic is able to pass through the firewall protecting the DMZ. In order to protect the internal network, another firewall is located between the DMZ and the internal network (6). This firewall is able to filter the decrypted webtraffic and protect the internal network from malicious traffic.

An employee can establish a VPN connection using a device with a local Internet link (7). In a corporate setting, this device can be company-issued and pre-configured. Employees are provided with a user account and will need to fill in their credentials in order to authenticate themselves. Authentication can be done directly by the VPN server itself, or it can be done by an external authentication server (8). If authentication is performed by an external authentication server, this server will send a ticket to the VPN server, so the employee can establish a VPN connection. When authentication is successful, a VPN connection is established and employees can access the internal network. However, the internal network consists of multiple segments and it depends on the authorization of the user which segments he or she may access (9).

Additionally, The VPN can be in own management or be provided by a third party. Because of price considerations, often a VPN service is provided by a third party. When a VPN service is provided by a third party, certain risks are introduced. For example, the VPN provider can make a mistake when implementing the solution and encryption protocols. Or, the employees from the VPN provider can misuse their access. These examples illustrate that certain arrangements need to be made when the VPN is provided by a third party.

Furthermore, a choice must be made by the organization on whether to allow Internet communication for VPN users. If this is the case, all webtraffic will be routed via the VPN server. Another option is to let employees visit any public website via their local Internet connection and not route this traffic via the VPN server (10). This is called a split tunnel. Using a split tunnel can pose a risk, where an Internet attack could breach the remote host and then use the VPN to access the corporate network.

Lastly, if the VPN uses tunnel mode encryption, the identity of the original sending device is confidential. In tunnel mode encryption, the original IP packet's header and payload are encrypted and this packet becomes the payload of a new IP packet, with a new IP header. Another option is transport mode encryption, which only encrypts the original IP packet's payload. Transport mode encryption helps VPNs link individual computers together and is in principle not used for remote access VPNs.

2.2.2 End-User Virtual Private Network

Aside from the use of a VPN in a corporate setting, a VPN can also be used in a personal setting. In a personal setting, the VPN is not provided by an organization to an employee, but is a service acquired by a person. The person can set up his or her own VPN, but in most cases the VPN service is acquired from a company.

When a VPN is used for personal use, the motivation to use a VPN and the technology behind the VPN is somewhat different. The motivation is different in the sense that the VPN would solely be used to access the Internet, and not a corporate network. Additionally, the personal VPN can be used to circumvent local restrictions or to protect someone's identity online.

Local restrictions can be circumvented when the VPN encrypts the IP packet's payload and header and the packet is sent to a VPN server in a different location. When this happens, the message cannot be read and thus not filtered to check for local restrictions, and is sent unencrypted from the VPN server onwards. For example, when a local government blocks a certain website, a VPN can be used to visit this website as if a person were to be in a different country. Another example is to circumvent restrictions in place by streaming services. If someone would want to access content not available in their place of residence, this someone can make a VPN connection with a VPN server in a different place and circumvent this restriction. Many VPN service providers for personal use let the user choose with which VPN server they want to make a connection, where the VPN servers are located in different countries. This way, the VPN service provider lets the user choose from which location they want to access a website, for example the United States of America or Brazil.

The identity of a user is protected online if the original IP packet's header is encrypted. The packet will get a new IP header and it is impossible to trace the packet back to the original sending device.

There are some important notions to be made when a VPN service is acquired for personal use. First, it is important to consider whether the VPN provider monitors, collects, or sells data about the webtraffic. Second, a lot of configurations can be made when a VPN is set up, this is also true regarding whether encryption is used.

2.3 Literature review

This section describes an overview of the literature on mental models of risk perception in the field of cybersecurity. The literature is grouped based on the subject and topic of study and within categories based on year of publication.

2.3.1 Mental models as metaphors

Camp (2009) proposed to use mental models to communicate cybersecurity risks. She suggested to use five metaphors as mental models, namely physical security, medical risks, crime, warfare, and markets. Camp did not describe the origin of these metaphors and they seem to be based on her own observations rather than literature or research.

Asgharpour et al. (2007) researched to which group experts and non-experts relate certain cyber concepts. They conducted two closed card-sorting experiments with 33 experts and 76 non-experts and based their groups on the metaphors identified by Camp (2009). Asgharpour et al. (2007) found that experts and non-experts have significantly different mental models. A stricter definition of expert and non-expert led to even more dispersed mental models. However, the definition of experts and non-experts should not be confused with experts and laypeople. All participants in the study were faculty, staff, graduate or undergraduate students in informatics or computer science departments, where experts were longer active in the field than non-experts.

2.3.2 Mental models in response scenarios

Bravo-Lillo et al. (2011) conducted interviews with 30 participants, of which 10 were advanced users in security and privacy and 20 were novice users, to capture their perception of security warning messages. Security warnings from popular operating systems and application software were used during the interview. The findings showed that all participants went through three phases when seeing the messages. Laypeople focused on the visual appearance of the message, while experts evaluated actions that could have led to a warning message and would look on the Internet to estimate its legitimacy.

Zou et al. (2018) studied the perceptions of laypeople of a data breach in a case study of the Equifax breach. Interviews were held with 24 participants and the results indicate the participants did not take action upon being notified of the breach, because they felt the cost of the actions were too high compared to the risk of identity theft.

Deline et al. (2019) suggested the existence of shared mental models in a cyber defense team in an incident response scenario and that communication is centered on both the task and the team. The participants in the study were graduate students from an engineering school, therefore the study may yield different results if conducted with professionals.

2.3.3 Expert mental models

Al Sabbagh & Kowalski (2012) used interviews to collect the mental models on risk appetite of 35 IT-workers with different positions and levels of expertise in Saudi Arabia. They asked their participants to prioritize mitigation measures, which assumes participants know and understand these measures. The results show that the participants have different mental models if the security problem is personal, national, or organizational, and are not influenced by funding conditions. The authors note that “in several occasions we heard interviewees commenting they are not sure what answers to choose” (p. 116), which questions the validity of the results.

Paul & Whitley (2013) used interviews, observations and a card-sorting experiment with six cybersecurity analysts to capture the taxonomy of questions a cybersecurity analyst asks themselves in the case of a possible network event. The participants were responsible for intrusion detection and therefore the taxonomy is lacking for incident response questions.

Märki et al. (2016) researched the beliefs of software developers about security and how vulnerabilities arise, and which actions they take to increase the security of their software. They used the structure formation technique, combining interviews with card-sorting, and included five participants. The researchers themselves already state that five participants limits the completeness of the results.

Maier et al. (2017) studied mental models of seven governmental cybersecurity experts on cyber attacks and possible countermeasures. Participants were requested to draw two attacks and possible countermeasures on a template. The results indicate that the operational and analytical employees were able to describe the attacks in a more detailed and fluent manner compared to managers. The countermeasures proposed were mainly technical and awareness related, few were related to law enforcement.

Dietrich et al. (2018) examined the perception of system operators on security misconfigurations. Six interviews were held via Internet relay chat and the results were used to design a survey with 221 participants. One third of the respondents described that a witnessed misconfiguration resulted in an actual security incident, but all misconfigurations had this potential. The results additionally indicated that institutional, organizational, and personal factors are a cause of human error in security operators. Theoretical saturation in the interviews had not been reached and self-selection bias may have occurred in the survey.

2.3.4 Expert and laypeople mental models

Kang et al. (2015) explored mental models of the Internet through interviews, a survey, and a drawing task. Laypeople did not mention Internet levels, organizations, and entities, whereas experts did. The results did not indicate a connection between a person's technical background and actions to protect their privacy and security.

Gallagher et al. (2017) interviewed six experts and eleven laypeople on their perception of the Tor anonymity system. The grounded theory results show that laypeople use abstractions and metaphors to convey their perception and that they have a lesser understanding of how Tor operates than experts.

Oates et al. (2018) performed a secondary data analysis of 366 drawings created in response to the question what privacy meant to the participants. Experts' drawings focused on data privacy, whereas laypeople's drawings showed a division between private and public physical spaces. The children in the study drew bedroom or bathrooms, but did not pertain data privacy.

Krombholz et al. (2019) studied the mental models of laypeople and system administrators of HyperText Transfer Protocol Secure (HTTPS). Interviews were combined with a drawing task. The results indicate that many users confuse encryption with authentication, laypeople underestimate the security benefits of HTTPS, and both laypeople and system administrators distrust security indicators.

2.3.5 Laypeople mental models of malware

Wash (2010) used interviews to elicit mental models from 33 laypeople on cybersecurity concepts, in particular four mental models on viruses and other malware and four on hackers. He illustrated mistaken beliefs in the mental models and shows how the mental models affect the manner in which laypeople react to security advice. Wash grouped participants based on their beliefs and identified similar security behaviors among group members and differences between groups. An important finding is that a more complete and correct mental model does not necessarily lead to better security decisions. Because Wash used mental models and security behaviors of 33 laypeople, this relation is not statistically significant. Furthermore, snowballing was used as participant sampling method, therefore the study may include people who share the same mental model.

Blythe & Camp (2012) used the mental models found by Wash (2010) in an agent based simulation. They identified that the agents make broadly similar decisions on security behavior as those reported by human subjects. Comparative numbers on security behaviors by human subjects were not presented.

Wash & Rader (2015) used a survey to study the prevalence of beliefs on computer security and security behavior among a representative sample of US Internet users. The beliefs questioned were based on the findings of Wash (2010). The results suggest that variation in beliefs and level of education might result in different behavior. An important notion made is that the relation between a mental model and behavior is not as straightforward as Wash (2010) suggested. Wash & Rader (2015) measured secure behavior by enquiring into self-reported past behaviors. A limitation of this method is imperfect recall, which could lead to incorrect conclusions. Furthermore, self-reported behavior does not always correlate with actual behavior (Wash et al., 2017).

Spero et al. (2019) studied mental models of regular software and malware. Forty participants were asked to draw how a word processor works and how this processor can be infected with malware. The results illustrate that participants think regular software has another purpose compared to malware and that the drawings of

malware were less detailed. A positive correlation between technical knowledge and level of detail in the drawing was not identified. The authors have coded the drawings, but do not mention analyzing the participants' thinking process as well. Therefore, the mental models described might be incomplete.

2.3.6 Other laypeople mental models

Wash & Rader (2011) performed a literature review on the use of mental models in cybersecurity and proposed two things in order to change laypeople's mental models. First, it must be identified how people form mental models and how they can be influenced. Second, it must be identified which models are associated with what security behaviors, so it can be determined which models laypeople should possess.

Furman et al. (2012) conducted interviews with 40 participants on a very wide range of security topics. The results indicate participants generally thought they were knowledgeable about computer security. However, the results show an incomplete and unsolid skill set, incomplete mental models, and the use coping mechanisms derived from personal and life experiences. The researchers state that the participant's mental model is incomplete if they do not address confidentiality, integrity, and availability and conclude that educating efforts should focus on completing mental models. Out of the 40 participants, only two had no college education, a relatively small percentage compared to the general population in the US. This could indicate that not all mental models in the population are captured. Furthermore, one-hour interviews were held on a broad range of topics. This limited time for a large range of topics could have prevented them from going in depth on the topics.

Vaniea et al. (2014) analyzed how decisions on Microsoft Windows 7 software updates are made. Data from interviews, a survey, and computer logs was collected and compared from 37 participants. The results show that laypeople's perception and intention was not equal to what actually happened. Interestingly, most computers were more secure than the user intended.

Ramokapane et al. (2017) studied perception of deleting a file in the cloud. Findings indicate participants had difficulties deleting a file, due to a lack of information, incomplete mental models, and misunderstandings about the user interface. Theoretical saturation was reached after 13 out of 26 interviews, however the protocol changed after reaching saturation and it is not indicated if saturation was reached with the new protocol.

Abu-Salma et al. (2017) researched mental models on secure communication tools. It was found that laypeople hold incorrect mental models, which is suggested to hinder them in adopting secure communication tools. They interviewed a sample size of 60 persons, but did not include a wide range of cultural backgrounds and they did not use an additional elicitation technique to support the interviews, therefore their results could be incomplete.

Abu-Salma et al. (2018) used a survey to study the prevalence of the mental models of end-to-end encryption described in the research of Abu-Salma et al. (2017). They surveyed 125 people, who might not be representative for the demographic factors gender, age, race, educational level, and employment status. The results show that half to two-thirds of participants have a (partially) correct mental model. Generalizability is limited due to the small sample size and the non-representativeness of demographic factors.

Abdi et al. (2019) conducted 17 interviews to examine the security and privacy perceptions of smart home personal assistants. The results indicate mistaken beliefs of where data is stored, processed and shared. Participants use non-technical coping strategies to try to increase their security and privacy, such as using only limited functionalities of the smart assistant.

Choong et al. (2019) distributed a survey at two schools in the USA in order to research children's practices, perceptions, and knowledge of passwords. The results show that children see passwords as a way to provide access control, but do not use strong passwords. The children demonstrated good password practices such as memorizing passwords, not writing passwords down, keeping their passwords private, and they log out after each session. The authors conclude that children have appropriate mental models of passwords. Secure behavior is measured using self-reported data. While the questions were formulated specifically for children, it is

questionable how reliable the answers of children aged 8-12 and 11-15 are. The possible options for answering questions were ‘never’, ‘sometimes’, or ‘always’, no option was included for ‘I do not know’. This may result in children randomly choosing an answer if they do not know the answer. Furthermore, during the analysis phase, the answers for ‘always’ and ‘sometimes’ were combined, but the researchers draw conclusions that sometimes is equal to good password hygiene on that specific question.

An overview of the articles included in this review, ordered based on year of publication, can be found in Table 1. The number of citations is based on Google Scholar at November 15, 2020.

Table 1: Overview of papers included in literature review

Authors	Year	Citations	Theme
Asgharpour, Liu & Camp	2007	97	Grouping of security related concepts into categories corresponding to the five metaphors defined by Camp (2009)
Camp	2009	177	Proposed five metaphors to be used as mental models: physical security, medical risks, crime, warfare, and markets
Wash	2010	327	Mental models of laypeople on cybersecurity concepts, in particular viruses and other malware, and hackers
Bravo-Lillo, Cranor, Downs & Komanduri	2011	62	Expert and laypeople perception of security warnings
Wash & Rader	2011	67	Literature review on mental models in cybersecurity and proposal of a research agenda
Al Sabbagh & Kowalski	2012	19	Mental models of IT workers on risk appetite
Furman, Theofanos, Choong & Stanton	2012	60	Mental models of a wide range of security topics
Blythe & Camp	2012	40	Usage of mental models found by Wash (2010) in agent based simulation
Paul & Whitley	2013	42	Taxonomy of questions cybersecurity analysts asks themselves in the case of a possible network event
Wash, Radar, Vaniea & Rizor	2014	67	Laypeople perception of Microsoft Windows 7 updates
Kang, Dabbish, Fruchter & Kiesler	2015	213	Expert and laypeople perception of the Internet
Wash & Rader	2015	83	Prevalence study of beliefs identified by Wash (2010) and secure behavior
Märki, Maas, Kauer-Franz & Oberle	2016	2	Software developer’s perspective of software security
Abu-Salma, Sasse, Bonneau, Danilova, Naiakshina & Smith	2017	82	Mental models of secure communication tools
Gallagher, Patil & Memon	2017	19	Expert and laypeople perception of the Tor anonymity system
Maier, Padmos, Bargh & Wörndl	2017	2	Mental models of seven governmental cybersecurity experts on cyber attacks and possible countermeasures
Ramokapane, Rashid & Such	2017	10	Laypeople perspective on how to delete a file in the cloud
Abu-Salma, Redmiles, Ur & Wei	2018	8	Prevalence study of the mental models of end-to-end encryption described by Abu-Salma et al. (2017)
Dietrich, Krombholz, Borgolte & Fiebig	2018	25	System operators’ perception of security misconfigurations
Oates, Ahmadullah, Marsh, Swoopes, Zhang, Balebako & Cranor	2018	14	Secondary data-analysis on drawings of privacy
Zou, Mhaidli, McCall & Schaub	2018	28	Case study of mental models of a data breach
Abdi, Ramokapane & Such	2019	17	Security and privacy perceptions of a smart home personal assistant
Choong, Theofanos, Renaud & Prior	2019	6	Children’s practices, perceptions, and knowledge regarding passwords
Deline, Guillet, Rauffet & Guérin	2019	0	The existence of shared mental models in a cyber defense team in an incident response scenario
Krombholz, Busse, Pfeffer, Smith & von Zeischwitz	2019	19	System administrators’ and laypeople mental models of HTTPS
Spero, Stojmenovic, Hassanzadeh, Chiasson & Biddle	2019	0	Mental models of regular software and malware

2.4 Discussion of the literature and identification of knowledge gaps

From this literature review it becomes clear that research on mental models in the field of cybersecurity is still developing and that the field is young. This means that a lot of research remains to be done and many knowledge gaps can be formulated. An important observation is that the mental models seem to always be incomplete and

contain mistaken beliefs. This is also found to be true in the mental models of experts (Kang et al., 2015; Krombholz et al., 2019). This underlines the necessity of research in this field, to ensure that the designed risk communication is as effective and efficient as possible, with the ultimate goal of making people more cyber resilient.

Research on mental models in the field of cybersecurity is done on different abstraction levels. Some research focuses on one concrete cyber mechanism (e.g. Abu-Salma et al., 2017; Krombholz et al., 2019), and other research focuses on mental models of cybersecurity as a whole (e.g. Furman et al., 2012). Research on risk perception of a high abstraction level results in a lack of depth in mental models and leaves crucial questions pending (Slovic, 2000). Therefore, for risk communication purposes, research in this field is most useful when focusing on the mental model of a concrete cyber mechanism. The level of detail needed to explicate the population's knowledge, mistaken beliefs and missing information will only be reached when studying specific mechanisms.

The first knowledge gap is the lack of a clear, established method to capture and elicit mental models. Most empirical research in this field use interviews to capture mental models, but others use card sorting, a drawing task without interview, a questionnaire, observations, or a combination of these methods. Some research use an additional elicitation technique to supplement the interview, such as a drawing task (e.g. Krombholz et al., 2019) or card sorting (e.g. Märki et al., 2016). The difference in methods used indicates that there is no consensus among researcher on how to best elicit and capture mental models.

A second knowledge gap is that it remains unknown which factors cause variance in mental models of the population. Currently, sampling in empirical research is done based on demographics, without concluding first that mental models (solely) vary based on demographic factors. Other factors could influence the mental models and therefore variance in the sample should exist on these factors as well to capture all mental models in the population. Therefore, it should be researched which factors influence the mental models of the population in the field of cybersecurity.

The third knowledge gap is that limited research has been done on the mental models of different cyber mechanisms. Research on mental models of different mechanisms is necessary, because educating the population on just one mechanism will not make them resilient on all areas.

The fourth knowledge gap is that it is unknown how secure behavior should be measured. If secure behavior (e.g. whether people use antivirus software or how often they check whether HTTPS is in place) is measured, this is done using self-reported data. As stated before, this is potentially problematic since self-reported behavior does not always correlate with actual behavior (Wash et al., 2017). Research should be done on how to measure secure behavior, in order to be able to determine whether an intervention is successful.

A fifth knowledge gap is that most research focuses on mental models, and just a few papers describe research on the prevalence of earlier found mental models on risk perception in the population. Therefore, we do not know much about the prevalence of mental models in the population, which is necessary to develop effective and efficient communication for this population (Morgan et al., 2002).

The sixth and final knowledge gap concerns the existence of differences of opinion on the goal of cyber risk communication. For example, Furman et al. (2012) state educating should focus on completing and correcting the mental models, while Wash & Rader (2011) suggest incorrect mental models should be accepted and/or encouraged if they lead to secure behavior. Thus, a discussion should be held on the goal of cyber risk communication. But, this is not only a question of effectivity and efficiency, but is also an ethical question. A discussion is needed on the ethics of educating the population with the aim to develop incorrect mental models, if this makes them behave more securely when interacting with IT systems.

2.5 Main research question

In the previous section we saw that a lot of opportunities exist for research on mental models of risk perception in the field of cybersecurity. This study addresses the third knowledge gap, and partly the first.

The first knowledge gap is partly addressed by performing a limited review of methods used to explicate mental models. The third knowledge gap is addressed since this research is focused on mental models of VPN, which have not been researched before in literature. Because VPN is a concrete cybersecurity mechanism, detailed mental models can be elicited.

This research is focused on a specific population, namely employees in a professional services firm in the Netherlands. This research is focused on the Netherlands because of practical considerations.

And finally, this research is focused on the similarities and differences between the mental models of experts and laypeople. The focus on similarities and differences allows to identify the perceptions of both experts and laypeople, and to describe the differences between the groups.

This brings us to the following main research question: *“What are the similarities and differences between the mental models of experts and laypeople of VPN in a professional services firm in the Netherlands?”*

3. Study design

This section contains the study design. It presents the subquestions formulated to be able to answer the main research question, and discusses the research approach and methods used to answer the subquestions and eventually the main question. A complete overview of the study design is presented in figure 3.

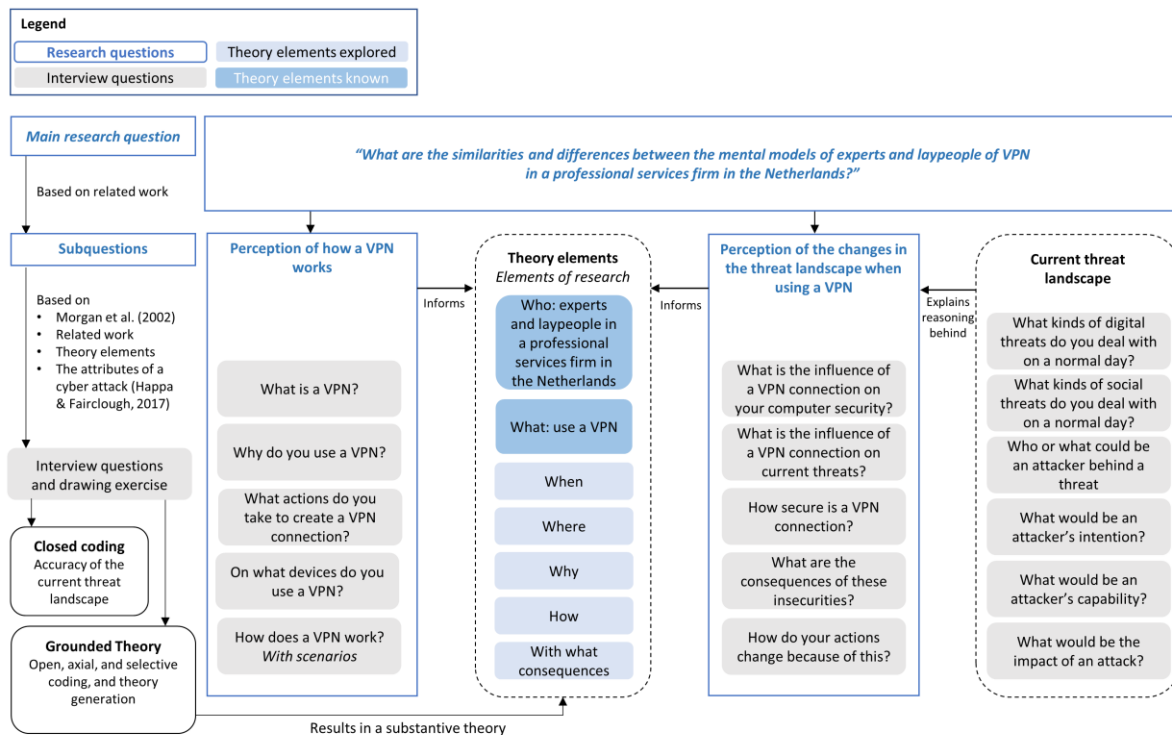


Figure 3: Conceptual model of the study design

In the next subsections the study design will be discussed in more detail. Section 3.1 presents the subquestions, section 3.2 introduces the research approach, section 3.3 presents the data collection method, section 3.4 discusses the target group, section 3.5 presents the data analysis method, and finally section 3.6 discusses the ethical considerations.

3.1 Subquestions

In this study the risk perception of the target group is researched, for which a mental model approach is used. Risk perception consists of multiple elements. In this study the focus is on the perception of how a VPN works and the perception of the changes in the threat landscape when using a VPN.

To be able to answer the main research question, the following subquestions are formulated. The subquestions are formulated based on related work.

1. What are experts' perceptions of how a VPN works in a professional services firm in the Netherlands?
2. What are experts' perceptions of the changes in the threat landscape when using a VPN in a professional services firm in the Netherlands?
3. What are laypeople's perceptions of how a VPN works in a professional services firm in the Netherlands?
4. What are laypeople's perceptions of the changes in the threat landscape when using a VPN in a professional services firm in the Netherlands?

3.2 Research approach

When capturing mental models of experts and laypeople, we essentially try to capture their knowledge about a certain topic. No theoretical framework exists at this moment for the topic of this study. To try to establish such a theoretical framework, an inductive exploratory approach is used. The objective for this research is to develop a substantive theory on the similarities and differences between the mental models of experts and laypeople of VPN in a professional services firm in the Netherlands.

The research approach is also a case study, since a detailed exploration of a specific case is done (Bryman, 2012). The case explored in this study is a professional services firm in the Netherlands. The selected case is representative for multinational professional services firms.

3.3 Data collection method

According to Sanders & Stappers (2012) four levels of knowledge can be distinguished. The first level is explicit knowledge, that what can be stated in words. The second level is observable knowledge, which contains thoughts and ideas that can be obtained by observing what happens or how people behave. The third level is tacit knowledge, which refers to things we know, but are not able to verbally communicate to others. The fourth and final level is latent knowledge, which represents the thoughts and ideas that we haven't experienced yet, but on which we can form an opinion based on past experiences.

Sanders & Stappers (2012) also describe techniques to help access these different levels of knowledge. These techniques can be categorized into three groups: what people say, what people do, and what people make. Combining these groups helps to elicit as much knowledge as possible. An additional benefit of combining methods is that it can help to structure the interviewee's mental model (Byrd et al., 1992), it can serve as means of verification (Jones et al., 2011), and reduces participant fatigue (Greyson et al., 2017). In this research what people say was combined with what they make.

What people can say about their mental model was elicited in an interview. Interviews were used as data collection method because of two reasons. First, interviews allow for a detailed exploration of a mental model. Second, interviews make it possible to identify mistaken beliefs.

During the interview, participants were requested to make a drawing. It depends on the specifications of the research which elicitation technique is suitable to use (Langan-Fox et al., 2000; Morgan et al., 2002). Multiple factors influence the decision for which elicitation technique is suitable, for example the interviewee's cognitive abilities, practical considerations, and the object of research. Examples of techniques that have been used in similar research are influence diagrams (Morgan et al., 2002), card sorting (Conrad & Tucker, 2019), mind mapping (Buitron de la Vega et al., 2018), free listing (Brewer, 2002), and drawing exercises (Krombholz et al., 2019; Maier et al., 2017). Drawing exercises were chosen in this research as elicitation technique to supplement the interviews because of multiple reasons. First, this technique helps to elicit visualizations of the interviewee's mental model (Morgan et al., 2002). Second, it offers the possibility to capture different concepts. Third, it allows to capture a wide range of relationships between these concepts. Fourth, drawing is a technique the interviewees are familiar with. And fifth, drawing offers freedom in the way of expression.

3.3.1 Interview design

The interviews were open-ended, semi-structured, one-on-one, online, and recorded. To give the interviewees the possibility to share detailed descriptions of their mental model an open-ended design was used as opposed to a closed-ended design like a questionnaire (Morgan et al., 2002). A semi-structured approach was used as opposed to an unstructured interview to ensure consistency in the interviewing method and to minimize researcher bias. One-on-one interviews were held to capture the perspective of only the interviewee and minimize the chance of the interviewee's perspective to be altered due to input from others. The interviews

were held online using conferencing software, because of government restrictions due to the COVID-19 pandemic. For analyzing purposes the interviews were recorded.

To make the interviewees feel as comfortable as possible, two choices were presented to the interviewee. The first choice was whether to enable video or not. The second choice was to hold the interview in either English or Dutch. If the interviewee did not have a language preference, the interview was held in English.

Before the start of the interview a short introduction was given. In this introduction participants were again informed about the purpose of the study, were asked to say as much as they know about a VPN during the interview and there were no wrong answers, and were again informed that the interview would be recorded. Additionally, a short demonstration of the drawing possibilities in the conferencing software was provided.

The interview consisted of three parts. The first part focused on how a VPN works. The second part focused on the current threat landscape. The third and final part focused on changes in the threat landscape that occur due to use of a VPN.

Questions were asked about the current threat landscape because of two reasons. First, the questions and answers provided a starting point to identify changes in the threat landscape. Second, it provided the possibility to estimate the accuracy of the perception of the current threat landscape. The accuracy of the perception of the current threat landscape is important to consider when reflecting on the perception of changes in the threat landscape due to VPN usage, because a distorted view on the current threat landscape could result in a distorted view on the changes in the threat landscape due to VPN usage. By evaluating the accuracy of the current threat landscape, this distorted view can be either identified or ruled out.

The interview questions were developed based on the methodology book of Morgan et al. (2002), related work, and the elements of a theory according to Strauss & Corbin (1998). The questions relating to the perception of the current threat landscape were developed based on the attributes of a cyber attack (Happa & Fairclough, 2017).

The first question of the interview was 'what is a VPN?'. This question was deliberately general of nature, to not bias the interviewee. Each topic mentioned was asked to elaborate. When a concept was named, the interviewee was asked to define that concept. When no new topics were introduced, the interviewer continued to the next question.

The remaining questions were developed so they were of a different type to introduce variance and as neutral as possible to not bias the interviewee. The interviewer tried to remain as passive as possible and only keep the oral fluency of the interviewee. The interviewer tried to use neutral continuation prompts to stimulate the interviewee to continue talking and to clarify topics. Examples of neutral continuation prompts are included in the interview protocol.

At the end of the interview, the participants were asked whether they knew anything else about a VPN that was not said yet and if they had any questions for the interviewer. Finally, when no new topics were introduced, the participants were thanked for their participation and the interview was finalized. The English and Dutch interview introduction and protocol can be found in Appendix A: Interview protocol.

3.3.2 Drawing task design

The drawing task commenced when the interviewee was asked 'how does a VPN work?' and was based on three scenarios. By including scenarios the influence of a specific context on the mental model can be researched (Bryman, 2012). The first was the basis scenario, where a VPN connection was established at home. The second scenario was based on a difference in physical location, where a VPN connection was made at a coffee bar. The third scenario was based on a specific task, where an e-mail was sent when connected via a VPN. At a later

moment in the interview, the interviewee was asked to also indicate where threats could present themselves in the drawing.

Participants were asked to think aloud while drawing. Thinking aloud while drawing was expected to provide rich verbal data (Fonteyn et al., 1993). Concurrent verbal report was used instead of retrospective, to capture more consistent and complete information about the interviewee's thinking process (Fonteyn et al., 1993).

No limitations were set on how to execute the drawing exercise, other than the use of the whiteboard in the conferencing platform. This was intentionally to preserve the freedom of expression of the interviewee and because it was expected that interviewees would picture the drawing exercise different in their mind. It was thought one might want to draw using words, while another would like to draw using symbols, or create a mind-map.

3.3.3 The platform: Big Blue Button

The interviews were administered on an online conferencing platform. The platform used is made available by Delft University of Technology. This platform uses the open source software BigBlueButton (BigBlueButton, n.d.) and the servers used for this service are provided by SURF (SURF, n.d.), a joint initiative of Dutch education institutions to provide IT services to the education sector. All servers used are located in the Netherlands.

For interviewees it was not necessary to download software to use this online platform. To enter the meeting room, interviewees had to provide a username and consent for the interview to be recorded. An illustration of the landing page is provided in figure 4.

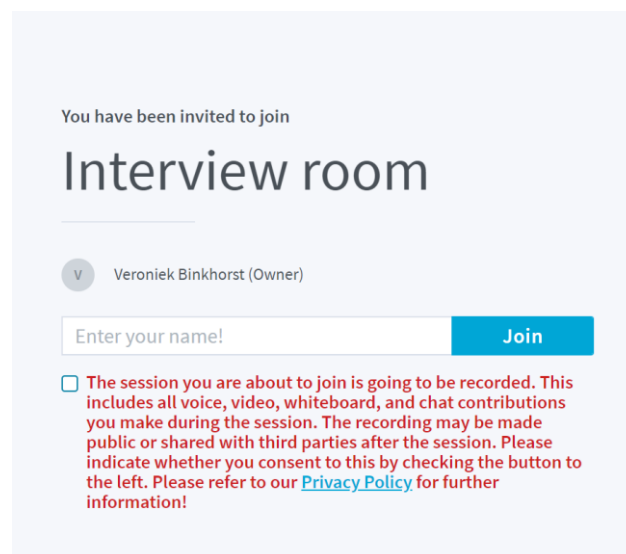


Figure 4: The landing page of the conferencing platform

The platform allows for audio- and videoconferencing and recording sessions. Additionally, it is possible to draw on a whiteboard, an illustration is provided in figure 5. On this whiteboard, it is possible to draw rectangles, triangles, circles, lines, and free-shapes using a pencil. It is also possible to type text, adjust the size of the lines, change colors, and undo actions. When using the whiteboard, all participants were able to see what was drawn and written by a participant, which made it possible to provide a concurrent verbal report when drawing.

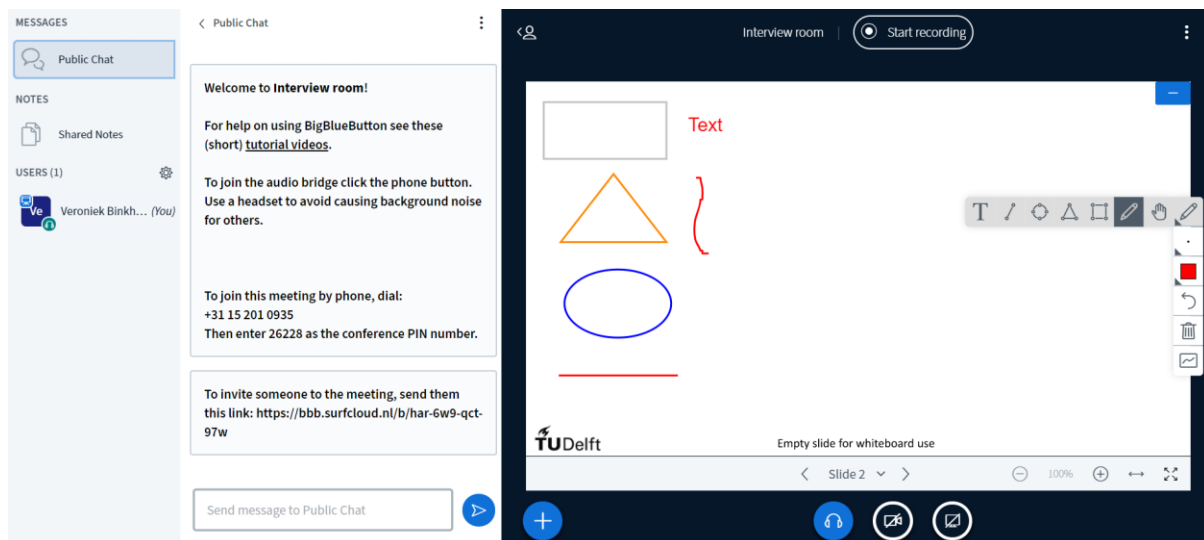


Figure 5: The whiteboard of the online conferencing platform

3.3.4 Validation of the interview protocol

To validate the study design pilot interviews were performed. Validation focused on the understandability and unambiguous interpretation of the interview protocol. Additionally, the answers provided in the pilot interviews were analyzed to prevent bias due to wording of the protocol.

Four pilot interviews were held with people who did not belong to the target group. These pilot interviews were held with friends, family, and a supervisor. Because the research focuses on a corporate VPN, a similar context was used as focus in these interviews (e.g. usage of a corporate VPN not in a professional services firm or a VPN used to connect with a university environment). After the completion of the pilot interviews, the four participants were asked if the questions were clear and whether they felt like a question was missing. The insights gained through these pilot interviews were used to adjust the protocol.

The adjusted protocol was used for the remaining pilot interviews, which included persons from the target group. These pilot interviews were administered with two experts and three laypeople. No additional adjustments were made to the interview protocol.

3.4 Target group

The population for this research is defined as employees in a professional services firm in The Netherlands. All employees interviewed handle confidential information and/or personally identifiable information.

3.4.1 Experts and Laypeople

To be able to answer the main research question the population has been divided into experts and laypeople. Experts are employees that work in an information technology department at the firm for a minimum of two years and/or employees that are in the possession of a relevant degree or certificate (e.g. EMITA, CISA, CISSP). Experts are considered expert users, not necessarily experts about VPN. Laypeople are employees that work in a department that is considered non-technical, for example the departments legal, finance, and HR.

Variation in knowledge naturally occurs in the expert and laypeople group. It was purposefully chosen not to select participants based on their knowledge about the research topic, in order to grasp all possible perceptions occurring in the target group.

3.4.2 Sampling method

Purposive sampling was used to draw a sample in a strategic way with the objective that the sample of employees consist of maximum variety on key characteristics. Sampling based on maximum variety was used in order to grasp all possible perceptions occurring in the target group.

The key characteristics were determined a priori. These key characteristics were educational qualifications, education area, role in the firm, and years active in the firm.

A fixed sample was used as opposed to sequential sampling, meaning that the sample was established at the start of the research (Bryman, 2012).

3.4.3 Sample size

In qualitative research data collection is done until the point at which no new concepts emerge from the data, this is called theoretical saturation (Bryman, 2012; Strauss & Corbin, 1998). Because of this reason, it was not determined a priori how many interviews were to be held. The intention was to collect and analyze data iteratively, to be able to determine when in three sequential interviews no new concepts emerged. If no new concepts emerged during these three interviews, theoretical saturation was established.

Because of participant availability and time restrictions, data collection and analyzes was not done fully iteratively. Whether theoretical saturation had been reached was determined after all interviews and data analyzes was completed.

In the expert group theoretical saturation has been reached, since in the last three interviews no new concepts were developed. When looking at the laypeople group separately, theoretical saturation has not been reached. However, when comparing the laypeople group with the expert group, no new concepts emerged in the laypeople group. Therefore, when looking at the complete sample, theoretical saturation has been reached.

3.4.4 Recruitment method

Access to the employees was facilitated by the company at which the researcher was performing a graduate internship. First, it was determined in which departments the target group could be found. Next, for each department a contact person was identified in consultation with the professional services firm. Once a list of contact persons was established, they were sent an e-mail.

In this e-mail the contact persons were informed about the study and requested to provide possible participants. In order to prevent selection bias, contact persons were not informed in this e-mail about VPN being the mechanism studied. The contact persons were informed about the purpose of maximum variation in participants and about the key characteristics. If requested by the contact person, more information about the study was provided.

In total contact persons for three expert departments and five laypeople departments were written. If no answer was provided to the initial e-mail, one or more reminders were sent. Eventually all contact persons replied to the initial e-mail or reminders. All three expert departments provided participants. One out of the five laypeople departments declined to participate. Another laypeople department indicated to search for participants, but did not reply anymore after several reminders. Eventually two out of the five laypeople departments provided participants and one laypeople department included a short recruitment message in their department newsletter.

Once a name of a possible participant was provided, he or she was sent an e-mail. A couple possible participants were informed by a contact person beforehand, but not all. Possible participants were informed about the purpose of the study, which contact person provided their information, the set-up of the interview, how collected data would be handled, and what would happen if they agreed to participate. They were purposefully not informed in this e-mail about VPN being the topic of research, to prevent self-selection bias or informing

themselves before the interview. Because it was expected that the possible participants were unfamiliar with the online conferencing platform used, the platform was explained to them and they were provided a link to an 'exploration room'. This exploration room was a special room created for the purpose of getting to know the platform. If possible participants felt the need to explore the platform beforehand, they could visit this room.

In total twelve possible expert participants and seven possible laypeople participants were written. If no answer was provided to the initial invitation, one or more reminders were sent. One expert participant declined to participate. The remaining eleven experts and seven laypeople agreed to participate in an interview.

A date and time was scheduled with the experts and laypeople who agreed to participate. In the meeting request a link to the 'interview room' on the online conferencing platform was included. Two days before the interview, the participants were sent an informed consent form via e-mail. In this informed consent form participants were able to find more information about the study, including the topic of the study being VPN, and with what they agreed by participating in the study. The informed consent form was provided two days before the interview, in order to provide the participants with enough time to read and process the information. Participants were asked to provide consent by replying to this e-mail, stating they give consent. All participant provided consent via e-mail. If a participant did not yet provide consent at the start of the interview, he or she was requested to read the consent form and provide consent before the start of the interview.

All participants were given the opportunity to ask questions in each phase of the recruitment process. The recruitment text for contact persons and possible participants and the informed consent form can be found in Appendix B: Recruitment Text and Informed Consent Form. This appendix does not contain the recruitment text in the department newsletter, as this text was short and contains many references to the concerning department. An overview of the recruitment process is provided in figure 6.

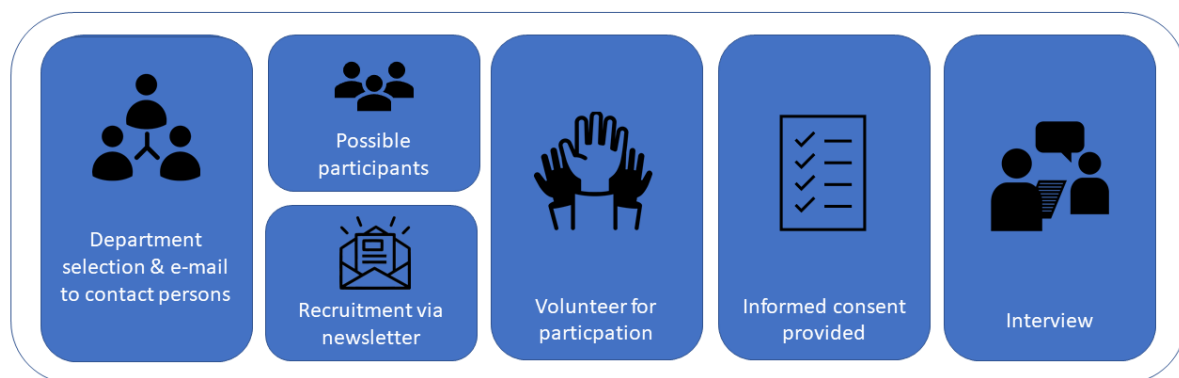


Figure 6: Overview of the recruitment process

3.5 Data analysis method

3.5.1 The data: transcriptions, drawings and notes of the interviewer

The data used as input for analysis consisted of transcriptions of the interviews, the drawings made during the interviews, and hand-written notes of the interviewer.

The interviews were transcribed with literal level of detail using the transcription software Express Scribe (NCH Software, n.d.). Literal transcription was used instead of verbatim transcription to be able to capture repetitions, which could indicate hesitation, and to capture unfinished sentences, which could provide more context. Extra literal was not used as transcription method because emotional expressions of interviewees, for example laughing, were not considered important for this research. All information relating to the identity of the company or employees was anonymized. A complete overview of all transcriptions can be found in Appendix C: Interview transcripts.

3.5.2 Grounded Theory

Grounded theory was used to systematically analyze the data (Corbin & Strauss, 1990, 2008; Strauss & Corbin, 1998). Grounded theory consists of four elements: open coding, axial coding, selective coding, and theory generation.

Open coding entails conceptualizing data based on characteristics and variations by assigning codes to the data. Codes are labels that assign meaning to pieces of the transcription (Miles et al., 2014). Open coding was done by exploring the data in a line-by-line manner. For open coding three methods described by Saldaña (2016) were used. The first method is descriptive coding, in which the code represents the topic of the statement. The second method is process coding, which represents actions that are described in the data. The third method is value coding, where codes represent values, attitudes and beliefs.

At the beginning of the coding process consultation took place between the student and a supervisor, in order to give a direction to the codebook. During this session, the initial coding of a couple transcripts was discussed and code description and criteria were reviewed.

During axial coding codes are grouped into categories and relationships between categories and between codes in categories are explored. Open coding and axial coding was performed iteratively. An illustration of axial coding with the use of post-its is provided in figure 7. Memo writing was used during the coding process to keep track of the thought process and theory development. It was documented what new codes were developed, why new codes were developed, what codes were difficult to differentiate, and what patterns and themes emerged. A complete overview of the developed code book can be found in Appendix D: Code book.

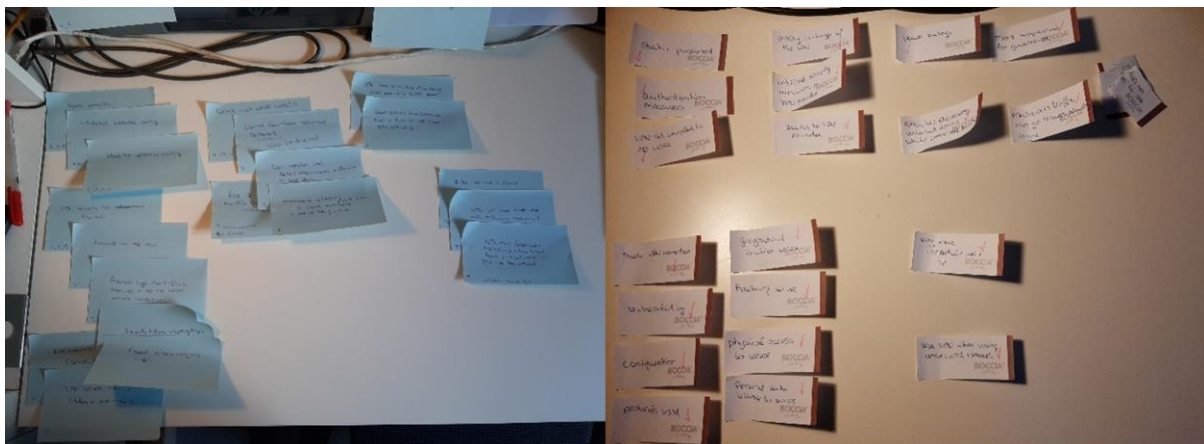


Figure 7: Axial coding with the use of post-its

Selective coding encompasses integrating and refining the theory. Integrating entails developing the central theme of the research. Refining the theory occurs by reviewing internal consistency and logic of the codes developed.

The last element of grounded theory is theory generation. According to Strauss & Corbin (1998, p. 15) a theory is “a set of well-developed concepts related through statements of relationship, which together constitute an integrated framework that can be used to explain or predict phenomena”. The statements of relationship explain who, what, when, where, why, how, and with what consequences an event occurs. The developed theory was validated by reviewing how well the abstracted, developed codes and their relationships fit with the original data, by revisiting the raw data. During coding, attention was given to negative cases, or outliers, to increase generalizability and explanatory power of the theory.

For coding the software ATLAS.ti version 8.4 (ATLAS.ti Scientific Software Development GmbH, n.d.) was used, for which the Delft University of Technology holds a license. Both the Dutch and English interviews were coded

using English codes. The Dutch transcripts were not translated due to time restrictions and to prevent bias occurring by altering the meaning of words during translation.

The intention was to perform interviewing, transcribing, and coding iteratively to be able to determine when theoretical saturation was reached. Therefore transcribing and coding started after the first interview was administered. Because coding took more time than anticipated, the process was not done fully iteratively.

3.5.3 Closed coding: the current threat landscape

To explore interviewee's perceptions of changes in the threat landscape, they were first asked to describe the current landscape. The description provided for the current general threat landscape was coded partially in a closed manner because of two reasons. First, frameworks already exist to describe different aspects of a general threat landscape. Second, it was not the intention to try to develop a new framework to describe this general threat landscape. The intention was to describe the current general threat landscape, in order to identify and describe the changes in the threat landscape due to the use of a VPN and estimate the accuracy of the perception of the current threat landscape.

Therefore, to code the threats mentioned, the threat actors, the threat actor's motivations and capability, and the possible impact of an attack, existing frameworks were used. The existing frameworks were applied after open and axial coding was done, in order to determine if all open codes could be covered by the existing frameworks. Currently no all-encompassing framework exists (Mavroeidis & Bromander, 2017). Therefore, different frameworks are used for the different categories.

Before the different frameworks are described, it is important to define a threat. A threat is defined as a potential cause of an unwanted incident, which can result in harm to a system or organization (ISO, 2018a).

3.5.3.1 Threat topology

Threats are coded according to the tactics in the MITRE ATT&CK framework (MITRE ATT&CK, n.d.). The tactics described in the framework encompass a group of individual techniques. The tactics and their description can be found in table 2.

Table 2: Closed coding framework for threats

Tactic	Description
Initial Access	The adversary is trying to get into the network
Execution	The adversary is trying to run malicious code
Persistence	The adversary is trying to maintain their foothold
Privilege Escalation	The adversary is trying to gain higher-level permissions
Defense Evasion	The adversary is trying to avoid being detected
Credential Access	The adversary is trying to steal account names and passwords
Discovery	The adversary is trying to figure out the environment
Lateral Movement	The adversary is trying to move through the environment
Collection	The adversary is trying to gather data of interest to their goal
Command and Control	The adversary is trying to communicate with compromised systems to control them
Exfiltration	The adversary is trying to steal data
Impact	The adversary is trying to manipulate, interrupt, or destroy systems and data

3.5.3.2 Threat actor topology

Threat actors are coded based on cyber threat actor topology of de Bruijne et al. (2017). In this framework, threat actors are described based on their characteristics. Examples of these characteristics are their target, expertise, and motivation.

In this research the questions regarding the current threat landscape were inquired separately. To illustrate, it was asked what threats were encountered on a normal day, then what threat actors were behind those threats. As a result, threat actors were named rather than described based on characteristics.

In order to not make assumptions on the relations between the different code categories, the threat actors are not described based on all characteristics used in the framework. Instead, an indicative description of who they are and/or what they do is used. Such a description has not been provided for all threat actors in the framework. In order to provide a description for the remaining threat actors, a description was established using the Cambridge Dictionary (Cambridge University Press, n.d.). The descriptions drafted using the dictionary are presented in *cursive* in table 3.

Table 3: Closed coding framework for threat actors

Threat actor	Description
Extortionists	<i>"Threat actor who tries to get something, especially money, by force or threats"</i>
Information brokers	Threat actor who trades (stolen) information in the world of cyber crime
Crime facilitators	Threat actor who provides technical support to the attacks of other criminal actors
Digital robbers	<i>"Threat actor who steals"</i>
Scammers and fraudsters	<i>"Threat actor who makes money using illegal methods, especially by tricking or deceiving people"</i>
Crackers	<i>"Threat actor who performs cracking, or the process of breaking into a computer or a network system"</i>
Insiders	<i>"A threat actor who works for a company or an organization and therefore has special knowledge or influence"</i>
Terrorists	<i>"Threat actor who uses violent action, or threats of violent action, for political purposes"</i>
Hacktivists	<i>"Threat actor who gets into computer systems without permission in order to achieve political aims"</i>
State actors	<i>"A country or its government"</i>
State-sponsored networks	State-affiliated groups which are organized in networks

Additionally, one more threat actor is introduced. This threat actor is professional criminals and comes from the framework from the annual Cyber Security Assessment of the Netherlands (NCSC, 2019). In the research of de Bruijne et al. (2017), their framework was compared with the framework used in this assessment. In this comparison, the threat actors extortionists, information brokers, crime facilitators, digital robbers, and scammers and fraudsters combined into the threat actor type professional criminals.

In this research, professional criminal are threat actors with experience, special training or education. The more specific threat actor type was used when possible. In other cases where interviewees were less specific, the threat actor type professional criminals was used.

3.5.3.3 Threat actor motivation topology

Motivations of threat actors are coded using the framework of Tim Casey (2015), presented in table 4.

Table 4: Closed coding framework for the motivation of a threat actor

Threat actor	Description
Accidental	Benevolent or harmless intent but with actions that inadvertently cause harm
Coercion	Forced to act illegally on behalf of another
Disgruntlement	A desire to avenge perceived wrongs through harm
Dominance	Attempting to assert superiority over another
Ideology	A passion to express a set of ideas, beliefs, and values that shapes and drives harmful acts
Notoriety	Seeking to become well known for harmful activity
Organizational gain	Seeking an advantage over a competitor's organization
Personal financial gain	Improve one's own financial status
Personal satisfaction	Fulfilling an emotional self-interest
Unpredictable	Acting without identifiable reason or purpose and creating unpredictable events

3.5.3.4 Threat actor capability topology

The capability of a threat actor is coded using the skills in the Threat Agent Library (Timothy Casey, 2007), presented in table 5.

Table 5: Closed coding framework for the capability of a threat actor

Capability	Description
None	Has average intelligence and ability and can easily carry out random acts of disruption or destruction, but has no expertise or training in the specific methods necessary for a targeted attack
Minimal	Can copy and use existing techniques
Operational	Understands underlying technology or methods and can create new attacks within a narrow domain
Adept	Expert in technology and attack methods, and can both apply existing attacks and create new ones to greatest advantage

3.5.3.5 Threat impact topology

Impact is coded using the description of threats in the annual Cyber Security Assessment of the Netherlands, published by the NCSC (2019), presented in table 6. While in the report the description is given of threats, it was thought they were more appropriate to describe the possible impact of a threat.

Table 6: Closed coding framework of the impact of a possible threat

Impact	Description
Disruption	Intentional temporary impairment of the accessibility of data, information systems or information services
Sabotage	Intentional and very long-lasting impairment of the accessibility of data, information systems or information services, possibly resulting in destruction
Data manipulation	Impairment of the integrity of information by means of the intentional editing of data
Data theft	Impairment of the confidentiality of information by means of the copying or removal of data
Leak	Impairment of confidentiality due to natural causes, technical difficulties or human error
Espionage	Impairment of the confidentiality of information by means of the copying or removal of data by nation-state actors or nation-state-affiliated actors
System manipulation	Impairment of information systems or information services targeting the confidentiality or integrity of these systems/services. These systems or services are subsequently used to carry out other attacks
Breakdown/Failure	Impairment of integrity or accessibility due to natural causes, technical difficulties or human error

3.5.4 Inter Coder Agreement

To ensure that the data is interpreted in the same way by all users, partial double coding was performed to determine the reliability of the codebook. Reliability means the degree in which the codes in the codebook are applied to the data in a consistent manner by multiple persons (Krippendorff, 2004). When reliability is high, it can be said with more certainty that the theory formed based on the data is valid.

To infer reliability the Krippendorff c-alpha-binary was calculated. The c-alpha-binary coefficient indicates for each code whether the different coders have identified similar or the same areas in relation to a given code and takes chance agreements into account (ATLAS.ti Scientific Software Development GmbH, 2019; Krippendorff, n.d.). According to Krippendorff (2004), a semantic domain can be considered reliable if the coefficient is equal to or above 0.8, unreliable below 0.667, and only suitable for tentative conclusions if between 0.667 and 0.8. A semantic domain is a group of distinct codes that share a common meaning.

The data used for partial double coding consisted of three expert interviews. At first, the overall c-alpha binary was 0.724. As recommended by Barbour (2014), disagreements were explored to develop more nuanced and

useful codes. Disagreements consisted mainly of two issues. The first is a different application of the concept codes. The second is a difference in quotation length, where one researcher used one quotation, the other had divided it into two different quotations. After resolving these issues, the overall c-alpha binary was raised to 0,837, and equal to or above 0.74 for all semantic domains. This indicates a reliable codebook. It is important to note that the c-alpha-binary coefficient is not statistically significant, as the number of codings per semantic domain are not high enough to establish significance. A complete overview of the c-alpha-binary coefficients per semantic domain can be found in Appendix E: Overview of ICA coefficients per semantic domain.

3.5.5 Accuracy of the mental models

The identified theory, or mental models, were evaluated based on their accuracy to identify which concepts were correct and which concepts were mistaken beliefs.

To evaluate the accuracy of the perception of how a VPN works and the perception of changes in the threat landscape when a VPN is used, the concepts in the mental models were compared with how a VPN works in reality. The real-world representation of VPN organization is depicted in section 2.2: Virtual Private Networks. This real-world model is developed by the author of this research based on information provided by a supervisor, Dr.-Ing. Tobias Fiebig, and has been double checked by the same supervisor. This model was developed after all data was collected and coded, which limited confirmation bias and promoted open mindedness.

To evaluate the accuracy of the perceptions of the current threat landscape, the answers were compared with the Cyber Security Assessment Netherlands (NCSC, 2019). Specifically the results for threats, threat actors, and threat impact were compared with the threat matrix in the Cyber Security Assessment.

3.6 Ethical considerations

This research was reviewed and approved by the Human Research Ethics Committee of Delft University of Technology (reference number: 55223). During recruitment and in other phases of the research possible participants were not in any way deceived.

Participants were recruited via an informative e-mail after their name was provided by a contact person. When a participant agreed to be interviewed, an informed consent form was sent to them two days before the interview to provide them with ample time to review the form. Participants were informed they could withdraw at any point without the need to provide a reason. Participants were not compensated for their participation.

Five types of data were gathered. The first type is the e-mail addresses of the participants. Second is a PDF file of the informed consent e-mail. Third is demographic information of the interviewees. Demographic information consisted of educational qualification, education area, role in the firm, and years active in the firm. Fourth is the recording of the interviews, which included audio and included video if video was enabled during the interview. Fifth is the drawings made during the interview.

A possible risk for participants was identified, since their knowledge may be different than expected from experts and/or laypeople in a professional services firm. These concerns were addressed by taking five measures. First, the e-mail addresses, pdf file of the consent e-mail, demographic information, recordings of the interviews, and drawings made during the interviews were stored in a secure manner. Second, transcriptions and drawings were anonymized, so they were not traceable to a person or the professional services firm. Third, demographic information is presented in a summarized manner. Fourth, the original e-mails were deleted from the e-mail inbox. Fifth, the e-mail addresses, original demographic information, interview recordings, and original drawings were deleted after the end of the study.

The online conferencing platform used to administer the interviews is developed in a privacy preserving manner. The servers used for this service are located in The Netherlands.

The participants were informed that the summarized demographic information, anonymized transcriptions, and anonymized drawings would be shared in products of the study and would be stored on the 4TU.Centre for Research Data for a minimum retention period of 10 years¹ after publication or public release of the work of the research.

The participants were informed that it was within their rights to request access to and rectification or erasure of personal data. Nobody except the project research team had access to the data during the study period.

¹ In accordance with the TU Delft Research Data Framework Policy. Available online: <https://doi.org/10.5281/zenodo.2573160>

4. Results

In this section the results are presented. To illustrate the results, quotations from the interviews are included. Quotations that were originally Dutch have been translated to English. Section 4.1 presents the statistics of the interviews and participants. In section 4.2 the perception of how a VPN works is described. In section 4.3 the perception of the current threat landscape is outlined. And finally, in section 4.4 the perception of the current threat landscape is described. The subheadings of the sections 4.2 until 4.4 are based on the interview protocol and emerged themes.

4.1 Statistics interviews and participants

In total eighteen interviews were held. Of the eighteen interviews, eleven were with experts and seven with laypeople. One expert chose to enable video and five experts were interviewed in English. The remaining experts and laypeople chose to disable video and were interviewed in Dutch. Because the interview protocol was not changed during or after the pilot interviews, the pilot interviews are included in the study. Table 7 presents the interview statistics.

Table 7: Statistics of the interviews

	Experts (n = 11)	Laypeople (n = 7)	Total (n = 18)
Average duration [min]	52	31	44
Range [min]	29 – 88	13 - 48	13 - 88

The eighteen interviewees varied on key characteristics. Table 8 presents the demographic information of the participant. Important to note is that one person can hold multiple additional qualifications. All interviewees hold one or more additional qualification. Education area relates back to the educational qualifications, where again one person can be schooled in one or more education areas.

Table 8: Demographic information of the participants

Characteristic	Sub-characteristic	Experts (n = 11)	Laypeople (n = 7)
Educational qualifications	Master	9 (82%)	6 (86%)
	Bachelor	2 (18%)	1 (14%)
Additional qualifications	IT-audit (EMITA or CISA)	7 (64%)	-
	Privacy (CIPP/E, CIPM, FIP, CIPT, DPO)	6 (55%)	-
	Cybersecurity (CISSP, CSX-P or ISO27001)	5 (45%)	-
Education area	Business administration	4 (36%)	3 (43%)
	Computer science	4 (36%)	1 (14%)
	Crisis and security management	1 (9%)	-
	Engineering, non-computer	3 (27%)	-
	Law	1 (9%)	2 (29%)
	Accountancy	-	1 (14%)
	Marketing	-	1 (14%)
	Sociology	-	2 (29%)
Role in the firm	Department director	0 (0%)	2 (29%)
	Department manager	3 (27%)	2 (29%)
	Staff	8 (73%)	3 (43%)
Years active in the firm	Median	4	6
	Minimum	1,5	1
	Maximum	6,5	34

4.2 Perception of how a VPN works

4.2.1 Reason for use

Both experts and laypeople think the abbreviation VPN means a Virtual Private Network. Two reasons are described why a VPN is used. The first reason is to access the internal network and the second reason is for a security purpose.

The internal network is accessed to **access internal or private webpages or other resources**. When located outside of the corporate network, it is necessary to make a VPN connection to access these resources. It is not possible to access these resources if outside of the network and not connected to the VPN. However, one of the experts noted:

"I recently started using Edge or Chrome. And I believe, at least for Edge in the beginning, you sometimes didn't need a VPN connection to get to certain [the professional services firm] tools, so I found that interesting, how that works." [Expert 6]

Confusion exists among experts on what resources are only accessible via a VPN connection. The most prominent example on which confusion seems to exist is e-mail:

"But e-mail, if I only have to use e-mail and [cloud software], then I leave the VPN off, because then it is not necessary." [Expert 2]

"Within [the professional services firm] I use a VPN to set up a connection to [the professional services firm] network. People always say, so your traffic is safe. So I can safely check my e-mail." [Expert 10]

"And I know, for example, that previously it was necessary for our mail traffic to connect to the [the professional services firm] network, and that is no longer the case nowadays." [Expert 11]

The other reason why a VPN connection is used is because of a **security purpose**. A situation that leads to the need to create a secured connection is when the experts or laypeople are outside of the corporate network and not able to use a trusted network. An example of a trusted network is someone's home network. When presented with this situation, one out of two options are chosen.

The first option is to use an unsecured network, for example a Wi-Fi network in a café or train. This unsecured network can be protected with a password, but this is not necessarily the case. In this situation it can be chosen to establish a VPN connection to secure the connection. According to experts, and laypeople 2 and 7, this would protect the confidentiality and integrity of the communication:

"And that means that that connection basically forms a tunnel with the appropriate protocols and ensuring the encryption of the traffic. [...] to make sure the traffic is not readable to everyone around us, using the VPN to shield off and basically wrap-up the traffic in a format that they can't read it." [Expert 3]

In another situation, a layperson explains a network in the café might be less secure than a home network, because more people know the password to the network in the café:

"[...] look, in a cafe, when you log in to a cafe, formally you should check carefully whether you have a secure connection [...]"

X: Yes. And you say you need to check that it is a secure connection, what do you mean by that?

Y: Well, yes, I've always heard that. Well, look, if I look at my home situation then [...] I only have one person who logs in, who has the password for the router. At a café connection or well, Schiphol, whatever, then you have more people logging in on the same network. I don't know if that's [...] safe or not. I assume that the moment you use your VPN that it is safe." [Layperson 5]

He or she only does not explain what would make the connection more secure:

"X: And what is the difference between the situation that you are not using a VPN and that you are using a VPN?"

Y: Well, when I use a VPN, I can access all my systems and programs. The moment I don't do that, I won't be able to access that. So then I have no access to the secure data of [the professional services firm].

[...]

X: So what is the difference between a connection with VPN and without VPN?"

Y: Without a VPN you probably don't always have a secure connection. For the programs and data from [the professional services firm] you do. But that is just how you deal with it." [Layperson 5]

However, not all experts and laypeople think a VPN connection should be established when an unsecured network is used:

"[...] I am a bit scared to use VPN from public places, like if I am sitting in a barista café [...] Well, in a way I am worried that someone tries to target my system, just because I have sensitive information and I am connected to a publicly accessible network, which may or may not be very secure. [...] I know there are a lot of hacks possible from a network which is not secure, especially when you're connecting VPN [...]"

X: Why are you scared to use VPN in a public space?"

Y: Because I am partially aware of the kind of attacks that are possible. I do not know if someone will try to listen or look at the traffic that is going through the channel, if the Internet that I am connecting to is not secure." [Expert 5]

Experts who are presented with this situation explain that they would either use the unsecured network if strictly necessary, but without a VPN connection, or that they would use their mobile network.

The second option is solely described by experts and is to use a mobile network. A mobile network is thought to be more secure than an unsecured network because of two reasons. First, the mobile device is provided by the professional services firm, and therefore the firm has approved this mobile network:

"Well, first, the hotspot is provided by a network that is approved by [the professional services firm]. [...] The difference is, I have right now Internet connection through [telecom provider]. So, [telecom provider] is the preferred service provider for [the professional services firm]. I can imagine [telecom provider] taking extensive measures to make sure their, the Internet that they are providing through the phone is secure and it is not easily crackable." [Expert 5]

The second reason is that no entity is in the middle of the connection that could be listening in:

"So when I'm somewhere, like an airport or [example of restaurant], I just use my phone, that's a 4G network, that's my own network, so nobody can [...] listen in on it, eavesdrop." [Expert 1]

A reason to not use a mobile network instead of an unsecured network would be the cost of using the mobile network, for example when traveling outside of the European Union.

When using a mobile network, the choice to establish a VPN connection or not still remains. Reasons to make a connection could be because it is necessary to access the corporate network or for security purposes. Some doubt exists on how secure the mobile network itself actually is:

"X: And what is the difference between your personal hotspot and the public network?"

Y: Very good question. I don't dare to say and maybe that's why I always set up a VPN after all. [...] Better safe than sorry, let's just say." [Expert 10]

A simple reason not to establish a VPN connection would be because it is just not necessary to access the corporate network.

4.2.2 Device on which the VPN can be used

The corporate VPN can be used on three different types of devices provided by the professional services firm. It can be used on the **personal computer, a mobile phone, or a tablet**. Among both experts and laypeople confusion exists on whether their phone makes a VPN connection when internal applications are accessed:

"For work I only use my laptop. For my mobile device [...] I don't know the name of the application, but [example of mobile application], and I suspect that's also somehow secured.

X: Do you also mean secured via a VPN connection or in some other way?

Y: I don't really know. It's a bit strange as a security expert that I don't know that, but you do expect that your place of work has made good arrangements. But [...] you do receive a message that it is encrypted. So I expect it to be, yes, I don't know if it's really a VPN, but I do expect it to be somehow, um, secure." [Expert 2]

4.2.3 User steps to establish a connection

The user actions to establish a VPN connection are described as follows. First, the user needs to **connect to the Internet**. Second, the user needs to **launch the VPN software**. Third, according to only experts, the user needs to **enter his or her username**. Fourth, the user needs to **enter his or her password and access token code**. As the final step must be **clicked on the button connect to the VPN**. The code from the access token can be provided by a software or a hardware token.

Important to note is that one layperson explains the user actions taken to establish a connection with the internal network and does use the name of the VPN of the professional services firm, but also explicitly states he or she does not start the VPN. The VPN connection is made automatically when performing the user actions:

"Well, I press an icon at the bottom of my taskbar, because I put it there. Then I enter my personal password plus the, what are they, five digits that appear on the [the VPN of the professional services firm] app. And together they connect to the intranet of [the professional services firm]. I do not specifically start VPN. But my presumption is that that is behind it. That the intranet applications all are approached via a VPN connection and that you start it up automatically with [the VPN of the professional services firm]." [Layperson 7]

4.2.4 Infrastructure

4.2.4.1 Basic configuration

In the perceptions of the technical infrastructure of a VPN more variation exists. Laypeople and experts describe four possible configurations.

The most simple architecture is described as the own device making a connection with the corporate network, as illustrated in figure 8. Interviewees use different names for the corporate network interchangeable, for example internal network or private network, and it is not always certain to what exactly they refer. Therefore, in this section is referred to the corporate network, unless otherwise specified.

In a variation, layperson 5 explains a connection is made with a server or router of the professional services firm that is located in the corporate network. In this corporate network multiple servers can be found, described as a 'serverpark'. These servers reduce the risk of information loss, by being back-ups of each other.

In the second configuration named by both experts and laypeople, also depicted in figure 8, the traffic is routed through a VPN server to the corporate network. If a connection is made to a public website, this traffic is also

routed through the VPN server. The location of the VPN server is not specified or it is explicitly stated that the VPN server is located outside of the corporate network.

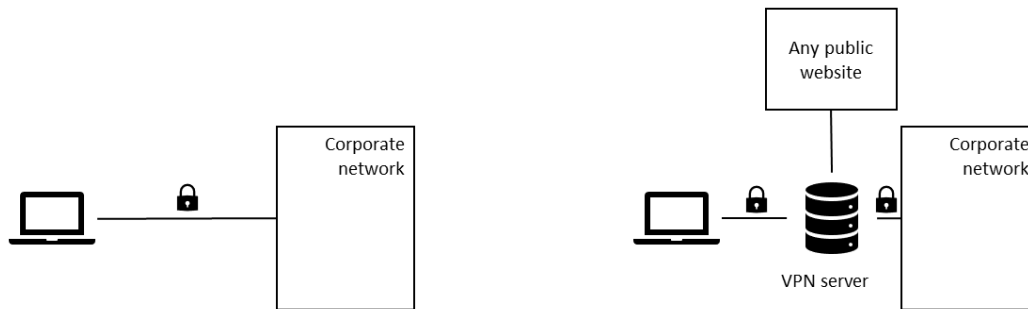


Figure 8: First and second basic configuration of the infrastructure

The third and fourth configuration are only named by experts. In the third architecture described, the location of the VPN server is inside the corporate network. This architecture is presented in figure 9. If a user wants to access internal resources, this is where the connection ends. Or, if a user wants to visit any public website, the traffic is routed through the VPN server in the corporate network to this public website. Contradictory, expert 1 stated that this architecture is not possible, that is just not exists.

The fourth architecture is also presented in figure 9 and depicts two situations. First, the server is located in a DMZ, or a demilitarized zone, which is described as a less secured, publicly available segment of the corporate network. The webtraffic is routed through the VPN server in the DMZ to the corporate network. The second variation of this architecture is the existence of a separate authentication server. As the name implies, when a connection is made, this server is used for authentication. When it has authenticated the user, a signal is send to the VPN server, making it possible to rout the traffic to the VPN server and access the corporate network.

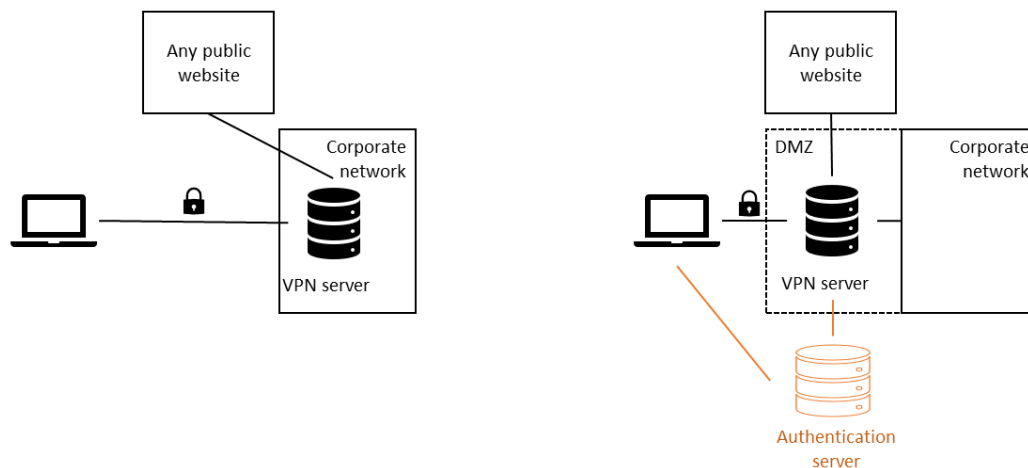


Figure 9: Third and fourth basic configuration of the infrastructure

In these configurations, it is important to determine what a server is. While the descriptions of experts vary a little, a VPN server is essentially described as a computer that facilitates the connection. Laypeople are in contention what a server exactly is:

"A server is really just a computer." [Layperson 2]

"I would describe that as an IT system where all data is stored." [Layperson 5]

"[...] actually a folder on eh, so, yeah, just really a documents folder [...]" [Layperson 1]

4.2.4.2 Additional specifications

Additional to the basic configurations, experts describe three additional specifications. The first specification, depicted in figure 10, is the existence of a complete and split VPN:

"[...] I call it complete and split tunnel. So you can route all the traffic through a VPN and what often happens, is you send all the traffic to the data center, which then redirects you back to the correct point. Either you have a shared or a split and then an organization determines which endpoints, or which IP addresses must go through a VPN tunnel and which not." [Expert 1]

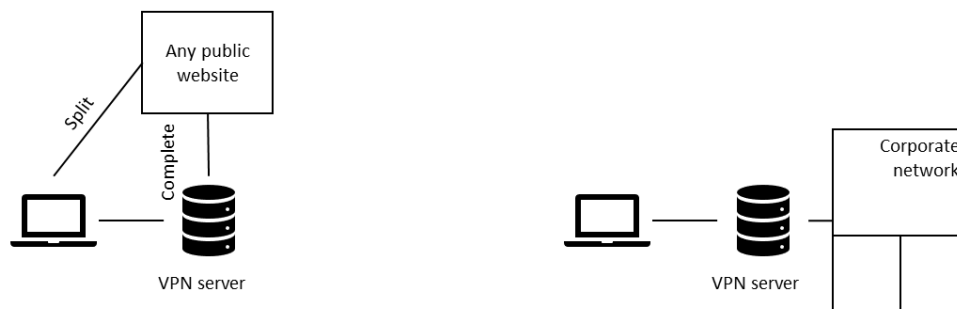


Figure 10: First and second additional specification of the infrastructure

The second specification, also depicted in figure 10, is segmentation of the internal network:

"X: What do you mean by that, that it is segmented?"

Y: [...] so it's anyway its own virtual network within what belongs to [the professional services firm]. Of course the VPN receiver will never be able to open up free connections to the entire network that way, but only make sure that I can connect to the network or parts of the network. As will be the case with a normal connection." [Expert 11]

The third specification is the entity that is providing the VPN connection. It can be that the professional services firm is its own provider. Or it can be that a third party is the VPN provider. According to one expert, it is possible that one organization can have multiple providers:

"[...] not all organizations have closed that for one, or opened that up for one specific VPN provider, but it can also be several, as long as you know the password. As long as you have the correct credentials to log in." [Expert 1]

4.2.4.3 What makes the connection secured

In section 4.2.1 Reason for use was specified that one of the reasons to use a VPN connection is to make a secured connection. In this section is described what employees mean when they refer to a secured connection. In total seven different meanings are identified for a secured connection. Not all employees refer to all options and different options can be combined.

Two options are described by both experts and laypeople. The first option is **encryption** to safeguard confidentiality and integrity. Encryption is described as a way to code text, so others cannot read it, except for the entity the communication is intended for:

"This encryption means that like when we are talking in a different language, the VPN is using another language. [...] With an encryption the VPN could be using a different language, which cannot be read by an outsider who doesn't have this list of decoding of the encryption. [...] Even if they were able to tap into this connection." [Expert 4]

"[...] if you send from one point to another, information encrypt need to have like the key to actually read the encryption, if you don't, if you see from here, you just see a lot of symbol, let's say inside. So, if you don't have the key to decrypt them, they have no sense for you. Have no meanings." [Expert 8]

Another description is given by layperson 7, who explains encryption as a tube in which you put your communication, which is protected by a key:

"[...] but the message you make, is put in a kind of tube, as it were. And that tube, there is a key on it and on the other side that key goes off again. So should that message somewhere on the way, or should that tube somewhere along the way be opened, then you have to have that key to be able to read that message in it." [Layperson 7]

When asked which of the connections were encrypted, answers varied. In figure 8 and 9, a lock is included to indicate to which of the connections were referred to as encrypted. When a lock is included, this does not entail that all interviewees indicated that this connection was encrypted, but at least one. Two interesting perceptions are that of laypeople 7 and 2:

"Well, I think the encryption takes place from the VPN server. [...] Whether that also applies between the user and the VPN connection itself, which also runs over the Internet, I do not know." [Layperson 7]

"Everything you do online from your computer, that does not go open towards the router and towards the Internet. That part is protected, so it goes through that tunnel. [...] Yes, because of course there is also the Internet provider [...] which cannot access it either. So then it's probably until the server of the Internet provider. Until where that tunnel goes, that's that last point. And yes, at that moment when it enters the Internet, then yes, that data is no longer protected [...]"

X: Okay. And suppose you connect now, or you want access to an internal application, what would that look like in this drawing?

Y: Um, yes, then the tunnel might go to that internal application." [Layperson 2]

Layperson 6 describes another use case of encryption via VPN, where it is used to encrypt communication between two people:

"I have a key on my side. [...] And then on the other side, I have the receiver here somewhere, whoever that is. Someone who is also on the [the professional services firm] network. [...]"

X: Yes. And you said that the [the professional services firm] receiver is someone who is also on the [the professional services firm] network-

Y: Hmhm. Yes.

X: What does this mean?

Y: That that is someone who, but I am not sure, but I actually assume this, that the receiver also has a VPN connection with [the professional services firm]. But that, no, what I am saying now is not true, because I think someone can just read the messages, even if they are not logged in via VPN. But I'm not sure about that.

X: Yes. And how would it work if someone who is not logged into the VPN can read the messages?

Y: Then I don't think it would work properly. So I guess if these messages are sent over VPN, then they are, because the [the professional services firm] receiver could be a system too, in this case. [...] So the [the professional services firm] receiver is apparently on the VPN network, because otherwise it cannot say that I, um, cannot connect.

[...]

X: Yes. And a [the professional services firm] receiver, can that also be a person?

Y: Yes, so that could also be a person, but that's a bit unclear to me now, because they had a lot of things behind the VPN before, for example, you could only access mail if you were connected to the network or was logged in via a VPN, but that they changed because of the corona woes. [...] So I know that in the beginning, that certain things were removed from VPN, [conferencing software] is another example. So those are not in the VPN network, so, in theory everyone could just read it." [Layperson 6]

The second option described by both experts and laypeople is that the connection is secured because of the **authentication measures** used to verify the user's identity:

"You say it is a secure connection, what do you mean by that?"

Y: Well, only that because you have an app on your phone that gives you a code, that not everyone can just get, that you can only log in to the network that way. So in the sense that it is technically enforced that you first need a software token code, before you can access the network at all." [Expert 6]

The authentication measures exist of the combination of username, password, and access token code.

The third until the seventh option are solely described by experts. The third option is referring to a VPN connection as **private**, but not encrypted:

"X: Okay. And you describe it as a private network, what do you mean with private?"

Y: Um, as in not connected to the external Internet, I suppose. It is like a shell around your organization and inside the shell all the data traffic is of course not linked to the outside world [...]" [Expert 9]

The fourth option is **filtering** of the connection. All webtraffic that goes through the VPN connection is filtered. This can be because the webtraffic goes through a firewall, IDS, IPS, antivirus, or just filters. Expert 9 indicates that filters exist on the connection, but does not know exactly what these are, as illustrated in the drawing made by expert 9 in figure 11.

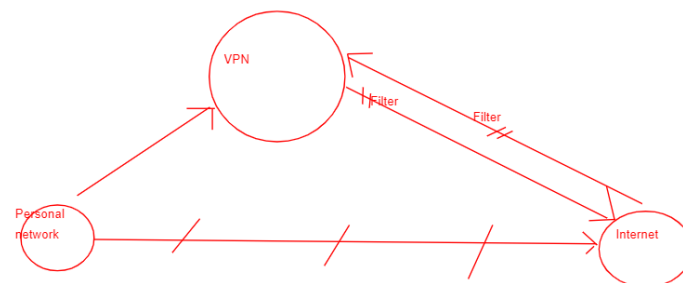


Figure 11: Drawing made by expert 9

Another expert indicates that the firewall and antivirus are located in the VPN server. He or she explains that the own device has an antivirus, but the antivirus on the VPN server is of a higher level and offers better protection against malicious software coming through the webtraffic, because it has all latest updates:

"Imagine that this server is your PC. And you are connected to this PC. Imagine that it is in your home, in your room, so this server has the latest version and the strongest version of antivirus, it has the strongest version of anti-hacking or malware, as they call it. [...] So, using this server can provide this extra layer whenever there is virus that is coming to your browser, coming to your PC, coming to your laptop. Through this server, the server should act as a firewall, a defense layer, that's stopping this virus." [Expert 4]

In this section is not described what experts understand a firewall or antivirus is, section 4.4.1 Mitigation of threats due to VPN usage explicates their perception of what these features can do.

The fifth option is the use of a **private IP-address**, that is only known between the VPN server and the corporate network:

"Normally I would connect to [the professional services firm] using my IP, which is my Internet name. [...] [the professional services firm] sees me as this and it will not allow me to enter their server to access their services. [...] So, I need to have a secure connection because this can be copied easily, this is a public IP, so anyone can use this public IP. [...] So, how can we make this secured connection is to have for example a number of secure IPs [...] it is a bit more complicated than this, but this is the concept that they have private IPs that are only known between the server and [the professional services firm]."
[Expert 4]

The sixth option is related to the **provider of the VPN connection**. Different types can be distinguished and they vary on the risk of someone intervening in the middle and the strength of the antivirus protection:

"[...] you have multiple types of VPN. So, you have the commercial VPN, some company who bought a server, put it online and ask people to pay subscriptions to use this VPN server. So, this would be secure, but it would not be highly secure. Then you have another VPN server which is from a well-known corporate, so for example using secure [company] server. So, this [company] server, they have a name they need to maintain so they use a really state-of-the-art server. So, this is the second level. The third level, which is the highest level, is that a VPN that is provided from your corporate, for example from where I work at [the professional services firm], they have provided their own VPN, this is known, this is the highest level. [...] There is no way of anyone intervening in the middle. No third party." [Expert 4]

The seventh and final option is **masking of the IP-address**. Because webtraffic is routed through the VPN server, the IP-address of the original sender is no longer visible to the receiving entity. Instead, it sees the IP-address of the VPN server:

"[...] it protects the, or it confuse your region IP. For instance, I can visit a website now from The Netherlands, but with some VPN connection I can appear as for instance I am in Italy." [Expert 8]

This allows for anonymous browsing. Or according to some experts, for partially anonymously browsing, because the IP-address can still be related back to the professional services firm.

4.2.4.4 Metaphors used

Both experts and laypeople use metaphors to illustrate their perceptions. These metaphors can be categorized into two groups. The first group of metaphors contains metaphors relating to authentication. In this group metaphors such as a safe, gate, door, shield, or secured zone are used, as illustrated in the drawing of expert 6 in figure 12. When a user does not have the right credentials, he or she is unable to open the safe, gate, or door, or unable to pass through the secured zone, and therefore is not able to establish the VPN connection:

"X: Can you tell us more about the yellow line?"

"[...]"

Y: [...] it is a certain zone that you basically have to go through. [...] I'm not quite sure if it's a zone, yeah, some sort of secured zone that you have to go through first [...]."

X: What do you mean by secured?"

Y: Yes, that you can only get through it if you get the right access."

X: And you also describe it as a tunnel, what do you mean by that?"

Y: Yes, a tunnel environment. [...] So there will be something like a tunnel or some kind of safe, which will only open if you enter the correct codes." [Expert 6]

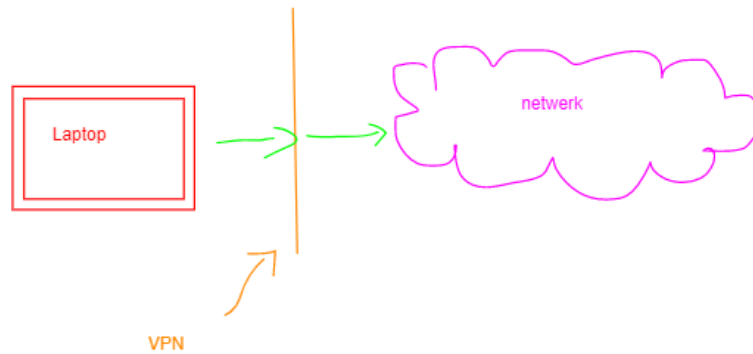


Figure 12: Drawing made by expert 6

Layperson 5 describes a shield in front of the corporate network, illustrated in the drawing of layperson 5 in figure 13. A connection can only be established with the corporate network if the right credentials are provided.

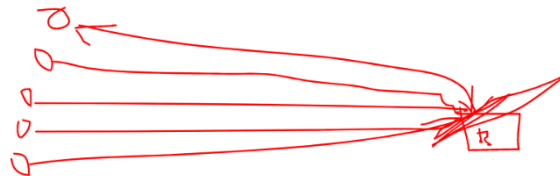


Figure 13: Drawing made by layperson 5

The second group of metaphors describe how information is protected in the data transfer. The connection is described as a tunnel, illustrated in the drawing by layperson 2 in figure 14. Other ways to describe it are a tube, or a shell. Information in this tunnel, tube, or shell is not readable to anyone trying to snoop in:

"X: You describe the connection as a tunnel, what do you mean by a tunnel?"

Y: Yes. I see it a bit as a kind of protective cover that surrounds the data.

[...]

Y: Yes, as a kind of protective layer, so that you cannot see through it, say from the outside, and where that data then passes. Instead of just being open." [Layperson 2]

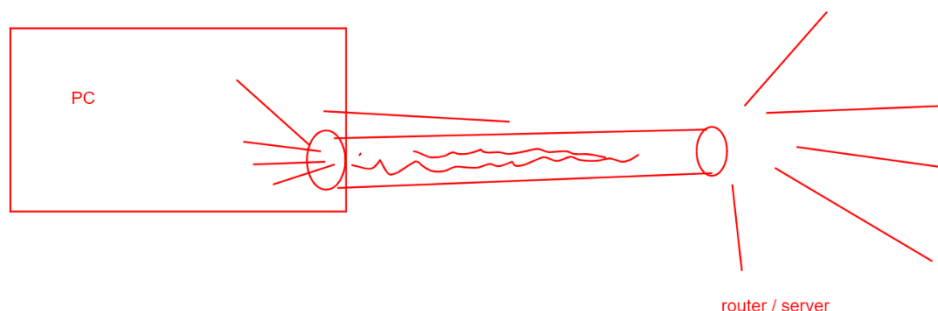


Figure 14: Drawing made by layperson 2

4.3 Perception of the current threat landscape

4.3.1 Threats

Numerous different threats were described by interviewees. Experts described threats relating to two or more categories and laypeople one to five. The category described most often is 'initial access'. Statements coded

with this category are for example relating to a threat actor getting access to a device, a threat actor connecting to office Wi-Fi, a device being stolen, or phishing.

The categories 'initial access', 'execution', 'credential access', 'collection', and 'impact' are mentioned by both groups and are present in the framework used for closed coding. Other codes from the framework that are mentioned by the experts are 'privilege escalation' and 'exfiltration'.

The statements that did not fit in any of the categories in the framework were statements that related to four different codes. The first code is 'hacking', which covers statements that describe a threat and refer to hacking, but were not specified further. The second code is 'unintentional threat', which covers statements that were not done by an adversary. Such statements are for example leaving a device somewhere or sending an e-mail to the wrong receiver. The third code is 'there are many', which relates to the recognition of the existence of many possible threats. The fourth code is 'many threats mitigated by firm', which is only mentioned by experts, and indicates that the interviewee is aware that they know that threats exist, but do not experience these threats themselves.

Expert 11 thinks he or she won't be targeted by an attack, but it can coincidentally happen that he or she is part of an attack. Furthermore, expert 2 and 11 perceive social threats to be less when working from home than working in an office. Laypeople 1 and 3 indicated that they are probably not aware of all threats.

Five threat categories from the framework were not mentioned by the interviewees. These categories are persistence, defense evasion, discovery, lateral movement, and command and control.

4.3.2 Threat actor

Experts mentioned one to six different categories of threat actors and laypeople up to four. Out of the categories, a 'cracker' was mentioned most often. Descriptions of threat actors that were coded as a cracker are for example a scriptkiddie, a rejected applicant, or a neighbor.

The threat actors 'hacktivists', 'cracker', 'state actor', and 'insider' from the threat topology of de Bruijne et al. (2017) are mentioned by both groups. Additionally, 'terrorist', 'state-sponsored network' are mentioned by experts. The threat actor 'professional criminals' from the framework of the NCSC (2019) is also mentioned by both groups.

Additionally, six codes were developed. The developed codes mentioned by both groups are 'competitor', 'clients', and the category 'there are many'. Additionally, experts mention as threat actors 'company with malicious intent' and 'social media company'. Laypeople mention an 'Internet Service Provider' as a threat actor.

Experts differ on perception whether these threat actors would target themselves or the professional services company. Experts 5, 9, and 11 indicated that they themselves would not be targeted by threat actors. Expert 5 is the only one who mentioned terrorist, and also thinks this threat actor group would not target the professional services firm. Other experts believe they are targeted by crackers, and a couple also think by professional criminals.

More divergent beliefs exist for the threat actors insiders, hacktivists, state actors, and competitors. Some experts indicate the professional services firm could be a target, but others think this is not the case.

Laypeople do not often indicate whether they think they themselves or the professional services firm would be targeted by these threat actors. Layperson 2 does mention a state actor will more probably go via judicial channels than try to hack the professional services firm.

Threat actors not named by the interviewees are 'extortionists', 'information brokers', 'crime facilitators', 'digital robbers', and 'scammers and fraudsters'.

4.3.3 Threat actor motivation

One to six different motivations were named by expert and up to four by laypeople. All motivations described could be fitted into one of the categories of the framework used. One extra code was introduced, 'there are many', to indicate when an interviewee states many different motivations exist. Two motivations were not named by both groups, namely 'accidental' and 'unpredictable'. Laypeople also did not mention 'notoriety' as a motivation.

4.3.4 Threat actor capability

Experts mention up to four different possible capabilities and laypeople up to two. The capability mentioned by most participants is 'operational skill'. Examples of statements coded as 'operational skill' include that the threat actor must have hacking skills, a broad technical education, or must be an experienced social engineer.

All descriptions for a threat actor's capability could be placed within the framework used. One threat actor capability from the closed coding framework is not mentioned by laypeople, namely 'adept skills'. Laypeople 1 and 7 remarked that the one executing the plan does not need to be the initiator.

4.3.5 Threat impact

Experts mention one to seven different types of impact and laypeople one to three. Two types of impact are mentioned most by experts. The first is 'data theft' and the second is 'reputation damage'. 'Data theft' is also the most frequent mentioned category by different laypeople.

The impact types 'disruption', 'data manipulation', 'data theft', and 'leak' come from the framework used and are mentioned by both groups. Furthermore, experts also report 'sabotage' and 'leak' as a possible impact.

Additionally, two other kinds of impact have been identified by both groups. These are 'reputation damage', and 'financial loss'. The code 'depends on access' was introduced for both groups to identify when the interviewee states the impact depends on the access of the threat actor. Furthermore, experts also identify as impact 'the incident needs to be investigated internally', 'inform affected persons', 'lawsuit', and 'notify data protection authority'.

Three types of impact from the framework were not mentioned by interviewees. These are 'espionage', 'system manipulation', and 'breakdown/failure'.

4.4 Perception of changes in the threat landscape when using a VPN

This section describes experts' and laypeople's perception of the changes in the threat landscape that occur when a VPN is used. In section 4.4.1 the perception on threat mitigated due to VPN usage are presented. In section 4.4.2 the perception on new threats that arise due to the use of VPN are outlined. And in section 4.4.3 is outlined how behavior changes to deal with the new threats.

4.4.1 Mitigation of threats due to VPN usage

According to experts and laypeople, establishing a VPN connection mitigates several threats. First, it is not possible for someone to **listen in on the data transfer**. The only ones who know what data is transferred are the sender and the receiver, and no one in the middle is able to read what is communicated. This is because the data transfer is **encrypted**:

"I assume that the data is encrypted, which in that sense simply cannot be cracked, traced back by people who are watching the connection at that moment." [Layperson 4]

According to experts, this is also a feature of the connection being **private**. Layperson 2 also thinks this is because of encryption, but is not entirely sure.

Second, using a VPN connection allows the user to **browse the web anonymously**, or according to some experts, more anonymously. Because **webtraffic is routed through the VPN server**, only the IP-address of the VPN server can be seen by the receiving entity:

“And if you use a VPN, I think that is like an extra wall in between, so my connection goes via the VPN to this external source. So, they cannot directly view what is my IP-address, among other data. I am not so sure what other data they can’t get to, but pretty sure about the IP-address part.” [Expert 9]

Laypeople are not exactly sure how the IP-address is changed. But, according to experts, routing the traffic has an additional benefit. It creates a **single point of attack** from threats via webtraffic:

“X: What do you mean by restricting channels?”

Y: Um, with your lines. So a line can be if I always let my data go through this server here, then I know that everything will enter here as well. So whether I go here to this point, go this way, go here, or go there, it always goes through this server instead of connecting directly from the client. Instead of having all those lines, thus have to catch all those threats, you now have that from a central point.” [Expert 7]

Third, if a threat actor is able to **gain access to a user’s device**, either physically or digitally, he or she is **unable to access the files**:

“Even if someone is able to steal my laptop, they will not be able to connect to the [the professional services firm] systems without the [access token provider] token, which is on my phone. Or in the case where it is a physical token, the thief will have to steal both of them to be able to access [the professional services firm] systems.” [Expert 5]

The following threats mitigated are solely described by experts. Because the VPN connection employs **filtering**, multiple threats are mitigated. The first threat mitigated is someone **accessing a malicious website**, by blocking the user from entering it:

“I think, what I have in my mind is just a whitelisting and blacklisting feature. So, if I am connected to the VPN, they can regulate what sources I visit.” [Expert 9]

The second threat mitigated by filtering is **the device getting infected with malicious software**. The filters in the VPN, being a firewall, IDS, IPS, antivirus, or just filters, can stop malicious software at or before the VPN server, to ensure it doesn’t reach the device:

“Because the VPN network of course has more security measures than I do at home, think of advanced firewall, think of analysis, the IDS and IPS, that adds to the security of my network traffic.” [Expert 11]

Additionally, the filters can deactivate the malicious part of a package, for example a malicious attachment from an e-mail, and only let the non-malicious part pass through:

“[...] this website sends back a packet data, a picture for example or a sort of data, that has a virus in it. [...] Now, within the VPN, they have the applications that should scan all coming packages for example, anti-virus, anti-ware, firewall- So, all of this is within the VPN, so the server, this computer, is equipped with all of the state-of-the-art applications that scan those packages and either remove, here, either stop this here, at this border, or for example only allow the secure part of the package and will not- So, for example you are receiving an e-mail from an unknown source, you will get the e-mail, but you will not be able to open the attachment. So, the attachment is deactivated for example.” [Expert 4]

Furthermore, the filters can block a user from completing a download, to prevent the user from downloading malicious software:

“Maybe when I am downloading something. If they don’t want me downloading a huge trojan from a shady website, then they can block the website, or they can even block the download.” [Expert 9]

Some disagreement exists among experts on the effect of a VPN on malicious software on a USB stick:

"And if I use a USB for example, a USB stick, in my device, this is a threat that the VPN is not covering. So, the VPN is only covering the risks from the Internet, as long as the VPN is activated." [Expert 4]

"Well, of course, I can plug it in myself, but for example, what files can be run, like if it has an alter executable on the USB stick, I think a VPN can play a role in that, in preventing, or at least detecting what I am doing, with the data on the USB stick." [Expert 9]

Filtering protects the user against two more threats. It protects against someone **uploading a certain unwanted file to the cloud**:

"It can also have alarming signals that someone who uploads something to [cloud software] that an IT team gets notified or something and then they can take appropriate action." [Expert 9]

The final threat mitigated due to filtering is a user **sending a certain file via an e-mail**:

"If they do configure it and go very far, like even block my [e-mail] use, that I don't send some confidential data to my private e-mail or something, it can be very secure, but also very annoying for the users." [Expert 9]

Because of these possibilities of filtering, expert 4 stated:

"The VPN is the most secure way to browse the Internet." [Expert 4]

Apart from these threats that are mitigated, the VPN connection also ensures the **software on the device is updated**:

"X: Okay. And how would the automatic updates be sent?"

Y: That should be pushed to your laptop via the admin. Probably that goes through VPN too, because as long as you don't turn on a VPN [...] no updates happen either." [Expert 2]

According to both experts and laypeople, all these measures included in the VPN connection create extra hurdles and thereby make it **more difficult for a threat actor** to successfully execute an attack. Although, experts and laypeople do note that a VPN connection **does not mitigate all computer security threats**.

4.4.2 New threats due to VPN usage

Using a VPN connection also introduces new threats. The first threat is a threat actor gaining **access to the device while the user is connected to a VPN**. This can be physically, but also digitally. An example of digital access is explained by layperson 6:

"The moment I set up a VPN connection of course and I have software on my computer, malware, that can eventually read everything or record all my key combinations, yes, then a VPN of course only has limited effect. Because people can then just read what I do." [Layperson 6]

The second threat is the current **authentication measures**. Multiple threats are identified by experts that can occur due to the current authentication measures. First, a threat actor can use a user's credentials to establish a VPN connection. Acquiring credentials can happen when for example the password is stored unencrypted or apprehended when the user enters it, the access token is stolen, or if someone were to comprehend how the access token code is constructed and able to replicate the code. Other threats related to the authentication measures identified are for example:

"[...] a VPN connection can be started from anyone who has a username and ultimately password plus key. But that also means that you can have multiple sessions per person. [...] So, yes, if you are looking for points for improvement in the current VPN, it might be a point of attention that your VPN connection

is also linked directly to your AD user. And that a standard part of your password [...] that it might be useful to change that regularly.” [Expert 7]

“[...] part of the team works with a hardware token, if that goes down, then you have no connection to the software we use.” [Layperson 5]

“It is the combination of your own password with a random number of six digits, I don't know if that at the bottom of the line, you create a lot of combination possibilities, I don't know if that is enough, or if that needs to be considered. I've also heard that you should, for example, use a double um, coding, to make it even more secure. But I don't know the details about that.

X: Yes. And what do you mean by a double coding?

Y: That you actually have to open a different VPN twice.

[...]

With those layers you build two different VPN connections. So you'd have to enter a password twice to get to the data and that would make it more secure.” [Layperson 5]

“What we use with VPNs, and in my experience that has been since it actually came into existence, codes, and you might wonder about- For example with fingerprints [...] perhaps that also makes it a bit safer.” [Layperson 1]

The third threat is solely named by laypeople and entails a threat actor **listening in on the connection**. Layperson 6 is not sure where the VPN connection starts and thinks it might be possible that someone can listen in on communication before the connection starts, for example on a user's own Wi-Fi network.

The fourth threat is closely related to the third threat and arises when **establishing a VPN when using an unsecured network**:

“X: Why are you scared to use VPN in a public space?

Y: Because I am partially aware of the kind of attacks that are possible. I do not know if someone will try to listen or look at the traffic that is going through the channel, if the Internet that I am connecting to is not secure. I do not know how, for example, the cookie and the communication logs are stored. Either way, I am not sure who the Internet Service Provider is for the café, how secure they are, what are their security measures, et cetera. So, all these things really make me worried a bit.” [Expert 5]

Layperson 1 contemplated if this threat can be ruled out by eliminating the need for Internet to make a VPN connection.

The fifth threat is the **VPN provider** itself. You need to trust the provider:

“[...] do you have confidence in your provider, where does the provider have his server, who has access to it, and that whole part of trust is very important in this. Who controls the business, who is the ultimate owner, how did they implement their internal security measures.

[...]

Well, I do trust the government itself, but I also know what they are capable of. And a VPN is not going to help with that. If they want your VPN connector or provider to give access to data, then I wonder if they would refuse. I don't even believe that.” [Expert 1]

If the professional services firm is its own provider, the employees who manage the VPN must still be trusted.

The sixth threat is when the VPN **server is compromised**, for example when someone is able to break into the server. Furthermore, experts also note that it is not known what data is monitored or even collected by the VPN server. Another threat identified by experts is the geographical location of the VPN server, since where the server is located also has implications for the security of the server.

The seventh threat identified is **hacking**:

"[...] there are still varying levels of security within that connection, because it ultimately depends on how you set it up and which protocols you use. And I know that some of the initial protocols that were used have been, you know, the encryption behind them has been broken." [Expert 3]

"I once understood that you can also establish a VPN connection, but without encryption. Yes, then that is I think less secure than when you also apply certain encryption in addition to it, and then it also depends on what kind of encryption. The more advanced your encryption, the better the security actually." [Layperson 6]

"If you know how to manipulate that [the connection], then it's probably a connection that implies a false sense of security and not something that will stop any random attacker." [Layperson 3]

"Well, just as you can break into other systems, you can probably break into a VPN tunnel. I mean, there are weaknesses everywhere, so probably also in that shell that surrounds it."

[...]

I was wondering if there is also a risk that that VPN connection, that the entire tunnel is moved, that it will go elsewhere. But eh-

X: And what do you mean it goes elsewhere?

Y: Well, that the end point changes here. In other words that it still goes via, yeah, if you know how to hijack this, then you can also maybe route the data that comes out to your own point, to your own Internet access point, and read it there." [Layperson 2]

Experts identify four more threats that are not mentioned by laypeople. The first threat is that **malicious traffic can go through the security layers** of the corporate network undetected, if the VPN server is located inside of the corporate network. Because no one other than the intended parties are able to read what data is transferred, malicious software can also pass through the security layers of the corporate network undetected.

The second threat identified solely by experts is a **malfunction**:

"I don't know how much um, powerful or how much big the servers are. So, there might be eh, if the powers goes off." [Expert 8]

The third threat is that using a VPN connection makes the user **more suspicious in the eyes of a state actor**:

"I think the NSA did that as well, that they actually were scanning for people using a VPN or you know, using their search terms to connect to a VPN and then put them on a list of people requiring more surveillance, because they felt that was by default suspicious, that someone would try and keep their web traffic and those connections private."

[...]

Of course you also see what kind of VPN service you connect to and if it of a very reputable firm, that's definitely something different than you know a guy from Minnesota that has suspicious spikes in web traffic anyway, using a custom built VPN." [Expert 3]

The fourth and final threat arises due to the **limitations of masking the IP-address**. While the user is able to browse the Internet a bit more anonymously, it is also possible to do a so-called 'ping trace':

"So it at least ensures that if you, for example, want to log in or just browsed or use the Internet, I don't know, and then they can't immediately see who you were. [...] Look how it works technically, you have of course hops, so between you and me are I think at least four hops. [...] and suppose you would look into our connection, then you see that last step. But what you can also do yourself is ping trace. That's just you following as a package. So then you can see exactly which hops are in between [...]" [Expert 1]

4.4.3 Change in human behavior to deal with new threats

When experts describe how their behavior changes to deal with new threats, they refer to threats that arise due to the authentication measures. They attempt to prevent access by other persons to their device and prevent other persons from being able to establish a VPN connection using their credentials:

"So basically, first, we do not share the same laptop. [partner] does not get to access the laptop [...] [partner] does not know the password to my system, [partner] cannot access it, [partner] doesn't have access to my phone, so [partner] cannot know the [access token provider] token ID. All this information I mean, that is something that actively I try to do. I isolate the work environment away from the partner, so that the details are only limited to me." [Expert 5]

"Yes, well, I always keep my token in my pencil case, I don't let it- I actually always have my pencil case closed, because I only take out a pen and then I close it again, so I do pay attention to that." [Expert 6]

Laypeople and other experts state that their behavior does not change due to the new threats that arise because of the use of a VPN connection. Their behavior does not change because they need to use the VPN connection in order to be able to work. Another reason provided is that they experience no control over how the VPN is set up:

"Not really, because there are some vulnerabilities that I might not be able to control, for instance where the VPN server is based, who is stealing with, like who is the service providers, there are some things, usually it is a third party. So, I don't have control over that. And it could not, could be something, for instance, also where the server is located. If it just a country where protection is not really in place, also, like, from the point of view of confidential information. [...] there are a lot of things that can happen that are outside the control of actually the user of the VPN." [Expert 8]

Layperson 7 does indicate that if he or she was aware that the connection is not protected with encryption, he or she would not send sensitive data via this connection. But it is assumed that encryption is used and thus sensitive data can be send using the VPN connection.

However, some experts do describe measures they personally take in general. For example, expert 7 and 11 state to only use the VPN connection when necessary, mostly because of capacity issues. Another example is that activities such as online banking would not be performed when connected to Internet via the corporate network. This can be via a VPN, but this is not necessarily the case. When online banking via the corporate network, personal data is visible to the corporate network and this is unwanted. The last general behavior described is using separate devices for work and private use, as described by expert 1 and 11.

5. The mental models of experts and laypeople

This section presents a framework illustrating the mental models (section 5.1) and evaluates the accuracy of these mental models (section 5.2).

5.1 Framework illustrating the mental models

Based on the results, a framework was designed that brings the mental models of experts and laypeople of VPN in a professional services firm in the Netherlands together into one. As described in section 3.5.2 Grounded Theory, a theory is “a set of well-developed concepts related through statements of relationship, which together constitute an integrated framework that can be used to explain or predict phenomena”. The statements of relationship explain *who*, *what*, *when*, *where*, *why*, *how*, and *with what consequences* an event occurs.

The framework in figure 15 explicates the perception of experts and laypeople in a professional services firm in the Netherlands of how a VPN works and the perception of the changes in the threat landscape when using a VPN. This framework can be used to explain how a VPN is used by the target group.

Indicated in framework are the theory elements known, which were determined at the outset of this research. At the center of the framework the selective code, or core category, is depicted. The framework has been divided into three core elements, namely the user element, the technology element, and the security element. Each of these elements encompass one or more concept groups, which correspond to a section in the results chapter. For these concepts groups, it is indicated which theory element they relate to, being *when*, *where*, *why*, *how*, or *with what consequences* a VPN is used. The lowest level of the framework encompasses the concepts, where a distinction has been made between concept that occur in the mental models of experts or in both groups.

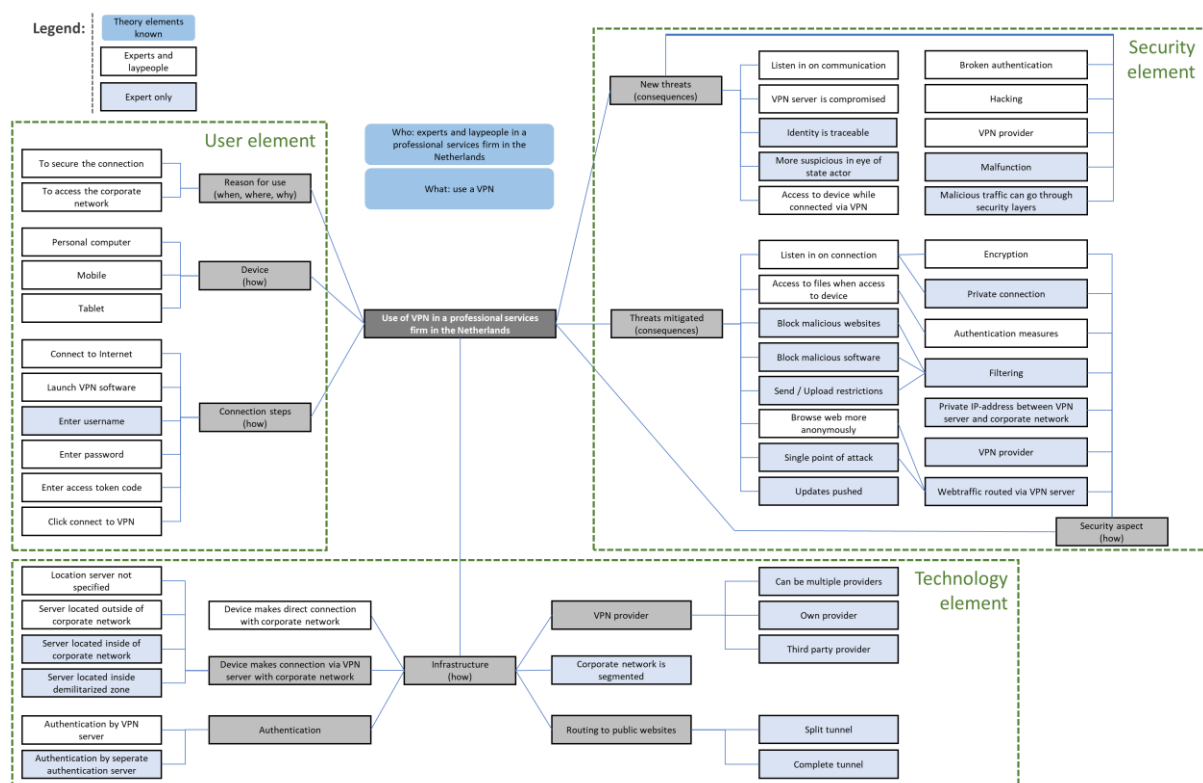


Figure 15: Framework of the mental models of experts and laypeople

5.2 Accuracy of the mental models

In this section the accuracy of the mental models is evaluated. In figure 16 the framework illustrating the mental models of experts and laypeople is depicted, including which concepts are correct and which concepts are mistaken beliefs. In this model three different color boxes are used to illustrate whether concepts are accurate. It is purposefully not stated that a concept is definitively accurate, because what concepts are accurate ultimately depends on the configuration choices made by an organization.

Because the concepts are abstractions, they do not represent all variations found in the mental models. The result is that when a concept is identified as accurate, the concept in itself is accurate, but not all variations in the mental models may be accurate.

In section 5.2.1 the accuracy of the perception of how a VPN works is evaluated, in section 5.2.2 the accuracy of the perception of the current threat landscape, and in section 5.2.3 the accuracy of the perception of changes that occur in the threat landscape when a VPN is used.

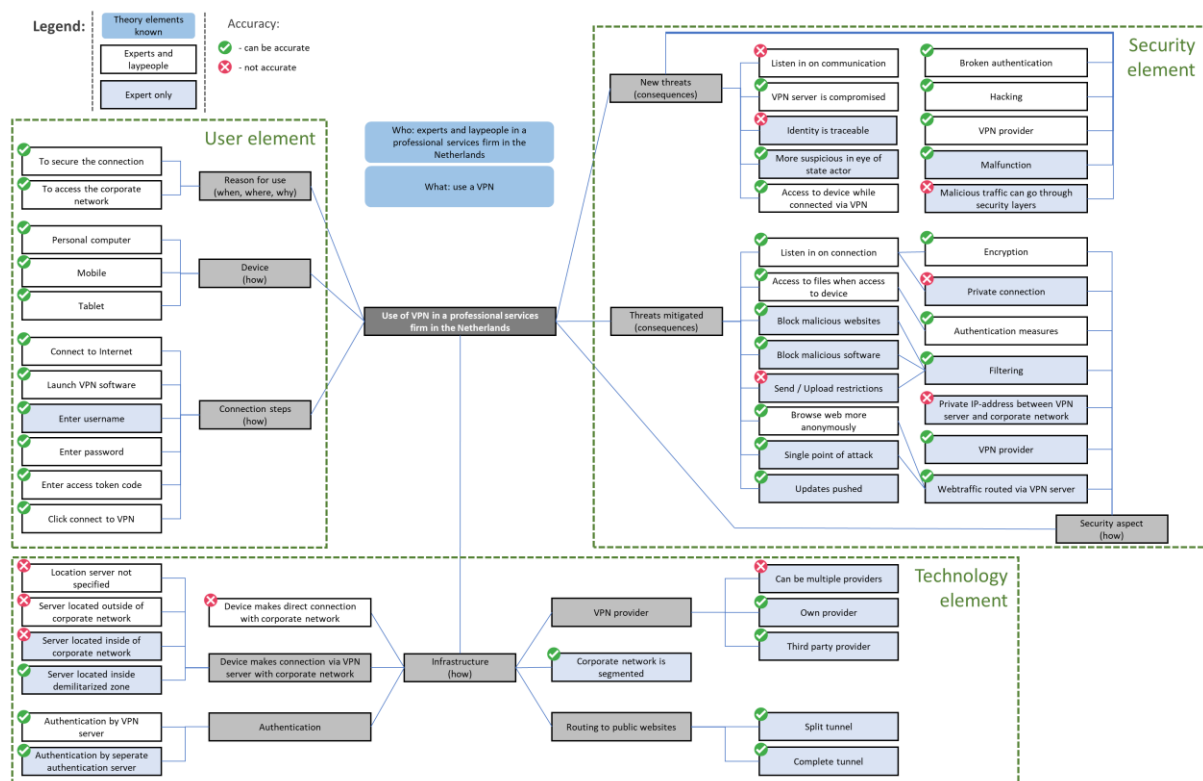


Figure 16: Framework of the mental models of experts and laypeople evaluated for accuracy

5.1.1 Accuracy perception of how a VPN works

In this section the accuracy of the perception of how a VPN works is evaluated. For the perception of how a VPN works, the focus is on the user element, the technology element, and the security aspect of the framework in figure 16.

As can be seen in the framework, all concepts identified for the user element can be accurate. This entails that none of these concepts are mistaken beliefs.

However, mistaken beliefs have been identified in the technology element and security aspect. In the technology element, five mistaken beliefs have been identified. The first four mistaken beliefs relate to how a connection is made between a device and the corporate network. As described in the real-world model, the connection is routed via a VPN server, which is located in a demilitarized zone. Strictly technical speaking, it is possible for the

VPN server to be located outside or inside the corporate network. However, because of security considerations, a VPN server will in reality not be placed outside or inside the corporate network, unless it is placed in a demilitarized zone.

The fifth mistaken belief in the technology element is that one organization can have multiple VPN providers. While strictly technical speaking this can also be true, this would be unpractical and would not be a choice adopted by organizations.

In the security element, two mistaken beliefs have been identified. The first mistaken belief is that the connection is private in the sense that the data is transferred separate from the rest of the Internet. The data is sent in a normal way over the Internet, and no private channel is created. But if the connection is encrypted, the data transferred does remain private, in the sense that no one is able to read the data aside from the ones who know the cypher.

The second mistaken belief in the security element is that an IP-address is only known between the VPN server and the corporate network. This is for the simple reason that a VPN server can also be used to connect to any public website, resulting in the IP-address of the VPN server being known by this website.

5.1.2 Accuracy perception of the current threat landscape

In this section the accuracy of the perception of the current threat landscape is evaluated. While these perceptions are not part of the developed framework, it is important to consider the accuracy of these perceptions when reflecting on the perception of changes in the threat landscape due to VPN usage. It is important to consider these perceptions, because a distorted view on the current threat landscape could result in a distorted view on the changes in the threat landscape due to VPN usage. By evaluating the accuracy of the current threat landscape, this distorted view can be either identified or ruled out.

The perception of the current threat landscape has been explored by considering five elements, namely threats in general, threat actors, a threat actor's motivation and capability, and the possible impact of a threat. Statements relating to these five elements could often be coded with a code from the closed coding frameworks. This indicates that the interviewees do not mention very surprising categories. Additionally, the new codes developed also can be seen as realistic.

To evaluate the accuracy of the perceptions of the current threat landscape, the answers were compared with the Cyber Security Assessment Netherlands (NCSC, 2019). Specifically the results for threats, threat actors, and threat impact were compared with the threat matrix in the Cyber Security Assessment.

According to the assessment, a threat actor to a private entity can be a professional criminal, cracker, insider, hacker, state actor, or state-sponsored network. A terrorist would not form a threat to a private entity. Comparing with the perceptions of interviewees some similarities, but also differences, can be identified. The differences relate to divergent beliefs among the experts on threat actors.

Comparing the threats and possible impacts, the difference between the assessment and perceptions are smaller. The similarities are that according to the assessment for a private entity and the interviewees a disruption, data manipulation, data theft, and leak is a real possibility.

On the other hand, the risk for sabotage is not identified in the assessment, but is identified by one expert. Moreover, laypeople did not identify a leak as a possible risk, but they do mention an unintentional threat as a risk, which has roughly the same meaning.

Some possible impacts were identified by the assessment, but not by the interviewees. Both experts and laypeople did not identify espionage, system manipulation, and breakdown/failure as a risk. It can be that they do not perceive this as a risk or it did not come to their minds during the interviews. One additional explanation

is the separation of the questions in the interview design. For example, the definition of espionage is ‘impairment of the confidentiality of information by means of the copying or removal of data by nation-state actors or nation-state-affiliated actors’. Because in the interview design the questions relating to threat, threat actors and possible impact were asked separately, it was not mentioned that a state actor, or state-sponsored network was responsible for data theft. However, they were identified separately.

To conclude, the perception of experts and laypeople in this sample of the current threat landscape is not completely accurate, but it can be seen as accurate enough to conclude that these interviewees do not have a distorted view on the current threat landscape. Because of this reason, the perception of the current threat landscape is deemed as accurate enough to reflect on the perception of changes in the current threat landscape, and rule out a distorted world view on the current threat landscape to be the cause of a potentially distorted view on the changes in the threat landscape due to VPN usage.

5.1.3 Accuracy perception of changes in the threat landscape when using a VPN

In this section the accuracy of the perception of changes in the threat landscape that occur when a VPN is used is evaluated. For the perception of changes in the threat landscape, the focus is on the concept groups threats mitigated and new threats, located in the security element of the framework in figure 16.

The concept group “Threats mitigated” consists of eight concepts, of which one has been identified as a mistaken belief. The concept ‘Send / Upload restrictions’ has been identified as a mistaken belief, because a VPN connection will not prevent a user from uploading malicious software or sending malicious software via an e-mail.

The concept group “New threats” consists of ten concepts, of which two are mistaken beliefs, and one has been identified as partially correct. The first mistaken belief is that a user’s identity is traceable when a VPN is used. This concept was introduced by expert 1, who believes that it is possible to do a ‘ping trace’ to trace a user’s IP-address. This is a mistaken belief, because it is only possible to trace the IP-address provided by the VPN server.

The second mistaken belief is that malicious traffic can go through security layers. This concept was introduced in relation to the VPN server being located inside the corporate network. As explained in the real-world model, the VPN connection passes through two firewalls. If malicious traffic is sent via the VPN connection, it is able to pass through the first firewall, because the webtraffic is encrypted. However, the malicious traffic will not be able to pass through the second firewall and enter the corporate network. Because the malicious traffic would not be able to pass through both firewalls, this concept has been identified as a mistaken belief.

The third and final mistaken belief is that a threat actor can listen in on communication send via the VPN connection. This concept entails two variations. The first variation is that someone would be able to listen in on webtraffic before the connection point starts, for which the example provided is on a user’s own Wi-Fi network. The second variation is the essentially the same problem, but in a different setting, where a connection is made via an unsecured network. This concept is a mistaken belief, because webtraffic would be encrypted at the user’s device, and thus not be readable when send over a user’s own Wi-Fi network or over an unsecured network.

6. Discussion and Conclusion

This section discusses the similarities and differences between the mental models (6.1), the scientific and societal implications (section 6.2), the limitations of the study (section 6.3), further research possibilities (section 6.4), and the embedding in the CoSEM curriculum, I&C track, and cybersecurity specialization (section 6.5).

6.1 Similarities and differences between the mental models

This section combines the results of the interviews, the framework of the mental models, and the accuracy of the mental models to answer the main research question of this study. The main research question is *“what are the similarities and differences between the mental models of experts and laypeople of VPN in a professional services firm in the Netherlands?”*.

6.1.1 Answers to the subquestions

Subquestions were formulated to answer the main research question. The subquestions comprised experts' and laypeople's perceptions of how a VPN works and their perception of the changes in the threat landscape when a VPN is used.

The results on experts' and laypeople's perceptions of how a VPN works show that a VPN is used to access the corporate network and to secure the connection. Second, the results present that a personal computer, mobile, and tablet are used to establish a VPN connection, however some confusion exists on whether their mobile phone makes a VPN connection. Third, the results show the six steps a user makes to establish a connection. Fourth, the results display what the infrastructure of a VPN looks like according to experts and laypeople, including the basic configuration, the VPN provider, network segmentation, a split or complete tunnel, the seven possibilities of the meaning of a secured connection, and the metaphors used to describe the infrastructure.

The results on experts' and laypeople's perceptions the changes in the threat landscape when a VPN is used describe the perception of what threats are mitigated and relate these to the seven possibilities of the meaning of a secured connection. Second, the results present the perception of new threats that arise due to the use of VPN. Third and final, the results reveal which changes occur in the target's group behavior to deal with these new threats. The results indicate that access to the device or credentials by other persons is prevented, but no other measures are taken to deal with new threats. No other measures are taken because they interviewees do not experience control over how the VPN is set up and because they need to use the VPN in order to work.

These results have been combined to design a framework that illustrates the mental models of experts and laypeople of VPN in a professional services firm in the Netherlands. The concepts in the framework explain *when, where, why, how, or with what consequences* a VPN is used. The accuracy of this framework has been evaluated, by comparing it with a real-world model of a VPN.

6.1.2 Answer to the main research question

Next, the results of the interviews, the framework illustrating the mental models, illustrated in figure 16, and the accuracy of the mental models are used to describe the similarities and differences between the mental models of experts and laypeople of VPN in a professional services firm in the Netherlands.

To start, the first similarity is that both experts and laypeople knew what a VPN was. None of the interviewees drew a blank when asked what a VPN is.

In the user element many similarities can be identified. Just one concept is only named by experts, namely enter username. An explanation for this could be that laypeople just forgot to mention it, or that experts did mention it, but they actually did not need to enter the username themselves.

In the technology element more differences can be identified. The concepts named by both experts and laypeople concern the more simplistic infrastructure configurations and straightforward authentication. The differences relate to more elaborate configurations and additional specifications such as the VPN provider, segmentation of the network, and a split or complete tunnel. Since almost all concepts named by only experts are also accurate, this indicates a less complete mental model for laypeople than experts on the technology element.

In the security element more differences can also be found in inaccurate concepts. These inaccurate concepts can be found in all three concept groups in the security element: the security aspect, the threats mitigated, and the new threats. Interesting to notice is that the inaccurate concepts in the security aspect group do not relate to additional inaccurate threats mitigated. The one inaccurate threat mitigated comes forth from an accurate concept, namely filtering. Another interesting fact to notice is that all inaccurate concepts in the groups security aspect and threats mitigated are named by only experts. On the other hand, experts do also name more accurate concepts than laypeople.

How the connection is secured in reality, and therefore what threats are mitigated, depends on the network configuration of the professional services firm and could be limited by the use of a split VPN. In what malicious software is protected against, some mistaken beliefs have been identified. This mistaken belief and the accurate perceptions that might not be in place in reality, depending on the network configuration, could result in an important consequence. This consequence can be that people think they are safer than they actually are, and therefore are either less watchful for threats or take more risks than they would otherwise. Since the mistaken belief is only mentioned by experts, and the other, more complicated, but accurate perceptions are only mentioned by experts as well, it can be expected that mainly experts in this target group overestimate the security of a VPN.

On the other hand, the inaccurate threats identified indicate a different result. In the group new threats, two inaccurate threats are identified by only experts and one inaccurate threat is identified by both groups. The two inaccurate threats identified by only experts, being that the user's identity is traceable and that malicious traffic can go through security layers, could actually result in an underestimation of the security of a VPN and to more secure behavior than necessary. The inaccurate threat identified by both groups, listen in on communication, results in a more tangible, unnecessary risk or precaution. Because some experts and laypeople think a VPN does not protect against someone listening in on the communication, it was identified that they would sometimes choose to not establish a VPN connection when they use an unsecured network. Experts indicated they would use a mobile network instead as a precaution, which is a good solution, but laypeople did not mention this. The result of this inaccurate perceived threat could be that an unsecured network is used, but without creating a VPN connection. Since this would create a threat, this would ultimately result in an unnecessary risk due to a mistaken belief.

To conclude, many similarities, but also important differences exist between the mental models of experts and laypeople. The perceptions of both groups contain accurate and mistaken beliefs. The mistaken beliefs could result in more or less secure behavior than necessary in reality, and therefore create unnecessary precautions and risks.

6.1.3 Comparison of the results to related work

First, differences between the perception of experts and laypeople have been identified and mistaken beliefs are present in the mental models of both groups. This results was also found by research on the perception of

experts and laypeople of the Tor anonymity system (Gallagher et al., 2017), Internet (Kang et al., 2015), and HTTPS (Krombholz et al., 2019).

Second, laypeople did not name any new concepts when compared with experts, as far as known, this result has not been found in previous research. However, results from other research have shown that laypeople name only less important operations aspects than experts (Gallagher et al., 2017).

Third, both groups use metaphors to convey their perceptions. This result has been found in related work as well. For example, in Gallagher et al. (2017) the Tor anonymity system is compared with a faucet, Fort Knox, and the Statue of Liberty. Furthermore, in Wash (2010), who researched laypeople's perception of viruses, malware, and hackers, metaphors were used to describe how a hacker works. For example, it is described that a hacker would search in a computer like a thief would in an attic or that a thief would take a digital picture of files on a computer and search through that picture.

Fourth, the results indicate that both experts and laypeople underestimate the risks. When aware of the risks, interviewees state to use a VPN on an unsecured network. This is not necessarily the case when using a mobile network. A reason provided for this is they do not think it is necessary. It is possible that the interviewee's underestimate their own risks. This can also be identified in the perception current threat landscape, where experts describe frequently that they do not think the professional services firm is targeted by a threat actor, or they themselves would not be targeted. Similar indications have been found in literature (Furman et al., 2012), and a recent research by the Dutch government concludes that risks are underestimated (Ministry of Economic Affairs and Climate Policy, 2020).

6.2 Scientific and societal implications

6.2.1 Scientific implications

This study contributes new academic insights in a field that is young and developing. This study addresses two knowledge gaps. The first knowledge gap is the lack of a clear, established method to capture and elicit mental models. This knowledge gap is partly addressed by performing a limited review of methods used to explicate mental models. Based on this review, semi-structured interviews were combined with a three part scenario-based drawing task in this study.

Because the interview design offered the possibility share detailed descriptions, ask for clarifications and in-depth questions, to identify mistaken beliefs, minimized cross-influence from other interviewees, and perform the interview in a consistent manner due to the semi-structured protocol, it is recommended to researchers to use the same or a similar method that encompasses these features.

The drawing task design offered more in-depth results and a visualization and verification of the mental models provided in the interviews. The drawing task and the whiteboard in the conferencing platform used offered freedom in the way of expression, and was used extensively by most interviewees. Thinking aloud with a concurrent verbal report provided rich verbal data and the scenario's used allowed to explore the mental models exhaustively. Because of these reasons, it is recommended to researcher, who perform similar research, to use a similar method as additional elicitation technique. But this technique will not be suitable for all mental models studies, as it depends on the specifications of the research which elicitation technique is suitable to use.

The second addressed knowledge gap is that limited research has been done on the mental models of different cyber mechanisms. This is the first study of perceptions and practices regarding VPN and therefore this knowledge gap has been addressed.

The professional services firm selected is representative for other multinational professional services firms. Therefore, it is expected that the results found in this research will be applicable to similar firms as well. By

studying both expert and laypeople perceptions, it was possible to explicate perceptions of both groups and differences between the groups. Mistaken beliefs in these perceptions have been identified and the consequences of these mistaken beliefs on behavior and its possible implications are described.

6.2.2 Societal implications

This study contributes to the design of more effective and efficient risk communication. Based on the mental models identified and the corresponding beliefs, it can be determined what message should be conveyed to the audience. Ultimately, this designed message can help people to become more resilient and able to act in a secure manner when interacting with IT systems.

Research of the Dutch NCSC (2019) shows that one out of nine persons were victim of cybercrime in 2017. Research on the effectivity of awareness campaigns on a user's security behavior is currently very important (NCSC 2019), and the creation of cyber situation awareness is one the three key challenges to reach adequate cybersecurity levels (Van den Berg, 2019). When cyber risk communication is designed, it is of importance to consider the information needs and the diversity of these needs among the audience (Stewart & Lacey, 2012). Risk communication should focus on what people need to know and the mental model approach can help to design this (Fischhoff, 1995). Mental models are thought to be a valuable source of information to design cyber risk communication, because the use of mental models has been very successful in other fields (Nurse et al., 2011). These fields are for example environmental (Camp, 2009; Morgan et al., 2002), health (Morgan et al., 2002), and drug risks (Camp, 2009). Additionally, more and more research indicates that people use mental models to understand, evaluate, and act on risks (Jones et al., 2011).

Moreover, cybercrime is increasing in both its sophistication and the size of potential targets (Europol & EC3, 2019). Research has shown that 59% of surveyed organizations have had either significant or material breach in 2019 (EY, 2020). Therefore, it is crucial to research cyber risk perception in organizations to be able to design effective and efficient cyber risk communication for employees in these organizations.

The professional services firm in this research, like similar other professional services firms, handles highly confidential and personally identifiable information. Effective risk communication aids in protecting the confidentiality, integrity, and availability of this information. Therefore, this research aids in securing this and similar firms, but most importantly this research aids in protecting the society, by indirectly protecting many people that could be implicated in an undesirable event.

Furthermore, mental models of VPN are an important topic to research because this mechanism offers people the capability to protect themselves against certain threats. Since users decide when and where they choose to establish a VPN connection, their behavior can have important consequences. This research can help people to cope with threats and increase their self-efficacy. Research has found coping/self-efficacy as a reliable, moderately strong predictor for cybersecurity intention and behavior, which indicates that interventions should focus on improving a user's ability to respond to cyber threats appropriately rather than simply stressing the threat (ENISA, 2018).

The results of this study contribute to the design of cyber risk communication in three ways. First, the results show what language is used by the audience and what certain terms mean to different persons in the audience. These results can be used to adjust the language in the communication to accommodate the information needs of the audience.

Second, the identified mistaken beliefs in the mental models can be used to improve the clarity of the message to the audience. Mistaken beliefs can cause confusion among the audience and the communication message to be understood incorrectly by the audience, because in their mental model something works in a different way than what's being told to them. The results of this study can help to adjust the communication to improve the clarity of the message to the audience.

Third and final, the mistaken beliefs can be used to focus the communication on what the audience needs to know, instead of repeating what the audience already knows. Additionally, by taking into account the results on when, where, and why a VPN is used and what changes in the behavior occur due to new threats that arise because a VPN is used, the risk communication message can be adjusted to maximize the impact on the resulting behavior.

6.3 Limitations of the study

While there is a general consensus on reliability, replicability, and validity as important quality criteria in quantitative research, there is no consensus on quality criteria in qualitative research (Barbour, 2014; Bryman, 2012). For this reason the limitations of this research are discussed in general rather than based on quality criteria.

First, generalizability is limited due to the research approach used. A qualitative approach is used, therefore the frequency distribution of perceptions is not necessarily representative for the population. This research focused which beliefs occur in the research population, but not how often these occur.

Generalizability is also limited because a case study is used. The beliefs among experts and laypeople in one professional services firm have been outlined. Factors such as company culture or national culture may influence the mental models of the population, resulting in different mental models in different firms or countries.

Second, the interviewing method and drawing can limit the quality of the results. The wording of the questions may introduce bias among interviewees. This has been minimized by using neutral formulations in the questions and by testing the interview protocol in pilot interviews. Additionally, most interviewees chose not to enable video during the interview. Therefore, the interviewer was unable to anticipate on the facial expressions or body language of the interviewee. But, the interviewee was also not influenced by the facial expressions or body language of the interviewer. Furthermore, because the drawings were made with limited tools online, this limits flexibility in the drawing.

Third, the participants were not familiar with the conferencing software used. Because of this reason, not all participants were able to participate in the interview using their personal computer and therefore two participants (laypeople 3 and 4) were not able to draw. Also, because participants were not familiar with the environment, they had to figure out how to use the drawing tools. This was mainly an issue in the beginning of the drawing exercise, as participants became familiar with the available tools during the interview. Before the interview, participants were given the opportunity to enter an 'exploration room', in order to become familiar with the environment. Also, a short overview of the possibilities of the drawing tools was provided before each interview started.

Fourth, interviewees could have not described their complete mental model or could have on purpose rigged the results. Also, self-reported behavior does not always correlate with actual behavior (Wash et al., 2017). Because of limited memory and recall, a lack of motivation, or participant fatigue, the interviewees could have report less than they actually know. To elicit as much information as possible and to try to prevent participant fatigue, a drawing exercise was used. Because participants volunteered to participate, they were motivated at least at the beginning of the interview. No indication exists that an interviewee deliberately told less than they know or something else than they actually thought.

Fifth, the interviewer is not an experienced interviewer or coder. With the use of the semi-structure interview protocol and neutral continuation prompts, it was attempted to prevent asking more than one question at a time or to ask leading questions. Furthermore, the manner of coding may influence the quality of the results. To ensure this quality, the theory was validated by revisiting the original data. To ensure the reliability of the codebook, partial double coding was performed by a second researcher and the inter coder agreement was reviewed.

6.4 Further research possibilities

Based on the performed research, its implications, and the addressed limitations, recommendations for future research can be formulated.

First, the completeness of the described mental models can be researched. This study researched the mental models of experts and laypeople, evaluated the accuracy of these mental models, and discussed possible implications. The real-world model developed to evaluate the accuracy was not a complete model of VPN and therefore knowledge gaps in the mental models of the target group have not been identified. Further research can therefore develop a complete real-world model, to evaluate on the completeness of the mental models resulting from this study.

Second, the generalizability of the identified beliefs can be researched. The generalizability of the results are limited due to the use of a case study approach. The results of this research explicates what beliefs occur in the target group. Further research can repeat this study design in another professional services firm, in another organization, or in yet another population, in order to determine if the results are generalizable to similar or other populations.

Third, the prevalence of the identified beliefs can be researched. The generalizability of the results are also limited due to the use of a qualitative study approach. Because a qualitative approach is used, the frequency distribution of the identified beliefs is not necessarily representative for the population. It is important to know this frequency distribution when risk communication is designed, to be able to focus the communication on frequently occurring beliefs, so the message has as much effect as possible. Therefore, further research can use the results of this study to determine the prevalence of the identified beliefs among similar or different populations.

And finally, the mental models can already be used to design risk communication in a more effective and efficient manner by considering the identified beliefs.

6.5 Embedding in CoSEM curriculum, I&C track, and cybersecurity specialization

This thesis is written as partial fulfillment of the Master's degree programme Complex Systems Engineering and Management (CoSEM) at the faculty Technology, Policy and Management at Delft University of Technology. The research objective of this thesis is related with the objectives of the Complex Systems Engineering and Management programme.

The objective of this research was *substantive theory development* on the similarities and differences between the mental models of experts and laypeople of VPN in a professional services firm in the Netherlands. The outcome of this research can be used to design effective and efficient risk communication and therefore has a *design component* and *aims at an effective intervention* in human security behavior. This research *uses CoSEM methods and tools* and is *multi-disciplinary* by using a *systems engineering approach* and a social research method, interviewing, to map the mental models of a *socio-technical system*, VPN and its social and digital threat environment. This research has a *systematic and methodological approach*, by iteratively performing interviewing, transcribing, and coding, and by systematically analyzing the data using Grounded Theory. The methods have been developed in a *creative way*, which was necessary because there is no general agreement among researchers on a method to capture mental models, on elicitation techniques, or on what method to use to analyze the data. And finally, because this research aids in securing a private firm and aids in protecting the society, this research covers *values originating from both the private and public domain*.

This research fits with the Information and Communication (I&C) track due to the subject of the mental models research being VPN, which is an information and communications technology application. The I&C track has provided the researcher with the necessary knowledge to be able to understand this application. The

cybersecurity specialization has provided the necessary knowledge to be able to understand the social and digital threat environment surrounding this application.

Reference list

- Abdi, N., Such, J. M., & Ramokapane, K. M. (2019). More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. *Proceedings of the 15th Symposium on Usable Privacy and Security*, 451–466. www.usenix.org/conference/soups2019/presentation/abdi
- Abu-Salma, R., Redmiles, E. M., Ur, B., & Wei, M. (2018). Exploring User Mental Models of End-to-End Encrypted Communication Tools. *Proceedings of the 8th USENIX Workshop on Free and Open Communications on the Internet*. <https://www.usenix.org/conference/foci18/presentation/abu-salma>
- Abu-Salma, R., Sasse, M. A., Bonneau, J., Danilova, A., Naiakshina, A., & Smith, M. (2017). Obstacles to the Adoption of Secure Communication Tools. *Proceedings of the IEEE Symposium on Security and Privacy*, 137–153. <https://doi.org/10.1109/SP.2017.65>
- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211. [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T)
- Al Sabbagh, B., & Kowalski, S. (2012). Developing Social Metrics for Security Modeling in the Security Culture of IT Workers Individuals (Case Study). *Proceedings of the 5th International Conference on Communications, Computers and Applications*, 112–118. <https://ieeexplore.ieee.org/abstract/document/6516793/>
- Asgharpour, F., Liu, D., & Camp, L. J. (2007). Mental Models of Security Risks. In S. Dietrich & R. Dhamija (Eds.), *Financial Cryptography and Data Security* (pp. 367–377). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-77366-5_34
- ATLAS.ti Scientific Software Development GmbH. (n.d.). *ATLAS.ti*. Retrieved April 22, 2020, from <https://atlasti.com/>
- ATLAS.ti Scientific Software Development GmbH. (2019). *Inter-Coder Agreement Analysis: ATLAS.ti 8 Windows*. http://downloads.atlasti.com/docs/ICA_a8_win_en.pdf
- Barbour, R. S. (2014). Quality of Data Analysis. In U. Flick (Ed.), *The SAGE Handbook of Qualitative Data Analysis* (pp. 496–510). SAGE Publications.
- BigBlueButton. (n.d.). *BigBlueButton*. Retrieved May 18, 2020, from <https://bigbluebutton.org/>
- Blythe, J., & Camp, L. J. (2012). Implementing mental models. *Proceedings of the IEEE Symposium on Security and Privacy Workshops*, 86–90. <https://doi.org/10.1109/SPW.2012.31>
- Bravo-Lillo, C., Cranor, L. F., Downs, J., & Komanduri, S. (2011). Bridging the gap in computer security warnings: A mental model approach. *IEEE Security and Privacy*, 9(2), 18–26. <https://doi.org/10.1109/MSP.2010.198>
- Brewer, D. D. (2002). Supplementary Interviewing Techniques to Maximize Output in Free Listing Tasks. *Field Methods*, 14(1), 108–118. <https://doi.org/10.1177/1525822X02014001007>
- Bryman, A. (2012). *Social Research Methods* (4th ed.). Oxford University Press Inc.
- Buitron de la Vega, P., Coe, C., Paasche-Orlow, M. K., Clark, J. A., Waite, K., Sanchez, M. J., Armstrong, E., & Bokhour, B. G. (2018). “It’s like a mirror image of my illness”: Exploring Patient Perceptions About Illness Using Health Mind Mapping—a Qualitative Study. *Journal of General Internal Medicine*, 33(10), 1692–1699. <https://doi.org/10.1007/s11606-018-4557-9>
- Byrd, T. A., Cossick, K. L., & Zmud, R. W. (1992). A synthesis of research on requirements analysis and knowledge acquisition techniques. *MIS Quarterly: Management Information Systems*, 16(1), 117–138. <https://doi.org/10.2307/249704>
- Cambridge University Press. (n.d.). *Cambridge Dictionary*. Retrieved September 21, 2020, from <https://dictionary.cambridge.org/>
- Camp, L. J. (2009). Mental Models of Privacy and Security. *IEEE Technology and Society Magazine*, 28(3), 37–46. <https://doi.org/10.1109/MTS.2009.934142>
- Casey, Tim. (2015). *Understanding Cyberthreat Motivations to Improve Defense*.

- <https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/understanding-cyberthreat-motivations-to-improve-defense-paper.pdf>
- Casey, Timothy. (2007). *Threat Agent Library Helps Identify Information Security Risks*.
https://www.researchgate.net/publication/324091298_Threat_Agent_Library_Helps_Identify_Information_Security_Risks
- Choong, Y.-Y., Theofanos, M. F., Renaud, K., & Prior, S. (2019). "Passwords protect my stuff"—a study of children's password practices. *Journal of Cybersecurity*, 5(1). <https://doi.org/10.1093/cybsec/tyz015>
- Conrad, L. Y., & Tucker, V. M. (2019). Making it tangible: hybrid card sorting within qualitative interviews. *Journal of Documentation*, 75(2), 397–416. <https://doi.org/10.1108/JD-06-2018-0091>
- Corbin, J., & Strauss, A. (1990). Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative Sociology*, 13(1). <https://doi.org/10.1007/BF00988593>
- Corbin, J., & Strauss, A. (2008). Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory. In *Basics of Qualitative Research (3rd ed.): Techniques and Procedures for Developing Grounded Theory* (3rd ed.). SAGE Publications, Inc. <https://doi.org/10.4135/9781452230153>
- de Bruijne, M., van Eeten, M., Gañán, C., & Pieters, W. (2017). *Towards a new cyber threat actor typology*.
<https://www.wodc.nl/onderzoeksdatabase/2740-categoriseren-en-motieven-cyberactoren.aspx>
- Deline, S., Guillet, L., Rauffet, P., & Guérin, C. (2019). Team cognition in a cyber defense context: focus on social support behaviors. *Cognition, Technology & Work*. <https://doi.org/10.1007/s10111-019-00614-y>
- Dietrich, C., Krombholz, K., Borgolte, K., & Fiebig, T. (2018). Investigating system operators' perspective on security misconfigurations. *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, 18, 1272–1289. <https://doi.org/10.1145/3243734.3243794>
- European Union Agency for Network and Information Security. (2016). *Definition of Cybersecurity*.
<https://doi.org/10.2824/4069>
- European Union Agency for Network and Information Security. (2018). *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*. <https://doi.org/10.2824/324042>
- Europol & EC3. (2019). *Internet Organised Crime Threat Assessment 2019*.
<https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019>
- EY. (2020). *EY Global Information Security Survey 2020*.
[https://www.ey.com/Publication/vwLUAssets/2020_GISS_pdf/\\$FILE/ey-global-information-security-survey-2020-report.pdf](https://www.ey.com/Publication/vwLUAssets/2020_GISS_pdf/$FILE/ey-global-information-security-survey-2020-report.pdf)
- Fischhoff, B. (1995). Risk Perception and Communication Unplugged: Twenty Years of Process. *Risk Analysis*, 15(2), 137–145. <https://doi.org/10.1111/j.1539-6924.1995.tb00308.x>
- Fischhoff, B. (2013). Risk perception and communication. In *Risk Analysis and Human Behavior* (1st ed., pp. 3–33). Routledge. <https://doi.org/10.4324/9780203140710>
- Fischhoff, B., & Kadavy, J. (2011). *Risk: A Very Short Introduction*. Oxford University Press.
- Fogg, B. (2009). A behavior model for persuasive design. *Proceedings of the 4th International Conference on Persuasive Technology*, 1–7. <https://doi.org/10.1145/1541948.1541999>
- Fonteyn, M. E., Kuipers, B., & Grobe, S. J. (1993). A Description of Think Aloud Method and Protocol Analysis. *Qualitative Health Research*, 3(4), 430–441. <https://doi.org/10.1177/104973239300300403>
- Furman, S., Theofanos, M. F., Choong, Y.-Y., & Stanton, B. (2012). Basing Cybersecurity Training on User Perceptions. *IEEE Security & Privacy Magazine*, 10(2), 40–49. <https://doi.org/10.1109/MSP.2011.180>
- Gallagher, K., Patil, S., & Memon, N. (2017). New Me: Understanding Expert and Non-Expert Perceptions and Usage of the Tor Anonymity Network. In *Proceedings of the 13th Symposium on Usable Privacy and*

- Security. <https://www.usenix.org/conference/soups2017/technical-sessions/presentation/gallagher>
- Garg, V., Lorenzen-Huber, L., Camp, L. J., & Connelly, K. (2012, June 29). Risk Communication Design for Older Adults. *Proceedings of the 29th International Symposium of Automation and Robotics in Construction*. <https://doi.org/10.22260/ISARC2012/0030>
- Greyson, D., O'Brien, H., & Shoveller, J. (2017). Information world mapping: A participatory arts-based elicitation method for information behavior interviews. *Library & Information Science Research*, 39(2), 149–157. <https://doi.org/10.1016/j.lisr.2017.03.003>
- Happa, J., & Fairclough, G. (2017). A Model to Facilitate Discussions About Cyber Attacks. In M. Taddeo & L. Glorioso (Eds.), *Ethics and Policies for Cyber Operations* (pp. 169–185). Springer International Publishing. https://doi.org/10.1007/978-3-319-45300-2_10
- International Organization for Standardization. (2009). *ISO/Guide 73:2009*. <https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en>
- International Organization for Standardization. (2012). *ISO/IEC 27032:2012*. <https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en>
- International Organization for Standardization. (2018a). *Information security management systems - Overview and vocabulary (ISO/IEC 27000:2018)*. <https://www.iso.org/standard/73906.html>
- International Organization for Standardization. (2018b). *ISO 3100:2018*. <https://www.iso.org/obp/ui/#iso:std:iso:3100:ed-2:v1:en:term:3.1>
- Johnson-Laird, P. (1986). *Mental models: Towards a cognitive science of language, inference and consciousness*. Harvard University Press.
- Jones, N. A., Ross, H., Lynam, T., Perez, P., & Leitch, A. (2011). Mental models: An interdisciplinary synthesis of theory and methods. *Ecology and Society*, 16(1). <https://doi.org/10.5751/ES-03802-160146>
- Kang, R., Dabbsih, L., Fruchter, N., & Kiesler, S. (2015). “My Data Just Goes Everywhere:” User Mental Models of the Internet and Implications for Privacy and Security. *Proceedings of the Eleventh Symposium On Usable Privacy and Security*, 39–52. <https://www.usenix.org/conference/soups2015/proceedings/presentation/kang>
- Krippendorff, K. (n.d.). *ATLAS.ti manual appendix: Inter-Coder Agreement in ATLAS.ti*. https://downloads.atlasti.com/docs/ICA_Appendix.pdf?_ga=2.154971064.1688372037.1574613096-50067560.1570971353
- Krippendorff, K. (2004). *Content Analysis: An Introduction to Its Methodology* (2nd ed.). Sage Publications, Inc.
- Krombholz, K., Busse, K., Pfeffer, K., Smith, M., & von Zezschwitz, E. (2019). “If HTTPS Were Secure, I Wouldn’t Need 2FA” - End User and Administrator Mental Models of HTTPS. *Proceedings of the IEEE Symposium on Security and Privacy*, 1138–1155. <https://doi.org/10.1109/sp.2019.00060>
- Langan-Fox, J., Code, S., & Langfield-Smith, K. (2000). Team mental models: Techniques, methods, and analytic approaches. *Human Factors*, 42(2), 242–271. <https://doi.org/10.1518/001872000779656534>
- Maier, J., Padmos, A., Bargh, M. S., & Wörndl, W. (2017). Influence of mental models on the design of cyber security dashboards. *Proceedings of the 12th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications*, 3, 128–139. <https://doi.org/10.5220/0006170901280139>
- Märki, H., Maas, M., Kauer-Franz, M., & Oberle, M. (2016). Increasing software security by using mental models. In D. Nicholson (Ed.), *Advances in Intelligent Systems and Computing* (pp. 347–359). Springer, Cham. https://doi.org/10.1007/978-3-319-41932-9_29
- Mavroeidis, V., & Bromander, S. (2017). Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. *Proceedings of the 2017 European Intelligence and Security Informatics Conference, 2017-January*, 91–98. <https://doi.org/10.1109/EISIC.2017.20>

- Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative Data Analysis: A Methods Sourcebook* (3rd ed.). SAGE Publications, Inc.
- Ministry of Economic Affairs and Climate Policy. (2020). *Veilig Online 2020*.
<https://www.rijksoverheid.nl/ministeries/ministerie-van-economische-zaken-en-klimaat/documenten/rapporten/2020/09/30/veilig-online-2020>
- MITRE ATT&CK. (n.d.). *Enterprise Tactics*. Retrieved September 11, 2020, from
<https://attack.mitre.org/tactics/enterprise/>
- Morgan, M. G., Fischhoff, B., Bostrom, A., & Atman, C. J. (2002). *Risk Communication: A Mental Models Approach*. Cambridge University Press.
- National Coordinator for Security and Counterterrorism. (2019). *Nederlandse Cybersecurity Agenda*.
<https://www.nctv.nl/onderwerpen/ncsa/documenten/publicaties/2018/04/21/nederlandse-cybersecurity-agenda>
- National Cyber Security Centre. (2019). *Cyber Security Assessment Netherlands 2019*.
<https://english.ncsc.nl/topics/cybersecurity-assessment-netherlands/documents/publications/2019/09/13/cyber-security-assessment-netherlands-2019>
- National Institute of Standards and Technology. (2012). *SP 800-30 Rev. 1 Guide for Conducting Risk Assessments*. <https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final>
- NCH Software. (n.d.). *Express Scribe Transcription Software*. Retrieved April 22, 2020, from
<https://www.nch.com.au/scribe/index.html>
- Nurse, J. R. C., Creese, S., Goldsmith, M., & Lamberts, K. (2011). Trustworthy and effective communication of cybersecurity risks: A review. *Proceedings of the 1st Workshop on Socio-Technical Aspects in Security and Trust*, 60–68. <https://doi.org/10.1109/STAST.2011.6059257>
- Oates, M., Ahmadullah, Y., Marsh, A., Swoopes, C., Zhang, S., Balebako, R., & Cranor, L. F. (2018). Turtles, Locks, and Bathrooms: Understanding Mental Models of Privacy Through Illustration. *Proceedings on Privacy Enhancing Technologies*, 2018(4), 5–32. <https://doi.org/10.1515/popets-2018-0029>
- Paul, C. L., & Whitley, K. (2013). A Taxonomy of Cyber Awareness Questions for the User-Centered Design of Cyber Situation Awareness. In L. Marinou & I. Askoxylakis (Eds.), *Human Aspects of Information Security, Privacy, and Trust* (pp. 145–154). https://doi.org/10.1007/978-3-642-39345-7_16
- Ramokapane, K. M., Rashid, A., & Such, J. M. (2017). “I feel stupid I can’t delete...”: A Study of Users’ Cloud Deletion Practices and Coping Strategies. *Proceedings of the 13th Symposium on Usable Privacy and Security*, 241–256. www.usenix.org/conference/soups2017/technical-sessions/presentation/ramokapane
- Rohrmann, B. (1992). The evaluation of risk communication effectiveness. *Acta Psychologica*, 81(2), 169–192. [https://doi.org/10.1016/0001-6918\(92\)90004-W](https://doi.org/10.1016/0001-6918(92)90004-W)
- Saldaña, J. (2016). *The Coding Manual for Qualitative Researchers*. SAGE Publications, Inc.
- Sanders, L., & Stappers, P. J. (2012). *Convivial Toolbox*. BIS Publishers B.V.
- Slovic, P. (2000). *The Perception of Risk* (R. E. Löfstedt (ed.)). Taylor & Francis Ltd.
- Spero, E., Stojmenovic, M., Hassanzadeh, Z., Chiasson, S., & Biddle, R. (2019). Mixed Pictures: Mental Models of Malware. *Proceedings of the 17th International Conference on Privacy, Security and Trust*.
<https://doi.org/10.1109/PST47121.2019.8949030>
- Stewart, G., & Lacey, D. (2012). Death by a thousand facts: Criticising the technocratic approach to information security awareness. In *Information Management and Computer Security* (Vol. 20, Issue 1, pp. 29–38).
<https://doi.org/10.1108/09685221211219182>
- Strauss, A., & Corbin, J. (1998). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory* (2nd ed.). Sage Publications, Inc.

- SURF. (n.d.). *SURF*. Retrieved May 18, 2020, from <https://www.surf.nl/>
- Van den Berg, J. (2018). Cybersecurity Best Practices. In M. Bartsch & S. Frey (Eds.), *Cybersecurity best practices* (pp. 571–583). Springer Fachmedien Wiesbaden. <https://doi.org/10.1007/978-3-658-21655-9>
- Van den Berg, J. (2019). Grasping Cybersecurity: A set of Essential Mental Models. *Proceedings of the 18th European Conference on Cyber Warfare and Security*, 534–543.
- Vania, K., Rader, E., & Wash, R. (2014). Mental models of software updates. *International Communication Association*, 1–39. <http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:No+Title#0>
- Wash, R. (2010). Folk models of home computer security. *Proceedings of the 6th Symposium on Usable Privacy and Security*, 1–16. <https://doi.org/10.1145/1837110.1837125>
- Wash, R., & Rader, E. (2011). Influencing Mental Models of Security: A Research Agenda. *Proceedings of the New Security Paradigms Workshop*, 57–66. <https://doi.org/10.1145/2073276.2073283>
- Wash, R., & Rader, E. (2015). Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users. *Proceedings of the 11th Symposium On Usable Privacy and Security*, 309–325. <https://www.usenix.org/conference/soups2015/proceedings/presentation/wash>
- Wash, R., Rader, E., & Fennel, C. (2017). Can People Self-Report Security Accurately?: Agreement Between Self-Report and Behavioral Measures. *Proceedings of the Conference on Human Factors in Computing Systems*, 2228–2232. <https://doi.org/10.1145/3025453.3025911>
- Zou, Y., Mhaidli, A. H., McCall, A., & Schaub, F. (2018). “I’ve Got Nothing to Lose”: Consumers’ Risk Perceptions and Protective Actions after the Equifax Data Breach. *Proceedings of the 14th Symposium on Usable Privacy and Security*, 197–216. <https://www.usenix.org/conference/soups2018/presentation/zou>

Appendix A: Interview protocol

This appendix contains the interview protocol in English and Dutch. At the beginning of the interview a short introduction was provided. The English and Dutch introduction can be found in section A.1 and A.2 The interview protocol can be found in section A.3.

A.1: English interview introduction

The aim of this research is to determine the differences between experts and non-experts in their perception of VPN. The focus is on the VPN in [the professional services firm]. In this interview, I will ask you some questions, and the intention is that you tell as much as possible about what you know about VPN. I would like to emphasize that there are no right and wrong answers, so tell everything you can think of. During the interview I will ask you to make a drawing based on an assignment. I ask you to think out loud as much as possible while making this drawing. For the drawing we will use the whiteboard in Big Blue Button. I will now show the whiteboard and briefly explain how it works. <Show the whiteboard and give a brief overview of the possibilities>.

I would like to inform you again that this interview will be recorded. The recording will be used to transcribe the interview and will not be viewed by anyone outside the research group. I have sent you a consent form by e-mail, have you been able to read this and do you have any questions about this? Do you have any other questions before we start the interview?

A.2: Dutch interview introduction

Het doel van dit onderzoek is bepalen wat de verschillen zijn tussen experts en niet-experts in hun perceptie van VPN. Het gaat hierbij om het gebruik van VPN in [the professional services firm]. In dit interview zal ik enkele vragen stellen, waarbij het de bedoeling is dat u zo veel mogelijk vertelt over wat u over VPN weet. Ik wil hierbij benadrukken dat er geen goede en foute antwoorden zijn, dus vertel alles wat u kunt bedenken. Tijdens het interview zal ik u vragen om een tekening te maken aan de hand van een opdracht. Ik vraag u om zo veel mogelijk hardop na te denken tijdens het maken van deze tekening. Voor de tekening zullen we gebruik maken van het whiteboard in Big Blue Button. Ik zal nu het whiteboard laten zien en kort uitleggen hoe het werkt. <Laat het whiteboard zien en geef een kort overzicht van de mogelijkheden>.

Ik wil u nogmaals informeren dat dit interview opgenomen zal worden. De opname zal worden gebruikt voor het transcriberen van het interview en wordt door niemand buiten de onderzoeksgroep ingezien. Ik heb u eerder een toestemmingsformulier gestuurd via de e-mail, heeft u dit kunnen doorlezen en heeft u hierover nog vragen? Heeft u nog andere vragen voordat wij beginnen met het interview?

A.3: Interview protocol

The complete overview is presented in table A.1. First a general question was asked (A), after which each topic mentioned was asked to elaborate. Continuation to the next section (B, C, or D) happened when either no new topics came up in the current section or when an interviewee naturally continued to a new section. When an interviewee continued to a new section, the interviewer let the interviewee continue and revisited the previous section when appropriate.

Table A.1: Interview protocol

Interview protocol English	Interview Protocol Dutch
A - Starting question 1. What is a VPN?	A - Start vraag 1. Wat is een VPN?
B - When drawing blank in block A (in order) 1. Have you ever heard the word VPN? Can you remember anything about it?	B – Als geen idee bij vraag A (op volgorde) 1. Heb je ooit gehoord van het woord VPN? Kan jij je er iets over herinneren?

2. Let's see whether we can jog your memory. VPN is called <name of VPN in firm> within <name of firm>.	2. Misschien kunnen we je geheugen helpen. VPN wordt <name of VPN in firm> genoemd binnen <name of firm>.
C - Questions how VPN works (not necessarily in this order) - Why do you use VPN? - When? - Where? - What actions do you take to create a VPN connection? - On what devices do you use a VPN? - How does a VPN work? / What happens when you make a VPN connection? - Drawing exercise - Basis scenario: Make a VPN connection at home - Second scenario (different location): Make a VPN connection at a coffee bar - Third scenario (specific task): Send an e-mail with an active VPN connection	C - Vragen voor how VPN works (volgorde kan verschillen) - Waarom gebruik jij VPN? - Wanneer? - Waar? - Welke handelingen voer je uit om een VPN verbinding te maken? - Op welke apparaten gebruik je een VPN? - Hoe werkt een VPN? / Wat gebeurt er als je een VPN verbinding maakt? - Teken opdracht - Basis scenario: Maak een VPN verbinding thuis - Tweede scenario (andere locatie): Maak een VPN verbinding in een café - Derde scenario (specifieke taak): Stuur een e-mail met een actieve VPN verbinding
D – Questions changes in threat landscape - What is the influence of a VPN connection on your computer security? - Why? - How? <u>In drawing</u>: draw influence in previous drawing. - What kinds of digital threats do you deal with on a normal day? - How does the threat change because of the VPN connection? - What kinds of social threats do you deal with on a normal day? - How does the threat change because of the VPN connection? - Who or what could be an attacker behind a threat? - How does the kind of attacker change because of the VPN connection? - What would be an attacker's intention? - What would be an attacker's capability? - What could be the impact of an attack? - Why? - How? <u>Vulnerabilities of VPN</u> - How secure is a VPN connection? - If not 100% secure: - Why?	D – Questions changes in threat landscape - Wat is de invloed van een VPN verbinding op jouw computerbeveiliging? - Waarom? - Hoe? <u>In tekening</u>: teken invloed in eerdere tekening. - Met wat voor digitale dreiging heb jij op een normale dag te maken? - Hoe verandert de soort dreiging door een VPN verbinding? - Met wat voor sociale dreiging heb jij op een normale dag te maken? - Hoe verandert de soort sociale dreiging door een VPN verbinding? - Wie of wat is de aanvaller die de dreiging veroorzaakt? - Hoe verandert de soort aanvaller door een VPN verbinding? - Wat is de motivatie van een aanvaller? - Wat voor achtergrond heeft een aanvaller? - Wat zou de impact van een aanval kunnen zijn? - Waarom? - Hoe? <u>Kwetsbaarheden van VPN</u> - Hoe veilig is een VPN verbinding? - Als niet 100% veilig: - Waarom?

○ <u>In drawing:</u> draw where it is not secure and the cause ○ How do your actions change because of this? ○ What are the consequences of these insecurities?	○ <u>In tekening:</u> teken waar het niet veilig is en waardoor ○ Hoe veranderen jouw handelingen hierdoor? ○ Wat zijn de consequenties van deze onveiligheden?
E - Example neutral continuation prompts • Could you elaborate on that? • Could you go into more detail about that? • Sorry, could you explain what you mean with ...? • What do you mean with ...? • Why do you say ...? • What is ...?	E - Voorbeelden neutrale aanmoedigingen om meer te vertellen • Kan je meer vertellen over ...? • Zou je kunnen uitleggen wat je bedoelt met ...? • Wat bedoel je met ...? • Waarom zeg je ...? • Wat is ...?

Appendix B: Recruitment Text and Informed Consent Form

This appendix contains the recruitment text for contact persons and possible participants and the informed consent form.

B.1: Recruitment text for contact persons experts Dutch

Beste <naam>,

Voor afronding van mijn studie loop ik stage bij EY. Het doel van mijn thesis is om communicatie omtrent cybersecurity effectiever en efficiënter te maken, om uiteindelijk mensen veiliger om te laten gaan met IT systemen. Om dit te bereiken wil ik de informatiebehoefte van [the professional services firm] medewerkers bepalen omtrent een specifiek cybermechanisme.

Om deze informatiebehoefte te bepalen zal ik twee groepen gaan interviewen: experts en niet-experts. Ik benader u, omdat ik denk dat u mij kunt helpen om in contact te komen met experts. In eerste instantie ben ik op zoek naar 2 experts om te interviewen begin juni. Daarna volgen nog extra interviews met ongeveer 5 experts in juli. Ik verwacht dat een interview maximaal 1 á 1,5 uur duurt.

Kunt u mij in contact brengen met experts of weet u wie ik beter hiervoor kan contacteren? Experts dienen minimaal 2 jaar binnen [the professional services firm] te werken en/of een relevant certificaat te bezitten (bijvoorbeeld RE IT-Audit, CISA of CISSP). Mijn doel is om een gevarieerde set aan experts te interviewen, die variëren op het gebied van opleidingsachtergrond, rol in de afdeling en aantal jaren werkzaam bij [the professional services firm].

Alvast bedankt. Met vriendelijke groet,

Veroniek Binkhorst

B.2: Recruitment text for contact persons experts English

Dear <name>,

To complete my studies, I am doing an internship at EY. The aim of my thesis is to make cybersecurity communication more effective and efficient, and ultimately to enable people to interact with IT systems in a more secure manner. To achieve this, I want to determine the information needs of [the professional services firm] employees regarding a specific cybermechanism.

To determine this information need, I will interview two groups: experts and non-experts. I can use this information to eventually compare the knowledge of non-experts. Experts must work for at least 2 years within [the professional services firm] and / or have a relevant certificate (for example RE IT-Audit, CISA or CISSP).

I'm approaching you because I think you can help me get in touch with experts. At first I am looking for 2 experts to interview in early June. Additional interviews will follow with approximately 5 experts at the end of June. I expect an interview to last 1 to 1.5 hours.

Could you help me to get in touch with experts or do you know who I can contact for this? My goal is to interview a diverse set of experts, varying in educational background, role in the department and number of years working at [the professional services firm].

Kind regards,

Veroniek Binkhorst

B.3: Recruitment text for contact persons laypeople Dutch

Beste <naam>,

Voor afronding van mijn studie loop ik stage bij EY. Het doel van mijn thesis is om communicatie omtrent cybersecurity effectiever en efficiënter te maken, om uiteindelijk mensen veiliger om te laten gaan met IT systemen. Om dit te bereiken wil ik de informatiebehoefte van [the professional services firm] medewerkers bepalen omtrent een specifiek cybermechanisme.

Ik benader u, omdat ik denk dat u mij kunt helpen om in contact te komen met medewerkers van de afdeling <naam afdeling>. In eerste instantie ben ik op zoek naar 1 medewerker om te interviewen begin juni. Daarna volgen nog extra interviews met ongeveer 5 medewerkers in juli. Ik verwacht dat een interview maximaal 1 uur duurt.

Kunt u mij in contact brengen met medewerkers van de afdeling <naam afdeling> of weet u wie ik beter hiervoor kan contacteren? Mijn doel is om een gevarieerde set aan medewerkers te interviewen, die variëren op het gebied van opleidingsachtergrond, rol in de afdeling en aantal jaren werkzaam bij [the professional services firm].

Alvast bedankt. Met vriendelijke groet,

Veroniek Binkhorst

B.4: Recruitment text for possible participants English

Dear <name>,

To complete my studies, I am doing an internship at EY. The aim of my thesis is to make cybersecurity communication more effective and efficient, and ultimately to enable people to interact with IT systems in a more secure manner. To achieve this, I want to determine the information needs of [the professional services firm] employees regarding a specific cyber mechanism.

I am approaching you because <contact name> referred me to you. Would you be willing to participate in an interview in <date / week / month>? I expect an interview to last maximum <1 hour / 1 to 1.5 hours>.

Purpose of the interview

As stated, the aim of the study is to determine the information needs of [the professional services firm] employees regarding a specific cyber mechanism. The information need is determined by looking at how much and what you can tell about this specific cyber mechanism. What this specific cyber mechanism is remains unknown for now, to prevent participants from informing themselves before the interview.

Interview set-up

The interview has an open design and will be guided by open questions asked by me. The idea is that you tell as much as you know about the subject and the question. There are no right or wrong answers. The interview will take place via the platform Big Blue Button. This platform is supported by SURFcloud and is made available by Delft University of Technology. It is not necessary to explore the platform in advance, but if you wish, you can do so by clicking on the following link: <https://bbb.surfcloud.nl/b/997-2x6-j6u-7x7>.

How collected data is handled

At the beginning of the interview, I will ask you about your educational background, your role in the department and the number of years you have worked at [the professional services firm]. The results on these demographic questions will be combined with the results of the other participants in the study proceedings

and cannot be traced back to you. Then I will start the interview with the first question. The interview will be recorded in Big Blue Button. The recording will only be used to transcribe the interview. The recording will not be shared with anyone outside the research group and will be destroyed at the end of the research period. The transcription will be made anonymous and serves as data for the research. Finally, I will ask you to complete a couple drawing exercises during the interview, for which we will use the whiteboard in Big Blue Button.

Continuation if you decide to participate

Participation in this study is entirely without obligation and you can request access to, correction or deletion of your personal data at any time. If you decide to participate I will send you a calendar invite with a date and time, with a link to the Big Blue Button environment attached. Before the interview takes place I will send you a separate e-mail with an English informed consent form. In this informed consent form, you can find more information about the study and what you agree to when you participate in the study. Consent can be given by replying to that e-mail.

You would help me a lot by participating in the study.

Kind regards,

Veroniek Binkhorst

B.5: Recruitment text for possible participants Dutch

Beste <naam>,

Voor afronding van mijn studie loop ik stage bij EY. Het doel van mijn thesis is om communicatie omtrent cybersecurity effectiever en efficiënter te maken, om uiteindelijk mensen veiliger om te laten gaan met IT systemen. Om dit te bereiken wil ik de informatiebehoefte van [the professional services firm] medewerkers bepalen omtrent een specifiek cybermechanisme.

Ik benader u, omdat ik uw naam heb doorgekregen van <naam contactpersoon>. Bent u bereid om deel te nemen aan een interview in <datum/week/maand>? Ik verwacht dat een interview maximaal <1 uur / 1 tot 1,5 uur> duurt.

Doel van het interview

Zoals gezegd is het doel van het onderzoek om de informatiebehoefte van [the professional services firm] medewerkers te bepalen omtrent een specifiek cybermechanisme. Uw rol hierin is helpen bij het creëren van een compleet beeld van het cybermechanisme. Wat dit specifieke cybermechanisme is blijft nog even onbekend, om te voorkomen dat deelnemers zich van te voren gaan informeren.

Opzet van het interview

Het interview heeft een open opzet en wordt geleid door open vragen vanuit mij. Het idee is dat u zo veel mogelijk vertelt wat u kunt bedenken omtrent het onderwerp en de vraag. Hierbij zijn geen goede of foute antwoorden. Het interview zal plaatsvinden via het platform Big Blue Button. Dit platform wordt ondersteund door SURFcloud en is beschikbaar gesteld door de Technische Universiteit Delft. Het is niet nodig om het platform van te voren te verkennen, maar mocht u dit willen dan kunt u dit doen door te klikken op de volgende de volgende link: <https://bbb.surfcloud.nl/b/997-2x6-j6u-7x7>.

Omgang met verzamelde data

Aan het begin van het interview zal ik u vragen naar uw opleidingsachtergrond, uw rol in de afdeling en het aantal jaren dat u werkzaam bent bij [the professional services firm]. De resultaten van deze demografische

vragen zullen in de verslaglegging gecombineerd worden met de resultaten van de andere participanten en niet herleidbaar zijn naar u. Vervolgens open ik met de eerste vraag. Het interview zal worden opgenomen in Big Blue Button. De opnames dienen alleen voor het transcriberen van het interview. De opname wordt door niemand buiten de onderzoeksgroep ingezien en zal aan het eind van het de onderzoeksperiode worden vernietigd. De transcriptie zal worden geanonimiseerd en dient als data voor het onderzoek. Ten slotte zal ik u vragen om tijdens het interview enkele tekenopdrachten te voltooien, waarbij gebruik zal worden gemaakt van het whiteboard in Big Blue Button.

Vervolg als u besluit deel te nemen

Deelname aan dit onderzoek is geheel vrijblijvend en u kunt op elk moment om inzage, correctie of verwijdering van uw persoonlijke gegevens vragen. Indien u besluit deel te nemen zal ik u een agenda verzoek met een datum en tijd sturen, met een link naar de Big Blue Button omgeving bijgevoegd. Voordat het interview plaatsvindt zal ik u een aparte e-mail sturen met een Engelstalig toestemmingsformulier. In dit toestemmingsformulier kunt u meer informatie over het onderzoek vinden en vinden waar u mee instemt als u deelneemt aan het onderzoek. Toezegging van toestemming gebeurt door te antwoorden op die e-mail.

U helpt mij erg door deel te nemen aan het onderzoek en ik hoor graag of u hiertoe bereid bent.

Met vriendelijke groet,

Veroniek Binkhorst

B.8: Informed consent form via e-mail

Dear <name>,

In this e-mail I send you the consent form for the interview upcoming <day>. In this consent form you will find more information regarding the study and you can find to what you agree by participating in the study. Giving consent can by replying on this e-mail, stating that you give consent. If you have any questions regarding the interview or the consent form, you can e-mail me or ask the questions at the beginning of the interview.

Information regarding the study, data processing, and questions.

1. Background and aims of the study

The purpose of this research is to determine the similarities and differences between experts and non-experts of their perception of VPN in a professional services firm in the Netherlands. This study aims at empirically investigating the perception of experts and non-experts on: 1) What a VPN is, 2) For what purpose a VPN is used, 3) What the technical infrastructure of a VPN looks like, 3) What the security benefits and/or risks of using a VPN are, 4) What changes occur in the threat landscape when using a VPN, and 5) What the impact of a possible attack could be when using VPN.

2. Do I have to participate?

You can ask questions about the study before deciding whether or not to participate. If you do agree to participate, you may withdraw yourself from the study at any time, without giving a reason and without penalty, by informing the researchers of this decision.

3. What will happen in the study?

If you agree to take part in the study, you will be asked to participate in an approximately 60 minute semi-structured interview in English or Dutch. The researcher will conduct the interview by using the conferencing software Big Blue Button. As part of the interview a drawing task will be completed using the whiteboard in the Big Blue Button. The interview will be recorded, and transcribed to text after the interview has taken place. The recording consists of audio, and video if the participants chooses to enable video.

4. Are there any potential risks in taking part?

Interviews will be held with employees in a professional services firm on their beliefs of how a VPN works. The knowledge of participants may be different than expected from experts and/or laypeople. We aim to address such concerns by:

- a. Storing e-mail addresses, the recordings of the interviews, demographic information, and a pdf file of the consent e-mail securely.
- b. Anonymizing the transcriptions.
- c. Summarizing demographic information.
- d. Deleting the original e-mail from the e-mail inbox.
- e. Destroying the collected e-mail addresses, recordings, original demographic data, and pdf file of the consent e-mails after the end of the study.

5. Are there any benefits in taking part?

There are no benefits involved for the participants of the study.

6. What happens to the data provided?

We will securely store all collected data at the EY laptop of the researcher. A back-up of the collected data will be securely stored on SURFdrive. Nobody except the project research team will have access to the data during the study period. The collected e-mail address, recording of the interview, original demographic data, and pdf file of the consent e-mail will be destroyed after the end of the study.

At no point will we ask for your name except to confirm your consent. Consent will be confirmed by replying in an e-mail stating the participant gives consent. We will ask for the participant's educational qualifications, education area, role in the firm, and years active in the firm. As this can be used to identify certain individuals, we will treat this as personal data and store it securely. The answers on the questions regarding personal data will not be published per individual participant, but will be presented in the study results in a summarized matter.

The participant has the right to request access to and rectification or erasure of personal data.

The anonymized transcription, drawings made during the interview, and summarized demographic data will be shared in products of the study and in will be stored on the 4TU.Centre for Research Data for a minimum retention period of 10 years² after publication or public release of the work of the research.

We ask participants for their permission to use direct quotes, these will be attributed to a participant number.

7. Will the research be published?

The results will contribute to the completion of a master's thesis project and a paper submitted to an academic venue. To protect the participants' anonymity we will anonymize all information relating to the participants and the employer of the participants.

8. Who has reviewed this study?

This study has been reviewed by, and received ethics clearance through, the Delft University of Technology Human Research Ethics Committee (reference number: 55223)

9. Who do I contact if I have a concern about the study or I wish to file a complaint?

If you have a concern about any aspect of this study, please speak to the relevant researcher V. Binkhorst (v.f.binkhorst@student.tudelft.nl), who will do their best to answer your query. The researcher should acknowledge your concern within 10 working days and give you an indication of

² In accordance with the TU Delft Research Data Framework Policy. Available online: <https://doi.org/10.5281/zenodo.2573160>

how they intend to deal with it. If you remain unhappy or wish to make a formal complaint, please contact the relevant chair of the Human Research Ethics Committee at the Delft University of Technology who will seek to resolve the matter in a reasonably expeditious manner:

Chair, Human Research Ethics Committee; Email: HREC@tudelft.nl.

10. Contact details

If you would like to discuss the research with someone beforehand (or if you have questions afterwards), please contact:

Veroniek Binkhorst
Email: v.f.binkhorst@student.tudelft.nl

Consent Form for mental models of VPN in a professional services firm in The Netherlands: A study

Taking part in the study

I have read and understood the study information dated <date>, or it has been read to me. I have been able to ask questions about the study and my questions have been answered to my satisfaction.

I consent voluntarily to be a participant in this study and understand that I can refuse to answer questions and I can withdraw from the study at any time, without having to give a reason.

I understand that taking part in the study involves participating in an audio recorded interview. I understand that if I decide to enable video during the interview this will also be recorded. I understand that part of the interview includes a drawing task. I understand that the recorded interview will be transcribed as text and anonymized and the recording will be destroyed after the end of the study.

Use of the information in the study

I understand that information I provide will be used for a master thesis report and publications in academic venues (like conferences or journals).

I understand that personal information collected about me that can identify me, such as my name or email address, will not be shared beyond the study team.

I agree that my information can be quoted in research outputs.

I agree to joint copyright of the drawings created during the interview to Veroniek Binkhorst.

Future use and reuse of the information by others

I give permission for the anonymized interview transcript, drawings made during the interview, and summarized demographic information that I provide to be archived in the 4TU.Centre for Research Data so it can be used for future research and learning.

I look forward to your reply,

Kind regards,

Veroniek Binkhorst

Appendix C: Interview transcripts

This appendix contains all interview transcripts. In the transcripts the interviewer is identified as X and the interviewee as Y. Interviews were anonymized in a standardized manner, focused on preserving the context. Where part of a sentence could identify the interviewee or the professional services firm, this part was replaced by one of the insertions in table C.1.

Table C.1: Anonymization insertions in the interviews

[access token provider]	[example IP-address]	[partner]
[an internal page]	[example of mobile application]	[place]
[cloud software]	[example of restaurant]	[role]
[company]	[example of software provider]	[social media platform]
[conferencing software]	[me]	[the professional services firm]
[country]	[mobile phone]	[the VPN of the professional services firm]
[department]	[number]	[the Wi-Fi of the professional services firm]
[e-mail]		

If using one of these insertions was not possible, the text was omitted. This is resembled by placing the text [hh:mm:ss until hh:mm:ss has been omitted]. At some instances, it was not possible to hear what was being said. If this was the case, this is identified by three dots (example: ...).

To follow what is drawn at which moment in time, multiple versions of the drawings created by participants are included where necessary. Where a modification to a drawing is made, this is indicated in the transcript by [start drawing participant number_number drawing].

C.1: Transcript Expert 1

Duration: 82 minutes

Language: Dutch

Number of drawings: 22

X: Dan begin ik met de eerste vraag van het interview. Kan je mij vertellen wat een VPN is?

Y: Wat een VPN is? Eh, wat is de gewenste doelgroep voor deze uitleg?

X: Ja, het is de bedoeling dat je zo veel mogelijk vertelt wat jij van VPN weet, dus, eh, ja, mij uitlegt wat een VPN-verbinding is.

Y: Oké, voor mij is een VPN-verbinding- Het staat voor Virtual Private Network. Eh, virtueel betekent softwarematig. Eh, wat het doet is, het legt een verbinding eh, van een endpoint, ofwel een startpunt, dus een endpoint kan betekenen of jouw computer, of jouw eh, mobiel, of een tablet, een veilige verbinding te kunnen maken met een netwerk. En vaak noem je dat dan een intern netwerk. He, dus wat het doet, je legt eigenlijk een tunnel tussen iets wat normaal gesproken niet binnen het netwerk ligt, he, doordat je niet verbonden bent met het netwerk, eh, tot een netwerk, eh, ja, een intern netwerk, een intern onderdeel van het netwerk. Want meestal heb je, eh, vanuit een computernetwerk heb je eh, een, een, extern facing netwerk en een intern netwerk, he, dat zijn segmenten van een netwerk. Eh, het externe netwerk is vaak verbonden met het Internet. Daar kun je vanuit elk punt van de wereld, he, zolang je het adres weet, het uiteindelijke adres weet, kun je daarop inloggen. Eh, maar op het moment dat jij, bij resources of, he, de, de dingen, dingen, servers noemen we het op andere computers, websites wil met een privé IP adres zeg maar, moet je dat doen via ofwel connecten via het netwerk zelf, dat is vaak als jij binnen het kantoor bent of wat dan ook, dan maak je direct verbinding met het interne netwerk, he, dan kun je praten met alles binnen in ieder geval binnen dat segment van het netwerk. Maar bij een VPN laat je iemand toe die niet in

de buurt is van het netwerk, om via het Internet eigenlijk, eh, een andere lijn te leggen naar die interne netwerken. Eh, ja, dat is hoog over wat een VPN is. Een VPN is eigenlijk, ja, ze noemen het niet een end-to-end encrypted beveiligd, he, dus je maakt eigenlijk een beveiligde verbinding, maar die beveiliging die begint pas, he, die begint bij het apparaat tot aan waar je binnenkomt aan de andere kant van die lijn. He, dus op het moment dat je aan de andere kant zit, is je, is je, eh, is je netwerk, of je, ja, je traffic, je verkeer is dan niet meer beveiligd. Die beveiliging kun je dus op verschillende manieren doen, daar worden verschillende protocollen bij gebruikt, dat kun je zelf instellen. Dus, dat zijn, eh, bepaalde, eh, cryptografische, eh, ja, handshakes noemen ze dat, maar dat zijn protocollen, he, waar punt A met punt B praat, eh, en punt B weer terugpraat met punt A, om te zeggen, om te verifiëren wie je bent. En dat doe je door middel van bijvoorbeeld in te loggen met een wachtwoord eh, of een username en een password. Eh, en de meeste VPN-oplossingen die gebruiken ook een tweede vorm van verificatie, dus een hardware of een software token, die je toevoegt aan je gebruikersnaam en wachtwoord. Omdat het ontzettend gevoelig is om, om ineens vanuit een onvertrouwd punt in de wereld kunnen inloggen op een vertrouwd punt. Die zou je goed dicht moeten gooien. Eh, verder bestaan er ook verschillende vormen van VPN. Dus, waar je, eh, ja, ook een volledige, ja, ik noem het volledig en split, split tunnel. Dus je kunt al het verkeer door een VPN leiden en wat er dan vaak gebeurt, is dat je al het verkeer naar het datacenter stuurt, die je dan vervolgens weer doorstuurt naar het juiste punt. Of je hebt een gedeelde of een split, he, en dan bepaald een organisatie welke endpoints, oftewel welke IP-adressen door een VPN-tunnel moeten en welke niet. En daarmee kun je de hoeveelheid data die je door je datacenter heen leidt eh, verminderen. Heel veel mensen hebben niet door dat dat zo werkt. Dus een voorbeeld is dat een organisatie kan zeggen, oké, ik wil al het verkeer naar [social media platform], [social media platform], [social media platform], [social media platform], allerlei social media en [social media platform] bijvoorbeeld, die laat ik gewoon via het Internet verlopen. En al het andere verkeer, of al het verkeer dat naar een intern object is gericht, dat laten we door de VPN heenlopen. Eh, ja, dus dat zijn verschillen daarin. Eh, dan zijn de verschillen ook, ja, wat ik ook van VPN weet is dat er natuurlijk veel verschillende aanbieders zijn van VPN. He, dat is zoals ik al eerder zei, het is virtueel, dus het is software gedreven. Eh, en wat mensen ook vaak niet beseffen, is dat die, eh, dat die software ook, ja, eigenlijk, je kunt heel veel software gebruiken om tot een VPN-verbinding te komen, daar hoeft je niet, eh, niet alle organisaties hebben dat dichtgezet, voor één, of he, wordt dat opengezet voor één specifieke VPN-aanbieder, maar kunnen ook meerdere zijn, zolang je het wachtwoord maar weet. Zolang je de juiste credentials hebt om in te loggen. Eh, ja, ik denk dat dit wel redelijk gecovered is, in ieder geval. Ja, is dit in de richting van wat je, wat je zocht?

X: Ja. Je zegt een endpoint, bijvoorbeeld noemde je een computer en een mobiel. Gebruik jij ook een VPN op jouw computer en jouw mobiel?

Y: Eh, ik gebruik alleen eh, actief VPN op mijn eh, computer. Eh, en ik gebruik, even kijken hoor, geen actieve VPN op mijn eh, mijn mobiel. Dat is afhankelijk van welke service ik gebruik hoor, want als ik de mobiele app gebruik dan doet die dat volgens mij automatisch. Eh, en hetzelfde met alle links die ik aanklik vanuit mijn e-mail, die gaan naar een beveiligde browser, dus er zit een soort van sandboxing in, die volgens mij automatisch leidt naar eh, een VPN-verbinding. Maar mijn computer, ja, dat is afhankelijk ook, he, want je merkt gewoon, er is wel snelheidsverlies. Toen ik inlogde op eh, dit interview, de Big Blue Button, eh, toen zag ik ook dat ik connected was met [the VPN of the professional services firm], ja, die heb ik uitgezet, want je merkt gewoon, ja, daar zit wat vertraging in. En daarbij merk ik dus dat, waarschijnlijk gebruikt [the professional services firm] een volledige VPN en niet een split tunnel.

X: En je noemde eerder over de beveiliging en encryptie, kun je daar meer over vertellen?

Y: Oeh, ja, je gebruikt natuurlijk, eh, ja, dat hangt er een beetje van af wat je, wat je, welk protocol je gebruikt, want er zijn natuurlijk meerdere protocollen, maar eh, volgens mij maken ze gebruik van, volgens mij zijn daar ook weer verschillende stromen in. En als ik het niet fout heb, en pin me daar niet aan vast, gebruiken ze een block cypher, dus AES-256 en daarbinnen een handshake, eh, dus met ook een certificaat. En dat certificaat wordt dan gebruikt om de data te encrypten. Dus je zegt eigenlijk ik ben deze partij, dat is eigenlijk je verificatiestap he, als je inlogt, dan zegt de server, oké, ik geloof dat, want zo ben je geregistreerd, dan kom je terug en volgens mij komt er dan eh, een certificaat op je computer te staan. En met dat certificaat, eh, dat gebruik je dan om stukken van je data, he, dat wordt opgesplitst in pakketjes

eh, en die pakketten worden dan versleuteld met dat certificaat en aan de andere kant hebben ze een versie van het certificaat waarmee ze de data kunnen eh, ja, terugdraaien, dus unencrypten, ontsleutelen.

X: Aan de andere kant?

Y: Ja, aan de andere kant. Dat zijn de, zeg maar, ja, je logt natuurlijk in via het Internet en dat heeft een plek waar dat aankomt. Dus er is data, eh, die je versleuteld, dat wordt verstuurd naar een server, of dat wordt verstuurd naar een eh, computer aan de andere kant, het netwerk dan noemen we dat. Maar dat komt natuurlijk niet aan op he, dat komt niet direct in het netwerk via eh, een server aan de andere kant, daar zitten stappen tussen. En of dat nou een load balancer is of dat nou een eh, ja, vaak wordt dat via een load balancer gedaan of een firewall of een ja, web application firewall, en die hebben vaak, die hebben vaak een, eh, manier om een certificaat te gebruiken. Die hebben dan het certificaat aan de andere kant om de data te ontsleutelen, zodat die data dan verstuurd kan worden naar de server in kwestie.

X: Oké. En wat is een load balancer?

Y: Een load balancer is eigenlijk een netwerk eh, ja, appliance noemen ze dat, ja, vroeger was het een hardware stuk, maar dat is het tegenwoordig niet meer, ja, eigenlijk ook weer wel, maar goed, daar gaan we maar niet op in. Eh, en die- Tegenwoordig is het veel software gedreven allemaal, he, ook de cloud en zo. Eh, en een load balancer is eigenlijk een stukje eh, netwerkkapparatuur waarin data wordt eh, ja, gedistribueerd, dus eigenlijk wordt gekeken van welke servers eh, kan dit verzoek aan. He, er is altijd een verzoek binnen het HTTP protocol, eh, of HTTPS protocol, of any protocol ook, maakt niet uit welk protocol je gebruikt. Eh, en die load balancer, die is eigenlijk om ervoor te zorgen dat de server niet overbelast raken met allerlei request of verzoeken. En die verzoeken worden dus verdeeld over de servers ofwel de apparaten die eh, waar het om gaat. Soms, soms zit er geen load balancer tussen hoor, maar dat is in de nieuwe vorm is dat wel een heel veel gebruikt stukje hardware of software.

X: Als er geen load balancer tussen zit, wat zit er dan tussen?

Y: Wat zei je?

X: Als er geen load balancer tussen zit, wat zit er dan wel tussen?

Y: Ofwel een firewall, ofwel geen firewall. Maar er zit vaak een type bescherming, een beschermingslaag tussen. Dus wat er ook wel eens in zit is dat je eerst een firewall raakt, dan kijkt die mag dit eigenlijk wel, dan gaat die naar een server, en soms zit daar nog een firewall achter, of een stuk bescherming tussen eh, en daarna ga je pas naar de server.

X: En je beschreef het eerder als een tunnel, wat bedoel je met een tunnel?

Y: Een tunnel. Voor mij, kijk, het is meer dat dat beeldspraak is, een tunnel. Je maakt eigenlijk gewoon een verbinding. Eh, en, en dat is, ja, dat wordt een soort van, he, door de ja, mensen die dat proberen te omschrijven, wordt dat als een tunnel weergegeven, wat je legt eigenlijk alsof je een fysieke verbinding neerlegt, eh, naar een, eh, een type netwerk. Dus je graaft eigenlijk een soort van een verbinding onderlangs, dus het is eigenlijk niet een normaal, een normaal type verkeer. Maar het is bedacht zodat je gewoon direct in een beschermd stukje kan komen, dus alsof je een tunnel graaft. Maar is het echt een tunnel? Nee, het is geen tunnel. Het is gewoon een verbinding. Je zegt gewoon, oké, mag A met B praten, ja dat mag onder bepaalde eh, omstandigheden. En die omstandigheden, die eh, die geef je, he, die geef je, die configureer je eigenlijk. Dus is het een tunnel? Nee, het is gewoon een verbinding.

X: En je noemde ook servers in het verhaal. Wat zijn servers?

Y: Servers. Servers zijn, eh, eigenlijk zijn het een soort van computers, zoals jij en ik ook een computer gebruiken, alleen die servers hebben maar een, een select, selecte functionaliteit. Ze doen eigenlijk he, ze zijn niet gemaakt om gebruikers eh, eh, ja, te helpen om hun werk te doen, he, maar het zijn eigenlijk apparaten die iets binnenkrijgen, een verzoek, het verzoek om content te leveren, bijvoorbeeld even een makkelijk voorbeeld is als je een website hebt en die zet je op een server eh, en, en iemand gaat naar een website toe, he, dus www.nu.nl bijvoorbeeld, dan is er bij nu.nl is er een server waar de inhoud van die website op dat moment staat. Eh, en wat die doet is op het moment dat jij nu.nl intypt, dat is eigenlijk een verzoek voor die website, en een server verwerkt dat eigenlijk. He, dat, dat kan door andere verzoeken intern te sturen, maar dat kan ook door gelijk de inhoud terug te sturen. Maar het is- Simpel gezegd is het niet meer dan dat.

X: Oké. En je maakte eerder onderscheidt tussen een intern en extern netwerk. Hoe wordt dat onderscheidt gemaakt?

Y: Eh, er is een eh, conventie, eh, voor IP-adres reeksen. Eh, dus er zijn eigenlijk maar heel- Ja, vroeger toen het IP, het Internet Protocol, bedacht werd, toen dachten ze oké dit aantal zal genoeg zijn. Dus ze hadden een schatting gemaakt van hoeveel IP-adressen er zullen zijn, eh, nou weet ik niet het exacte nummer, volgens mij iets van RFC9812 ofzo, zoiets, denk ik. Nou, eh, hebben ze gezegd we nemen drie, eh, vier octetten, zeg maar. He, dus een IP-adres bestaat uit vier getallen, eh, tussen vier puntjes, of drie puntjes. Dus je begint met een getal punt getal punt getal punt getal punt, dus A B C D noemen ze dat, vier octetten, eh, die geven eigenlijk aan, eh, dat, dat is hun adres eigenlijk, een Internetadres van een endpoint, daar hadden we het eerder over. Dus alle endpoints hebben eigenlijk een IP-adres. Dus dat kan zijn, eh, voor ja, jouw, jouw computer heeft een IP-adres, jouw telefoon heeft een IP-adres, een tablet heeft een, en servers hebben ook een IP-adres, net als alle netwerkapparaten hebben ook een IP-adres. Je kunt je voorstellen, zeker met de komst van Internet of Things, dat IP-adressen opraken. Want je hebt maximaal iets van, ja, wat is het, twee, ja, het gaat dus van nul, het zijn dus octetten he, dus nullen tot enen, dus acht keer een binair getal, nul tot een, dus twee tot de macht acht, en dan maal twee tot de maal acht, maal twee tot de maal acht, maal twee tot de maal acht, en volgens mij is dat iets van 6,5 miljoen of zo. Of, eh, aantal IP-adressen, dus dat is natuurlijk nooit eh, genoeg om alle eh, Internet apparaten te, te huisvesten. Nou, daar hebben ze iets slims op bedacht. Ze hebben een deel hebben ze gereserveerd voor een eh, publiek domein, he, dat zijn eigenlijk alle IP-adressen die eh, ja aangeroepen kunnen worden vanuit het Internet. He, dat zijn bepaalde reeksen, die weet ik niet precies uit mijn hoofd, maar volgens mij iets van 192 reeks, eh, ja, volgens mij 192, want als je zelf volgens mij ook je IP-adres zoekt zit je ook in 192. En dan zijn er een paar anderen, die zijn publiek, dat zijn er best wel veel. En er zijn er een aantal die zijn gereserveerd voor interne, intern gebruik. Dus elk bedrijf kan weer zijn eigen interne gebruiken en die kunnen dus ook overlappen. Dus elk bedrijf kan een tien reeks hebben bijvoorbeeld, een 172 reeks, een 192 reeks, et cetera. Dus, ja, elk bedrijf kan dat weer herhalen. Elk netwerk kan zijn eigen dingetje hebben, zolang endpoints maar niet hetzelfde IP-adres hebben, want ja, dan weet je ook niet meer waar je de data heen moet sturen. Eh, nou zo wordt onderscheidt gemaakt, even helemaal terugkomen naar je vraag, tussen intern en extern netwerk. Eh, dus als jij, bijvoorbeeld binnen [the professional services firm] naar [een interne pagina] gaat, die heeft een intern IP-adres, die heeft een IP-adres die je niet kan bereiken via het Internet, dus daar heb je VPN voor nodig om daarop te komen. Maar, de website van [the professional services firm], die heeft een publiek IP-adres, daar kun je vanuit overal komen.

X: Oké. En je noemde ook een hardware en een software token. Hoe past dit in dit verhaal?

Y: Ja. Eh, ja. Je hebt dus binnen, eh, je identity, je hebt een identiteit, en die identiteit, he, het gaat om wie jij bent zeg maar. En als jij praat met een computernetwerk, dan hebben we het over eh, verificatie. Dus jij zegt eigenlijk dat jij Veroniek bent, maar dat computernetwerk dat gaat vragen oké, laat maar zien dat jij Veroniek bent. He, dat kun je op verschillende manieren doen, he, dus eh, je hebt verschillende factoren die je kunt gebruiken. Dus iets, he, dus iets, je kunt dan laten zien iets wat je bent, he, bijvoorbeeld je, je vingerafdruk, je iris, je DNA, of weet ik veel, noem maar op. Iets wat je hebt, he, dus ofwel dat token, eh, of iets dat je weet, dat is het wachtwoord. Als je naar dat token gaat, dus iets wat je hebt, dan gaat het erom dat jij iets hebt dat, he, iets hebt dat niemand anders heeft. Dus iedereen heeft een token, maar die van jou is specifiek voor jou. He, en, eh, wat voor VPN heel veel gebruikt wordt is eh, een token dat om de 60 seconden geeft die een nieuwe, eh, een nieuwe, eh, ja, binnen [the professional services firm] is dat een zes-cijferig getal, dat je kunt toevoegen aan jouw wachtwoord. Die combinatie die wordt, die wordt, die, die, dat is dan zeg maar een sterkere combinatie dan alleen je wachtwoord, he bijvoorbeeld. Nou, je hebt dus daarin verschillende vormen, he, je hebt een, eh, hardware vorm, he, dan heb je echt een dingetje dat om de 60 seconden jou een nieuw getal geeft. Of je hebt een applicatie, he, een stukje software dus op jouw mobiel bijvoorbeeld, die hetzelfde doet, he, in principe niets anders, behalve dat het fysiek, he, dus hardware versus digitaal wat software is.

X: Deze opties zijn allebei beschikbaar binnen [the professional services firm]?

Y: Eh, volgens mij de laatste tijd niet meer. Want, eh, er zijn natuurlijk wat problemen met hardware tokens. Eh, dus vroeger had je wel zo een hardware token en dat hebben ze volgens mij afgelopen jaren eh, ja,

eigenlijk gemigeerd naar een software token. Dus ik denk, ja, je kunt natuurlijk je mobiel kwijtraken, he, maar met alle herstel mogelijkheden eh, kun je precies dezelfde software token terugkrijgen. En je mobiel raak je toch iets minder snel kwijt dan zo een klein dingetje. He, je mobiel gebruik je natuurlijk voor veel meer dingen dan alleen je, je verificatie. Terwijl dat hardware tokentje, dat was alleen daarvoor gebruikt. En dat, ja, dat was gewoon een klein ding dat je kwijtraakt. Daarnaast kan de batterij opgaan, hij kan beschadigd raken, hij kan gestolen worden. He, al die dingen, die, ja, dat helpt natuurlijk niet voor de veiligheid. En software klinkt makkelijker, maar er zit wel meer, als je je mobiel goed inricht, zit er wel meer beveiliging op. He, je kunt dus, je moet inloggen op je mobiel eh, om, om bij dat software token te komen. En je hebt ook meer pushberichten, he, die zijn er ook. Dus als je inlogt dat je gewoon een bericht krijgt van he, jij bent, er is iemand die inlogt op jouw identiteit, kun je dat bevestigen, nou, druk je op bevestigen. En dan krijg je als je op ja hebt geklikt, krijg je toegang tot, eh, tot de omgeving waar je recht toe hebt.

X: En je zei eerder ook dat er verschillende aanbieders zijn van VPN, hoe zit dit binnen [the professional services firm]?

Y: Volgens mij heeft [the professional services firm] maar een aanbieder, en dat is, ja, ik weet niet of ik dat mag noemen vanuit veiligheidsperspectief. Eh, maar er is in ieder geval een aanbieder, en daar gebruiken we het stukje software voor. Eh, en, ja, volgens mij wordt alleen verkeer vanuit die servers, vanuit die aanbieder eh, worden toegelaten tot het interne netwerk. Als het goed is, dat is een aanname.

X: En waarom gebruik jij een VPN?

Y: Eh, ik gebruik eigenlijk alleen een VPN als ik, als ik toegang moet hebben tot [the professional services firm] interne dingen.

X: En waar gebruik je VPN?

Y: Eh, waar?

X: Ja.

Y: Ja, kijk, in principe gebruik ik mijn computer nooit op onveilige netwerken, dus dat is niet eens een ding voor mij. Ik gebruik gewoon geen onveilige netwerken, punt zeg maar. Dus als ik ergens ben, bijvoorbeeld een vliegveld of een eh, nou, noem maar op, [example of restaurant], dan gebruik ik gewoon mijn telefoon, dat is een 4G netwerk, he, dat is mijn eigen netwerk, dus niemand kan daar, in ieder geval, niemand kan daarop insnoepen, meeluisteren. Eh, dus ik gebruik eigenlijk alleen mijn VPN als ik eh, diensten wil gebruiken van [the professional services firm]. He, ik weet dat zeg maar, op het moment dat je het onveilige netwerk gebruikt, je een VPN moet gebruiken, eh, en dat doe ik dan ook op het moment dat het echt moet. Er zijn natuurlijk situaties waar het echt moet. Dus ik kijk, eh, ik zal nooit inloggen of gebruik maken van een netwerk waar je geen wachtwoord in moet voeren. Dat je in ieder geval weet dat er in ieder geval beveiliging is en dan gebruik je nog VPN daar bovenop.

X: Waarom gebruik je VPN als je gebruik maakt van een onveilig netwerk?

Y: Omdat, ja, dan komt het beveiligingsstukje om de hoek. Want in principe is het heel onveilig om, eh, ja, onbeveiligde netwerken te gebruiken. Dat klinkt, ja, op zich klinkt dat heel logisch allemaal, maar hoe het werkt is natuurlijk dat verkeer wordt versleuteld. Eh, ja, in ieder geval je gaat ervan uit dan verkeer wordt versleuteld. Maar in principe kun je, als je controle hebt over een stukje netwerk. Dus stel ik ben bij de [example of restaurant], dat is het al bekende voorbeeld, daar zit geen netwerk op, dus je kunt gewoon in zeg maar. Op het moment dat iemand, eh, één controle heeft over het netwerk, dan kan die ook inlezen op jouw verkeer, dat is één. Eh, en ten tweede op het moment dat iemand zich voordoet als hetzelfde netwerk, eh, en controle heeft over dat netwerk, wat logisch is, eh, dan kan iemand jouw verkeer inlezen. En dat, dat kan gevolgen hebben voor, ja, je wilt natuurlijk dat data niet op straat komt te liggen. En je beschermt natuurlijk de, de, de, zowel de, he, dat zijn de drie, de triad van informatiebeveiliging, dat zijn ook de drie doelen, he, confidentiality, integrity en availability. En vooral confidentiality en vertrouwelijkheid, he, dus mag alleen iemand inzien die, he, de data inzien die de data in mag zien. Dat is een principe en de tweede is integriteit, is de data nog steeds de data, die, he, is het juist, is het goed, is het volledig, et cetera, je wilt weten dat niemand aan die data heeft gezeten. En een VPN, maar ook eigenlijk alle beveiliging die überhaupt is, even losstaand van een VPN. Encryptie in het algemeen, die zorgt er gewoon voor, eh, dat, eh, dat, dat die data of die vertrouwelijkheid en integriteit wordt bewaakt.

X: En je zei dat jij dan in publieke ruimtes gebruik maakt van 4G, wat is dan het verschil tussen een onveilig netwerk en 4G?

Y: 4G is een, eh, een op zichzelf al beveiligd, eh, ja, vooral als die je eigen is, he, want dat is gewoon verbonden aan jouw, eh, telefonie, eh, abonnement. En je mobiel zorgt ervoor dat, dat die data, ja, beveiligd is. En dan wordt het naar een satelliet gestuurd of een zendmast of whatever. Eh, en dan weer doorgezet naar het Internet. He, dus er zijn, voor mij is dat, heeft, je kunt niet zeggen dat het volledig veilig is, dat weet je nooit. Alleen de drempel van veiligheid is een stuk hoger. En dus de controle over dat netwerk wordt beter bewaakt dan, eh, die bij de [example of restaurant], bij wijze van spreken. Daar zit ofwel een telecomprovider, ofwel een netwerkprovider, ofwel zelfs een overheid. En dan is ook maar de vraag, oké, waarvoor, he, waarvoor ben je bang. Eh, maar in ieder geval, dat 4G netwerk, die levert in ieder geval een zekere mate van eh, vertrouwen voor mij in ieder geval. Eh, dat ik weet dat, dat, eh, dat daar niet gekke dingen mee gebeuren, eh, op het allerlaagste niveau. Klinkt een beetje paranoid, maar goed.

X: Ja, maar, op wat voor manier is dat dan veiliger?

Y: Oeh. Voor, ja, vanuit perspectief is die vraag?

X: Nou, je zegt, je noemde eerder allemaal beveiliging die er wel is als je gebruik maakt van een VPN en waarom je dan een VPN gebruikt op een onveilig netwerk. Maar, dan zeg je ook als je wel in een publieke ruimte bent, dat je gebruik maakt van 4G.

Y: Ja.

X: Is er dan nog een verschil in het beveiligingsniveau van 4G en VPN?

Y: Ja. Kijk, het ding is dat, hoe je het moet voorstellen is dat het bedrijf heeft natuurlijk gewoon een Internetverbinding. He, dus bijvoorbeeld een, een [example of restaurant], eh, die heeft dan routers of die gebruikt, he, die gebruikt acces points noemen we dat dan, noemen we de routers. Of in ieder geval die gebruikt apparaten, modems, om een connectie te leggen met het Internet. Daar zitten dus tussen jouw, bij wijze van spreken computer als je die gebruikt bij de [example of restaurant], tot aan die modem, nou daar heb je al een stukje, eh, ja, stukje dataverkeer. En dan dat apparaat naar het Internet toe. Nou, moet je voorstellen dat, op het moment dat iemand, eh, dus, he, dat kun je ook zelf zijn, dat kan ik ook zelf zijn. Maar als iemand dus die data, of die apparaten manipuleert die tussen dat dataverkeer inzitten, eh, dan, ja, is dat, ja, dan is dat natuurlijk onveilig. En de vraag is natuurlijk oké, wat maakt het dan minder veilig? Ik denk gewoon dat de drempel, eh, lager is. Dus, ja, je hebt gelijk, we kunnen niet uitgaan, we kunnen niet 100% zeker zijn dat 4G netwerken veilig zijn, daar zitten ook kwetsbaarheden in. Eh, he, dus dat heb je ook altijd. He, je hebt ook, eh, partijen die malafide kunnen zijn of kwade bedoelingen hebben, maar ik vind de drempel, is een stuk, stuk, stukken lager. Dus ik weet in ieder geval dat als ik mijn eigen mobiel gebruik, dan ben ik eigenlijk de persoon tussen de computer en het Internet. In plaats van dat iemand anders dat is. En ik heb controle over in ieder geval het stukje tussen mijn laptop, mijn mobiel en daarna, eh, het Internet. En daar kan iemand tussen zitten, dat klopt.

X: Heb je nog het whiteboard voor je?

Y: Eh, ik heb het whiteboard voor mij, als het goed is. Ja.

X: Zou je dan voor mij kunnen tekenen hoe deze situatie eruitziet als je een VPN-verbinding maakt?

Y: Met. Dus als ik, als ik bijvoorbeeld, eh, VPN, eh, op VPN inlog?

X: Ja.

Y: [\[start drawing 1_1\]](#). Oké. Even kijken. Ik heb alleen een pen, he. O, nee, ik heb meer. Eh, ja, dat kan ik. Dus als ik bijvoorbeeld. O, doet die iets. Wat ik doe, o, dit is wel heel dik. Laten we zeggen, dit is, eh, dit is het netwerk. Kan ik dit verplaatsen of niet. Dit is het interne netwerk. [\[start drawing 1_2\]](#). Dan is er ook nog een, he, wat ik noem, externe netwerk, he, dat hoort nog steeds bij dat bedrijf, he, noem het een DMZ, dat is een heel vaak gebruikte, ja, term voor het publieke, het publieke deel van je netwerk, demilitarized zone. Nou, in principe betekent dat gewoon, nou, het heeft een lagere mate van vertrouwen. [\[start drawing 1_3\]](#). Als jij als endpoint, jij bent, eh, het poppetje. Dat is je endpoint. Eh, even kijken, een poppetje. Nou, dat poppetje, dat wil eigenlijk naar een van de resources die hierin zit. [\[start drawing 1_4\]](#). Dus een server die, ik teken nog een netwerk erbij, want je hebt natuurlijk meerdere segmenten. Je hebt A, B, C, D, als een bedrijf dat goed doet, heb je gewoon meerdere segmenten. En dat, dat zorgt voor extra beveiliging. [\[start drawing 1_5\]](#). Nou, als jij verbinding wil maken, dan zeg je eigenlijk oké, ik wil verbinding maken met een

server die hier staat bijvoorbeeld, dus een ander endpoint. Jammer dat ik geen tekst kan toevoegen, maar dat maakt op zich niet uit.

X: Je kunt tekst toevoegen.

Y: Ja, hier.

X: Als je-

Y: O, dat kan wel, oké, nou. Hoe doe ik dat.

X: Op de pen klikken, en dan staat er een T.

Y: [\[start drawing 1_6\]](#). He, dus dit is DMZ bijvoorbeeld, external. Ik weet niet hoe lang ik hier over mag doen.

X: Zo lang als je wilt.

Y: Oké. Kan ik dit, kan ik dit klikken? Hier eigenlijk, eh. Dus dit is de DMZ, external facing network. Heb je hier nog internal facing network. [\[start drawing 1_7\]](#). Wat ik ga toevoegen is bijvoorbeeld, dit zijn allemaal servers die in de- Laten we zeggen dat dit allemaal endpoints zijn. Hier zitten allemaal endpoints, is allemaal leuk en aardig, maar hier wil je heen. [\[start drawing 1_8\]](#). Dit is je laten we zeggen, je, je target. En wat je doet op het moment dat je VPN aanzet, dit is eigenlijk de, de situatie op het moment dat je, dat je VPN eh, hebt eigenlijk, daar komt het op neer. Dus op het moment dat je het wilt vastleggen, he, dan stuur je eigenlijk een- Dan zorg je voor een, ja, hoe noem je dat, dan stuur je eigenlijk een verzoek. Dus je begint eigenlijk door het eerst te, vast te stellen zeg maar- [\[start drawing 1_9\]](#). En vaak is er wel nog een derde partij, dat is afhankelijk, heel afhankelijk van hoe je het ziet. Dus de inrichting is wel belangrijk, dus ik ga even van een situatie uit. Dus je hebt extern, intern, de VPN-aanbieder heeft dan ook een server waar die mee praat. Wat er zou kunnen gebeuren, dus dat is even hypothetisch he, want het zou ook hier kunnen gebeuren, maar wat ik, even voor het gemak, en ik denk een beetje in [the professional services firm] terms zeg maar. [\[start drawing 1_10\]](#). Wat die doet, op het moment dat jij VPN aan, start zeg maar, dan zeg je hé, doe mij een VPN-verbinding. Dat is eigenlijk een eerste verzoek. Nou, dan komt er een respons, zal ik even in rood doen. [\[start drawing 1_11\]](#). He, en als dat allemaal heen en weer goed is, want eigenlijk zeg je gewoon al bij zo een VPN, want die heb je al op je computer staan, die, dan stuur je al je credentials mee met het verzoek, he, dus dat doe je al meteen, nou dan komt er een connectie hier terug van ja, dat mag. [\[start drawing 1_12\]](#). En vaak gaat dat ook via, zou het zo kunnen, he, dus dat je zegt er is een respons naar een server in de DMZ die weet wie jij bent. [\[start drawing 1_13\]](#). He, en dat dit ding dan weer terugpraat, eh, van hé, het is goed. Of het gaat direct zo, boem, hiernaartoe. [\[start drawing 1_14\]](#). Er is nu ergens een server die dus met jou zeg maar zo een verbinding maakt. Dus dit is dan, een soort van, ja, afhankelijk van, dus je begint in ieder geval deze connectie ofwel deze connectie voor [the professional services firm] bijvoorbeeld het netwerk die, eh, ja, DMZ is. Dus dit kan allebei zijn, dat is even afhankelijk van de situatie. Dan heb je een verbinding met de, dat is zeg maar deze rode lijn. En die rode lijn zorgt er eigenlijk voor dat je dit stuk, kan, eh, overslaan, nou, doet die natuurlijk niet. Maar wat die dan wel doet, en dan gebruik ik hem even in groen bij wijze van spreken, dus de connectie is gelegd. [\[start drawing 1_15\]](#). En dan kun je hier doorheen, he, dan word je toegelaten. En je hebt een IP-adres, dat dit IP-adres is zeg maar, dus hier wil je heen. [\[start drawing 1_16\]](#). En deze zorgt er dan voor dat je deze verbinding kunt maken, he. [\[start drawing 1_17\]](#). En die verbinding zorgt er ook voor, he, dus met alle informatie van dien die je daarbinnen hebt, laten we paars gebruiken, die stuurt het allemaal terug naar hetzelfde punt en die stuurt dat dan weer terug naar jou. En zo heb je eigenlijk verkeer. Dus die groen, groen-paarse, is op het moment dat je een VPN hebt. En zwart-rood is eigenlijk om, om te valideren wie jij bent. En als je een split tunnel gebruikt, eh, dat ook zou kunnen gebeuren, he. Is dat stukje software, dat is afhankelijk van wat het doet, he, want daar hebben we het niet eens over gehad. [\[start drawing 1_18\]](#). Dat stukje, er kan ook een stuk software tussen zitten, dat is dan op je endpoint, die zorgt dat jij gewoon naar een endpoint gaat die helemaal niet in de buurt is van dat netwerk. [\[start drawing 1_19\]](#). Dus dat, dat als jij een split tunnel gebruikt kan dat stukje netwerk eigenlijk gewoon zeggen van nee we gaan niet via [the professional services firm], nee we gaan gewoon naar een publiek stukje netwerk, en dan is het verkeer ook gewoon tussen die twee dingen in. He, dus deze lijnen, die gaan allemaal via dat stukje software. [\[start drawing 1_20\]](#). En ook, kijk naar, ik denk dat ik nu te veel uitleg, maar hier heb je natuurlijk ook weer verbindingen tussen elkaar, dus die kan weer dit netwerk, zo lang deze grenzen dat toelaten. Dus zo zie ik VPN een beetje.

X: Oké. En je maakt dus verbinding via die demilitarized zone met de internal facing network?

Y: Ja, dat is eigenlijk het stukje, ja, je kan, je kan niet direct naar het stukje netwerk. Dat bestaat gewoon niet. Er zit iets tussen, he, er moet gewoon iets zijn wat, eh, wat, eh, wat, ja, eh, de logica heeft zeg maar, de beslissing kan maken of dit goed is of niet zeg maar, of het mag of niet. Dat doet een firewall ook, het zijn eigenlijk een beetje domme apparaten, want ze zeggen van mag dit, ja of nee. Onder welke voorwaarden.

X: Wat zijn dan die segmenten?

Y: Welke segmenten? Deze? Bij internal facing? Wat, eh, wat bedoel je?

X: Wat zijn de functie van die segmenten?

Y: Die segmenten. Ja, dus dat is eigenlijk een extra stukje beveiliging. He, want in principe kun je- Een netwerk kan plat zijn, noemen we dat. Dan kan alles met elkaar praten. [start drawing 1_21]. Dus wat je vaak ziet, gaan we even naar zwart toe, is dat er gewoon meerdere endpoints in een segment zitten. Wat vaak ingeregeld is, dus het is ook afhankelijk van hoe je het inregelt he, het is allemaal afhankelijk van, van, van de architectuur, eh, is dat deze direct met elkaar kunnen praten. Dus, dat er altijd verbinding gemaakt kan worden tussen al deze endpoints binnen het segment. [start drawing 1_22]. Maar he, dat, eh, even kijken, dat bijvoorbeeld dit is niet, niet bij voorbaat mogelijk. He, dat is alleen mogelijk als zeg maar, een firewall dit toelaat. Dus stel een endpoint zegt ik wil praten met dit apparaat en er staat nergens- En je hebt besloten om segmenten te nemen, eh, en er wordt niet specifiek gezegd dat punt A met punt B mag praten, dan komt dat ook niet tot stand. En zo voeg je eigenlijk een beetje extra lagen van beveiliging toe. Dus wat ik hier teken is eigenlijk een soort van eh, multi-tier architecture. Is wat, eh, eerst bijvoorbeeld een client, Internet facing stuk hebt, dan heb je een webserver bijvoorbeeld, he, dus de meeste website zijn zo ingericht. Dan heb je een, eh, website en die website heeft weer een database erachter. Alleen wat je niet wilt is dat eh, een endpoint direct praat met een database, want dan heb je echt, dan heb je, ja, het heet niet voor niets informatiebeveiliging. Nou waar staat informatie, die staat natuurlijk in databases. Eh, en als je direct toegang kan hebben tot de database kan je aardig wat schade aandoen. He, dus je wilt zo veel mogelijk stukken beveiliging inrichten voordat je bij die databases aankomt. He, en wat ook vaak gebeurt is dat iemand binnen het gebruikersnetwerk direct wel, he, wel direct toegang heeft tot die database, maar iemand vanuit een, een external facing netwerk dat niet kan. He, dat is heel afhankelijk van hoe dat is ingericht. Dus daar zijn- Deze grenzen worden allemaal bepaald door middel van regels of, eh, door middel van, eh, van, ja, omgevingsfactoren. Dus [example of softwareprovider] is daar heel erg mee bezig, is dat eh, he, zero trust noemen ze dat. Dus als ik het zo teken, dan is er wel een mate van vertrouwen. Als je eenmaal hier bent, dan mag je hiernaartoe, dat is een mate van vertrouwen. He, je voegt dan minder vertrouwen toe op het moment dat je meerdere segmenten toevoegt. En je hebt al helemaal geen vertrouwen op het moment dat jij een medewerker bent die in het interne netwerk zit. Dus bijvoorbeeld, [0:47:51 until 0:48:18 has been omitted] en je hebt zero trust, he, het model zero trust, dan, eh, kijken ze eerst naar oké, wie ben jij, ben jij ingelogd, heb jij de juiste, eh, permissies, bla bla bla. Je kunt nog verder gaan door te zeggen ja, log jij normaal gesproken op dit tijdstip met dit apparaat in, he, dat zijn die omgevingsfactoren die je kan inbouwen, en dat is iets waar [example of softwareprovider] heel erg sterk mee bezig is, omdat zij natuurlijk, ja, de grootste aanbieder zijn van, van, eh, ja, hoe heet dat, werkstations. [0:48:53 until 0:48:55 has been omitted], he, dus zij kunnen ook via software kunnen ze dingen toevoegen waardoor ja, per netwerksegment, per vierkantje hier kan worden bepaald, oké, op basis van welke van deze factoren mag iemand worden toegelaten. En dat zie je dus ook steeds meer met dat single sign-on verhaal, he, VPN speelt een heel grote rol in single sign-on, en eh, dat het lijkt alsof je alles mag, maar daar zit heel veel complexiteit achter en heel veel, ja, management achter. En dat zijn eigenlijk die stukken, he, dus stel dit is [een interne pagina], die mag je alleen onder bepaalde voorwaarden inzien.

X: Oké. En hoe wordt bepaald wat je in mag zien?

Y: Dat is allemaal configuratie. He, dus iemand met de rol, ja, noem het manager, noem het eh, supervisor, noem het lead, die heeft de verantwoordelijkheid gekregen om het netwerk in te richten. He, dat is vaak een, eh, nou ja, dat is vaak geen architect. Een architect bepaald eigenlijk meer, he, wat de toekomstplannen zijn. En op welke principes de plannen zijn gebaseerd, eh, en eh, eh, hoe alles verbonden moet worden. Maar uiteindelijk is er ook een soort van lopend proces, he, dus iemand heeft management, eh, ja, power

zeg maar om te bepalen op basis van welke, eh, voorwaarden dat wordt, eh, toegang wordt gegeven. Dus iemand is wel in de lead, er zal ook een security, eh, of een chief information security officer zijn binnen [the professional services firm], die dus bepaalt hoe, eh, hoe dat, eh, hoe dat moet verlopen. He, dat is echt een mensenstukje. Dus je kunt niet alles met techniek afdekken. Je kunt veel met techniek afdekken, zeker tegenwoordig. En zeker nu de grenzen van he, diensten, eh, met de cloud weet je wel, dat die overal staan, overal en nergens weer in Nederland staan. He, dus hoe krijg je meer controle over, he, dus niet alleen dit stukje aan de rechterkant, maar ook dat paarse bolletje, dat is niet een ding, dat zijn meerdere dingen. Dus, eh, makkelijke voorbeelden zijn natuurlijk [social media platform], ja, andere social media, maar wat als je [cloud software] gebruikt, wat als je een bestaande oplossing gebruikt, [cloud software] gebruikt, ja, dat staat niet altijd in het interne netwerk van [the professional services firm]. Dus het is vaak goedkoper, en eh, ja, je kunt gewoon van schaalvoordelen genieten op het moment dat jij een Software as a Service gebruikt, he. Met, eh, de, de, het inleveren van beveiliging die daarbij komt kijken.

X: En wat is de invloed van een VPN-verbinding op jouw computerbeveiliging?

Y: Sorry, kun je de vraag herhalen?

X: Ja. Wat is de invloed van een VPN-verbinding op jouw computerbeveiliging?

Y: Wat is de invloed ervan? Hm. Ik weet niet of ik, of ik, of ik die vraag kan beantwoorden, he, wat is de invloed van- Kan je die anders stellen?

X: Heeft een VPN-verbinding invloed op jouw computerbeveiliging?

Y: Ja, dat heeft zeker invloed op mijn computerbeveiliging. Dus eigenlijk alles wat ik nu genoemd heb, vooral vanuit vertrouwelijkheid en integriteit weet ik dat, eh, dat, eh, in ieder geval, ik heb het niet vastgesteld, maar dat is ook nog belangrijk. Eh, het bedrijf heeft gekozen voor deze oplossing, eh, en het bedrijf heeft ook vertrouwelijkheid en integriteit hoog in het vaandel. Eh, dus ik denk, denk dat dat zeer belangrijk is om te gebruiken, maar niet voor alles. He, dus ik zie het niet als de oplossing voor alle computerbeveiliging, er is zo veel meer in computerbeveiliging. He, malware kan ook via een VPN verlopen, maar, eh, ook heel veel impact hebben op jouw computerbeveiliging. He, het is dus een van de tools [0:53:25 until 0:53:30 has been omitted] voor informatiebeveiliging.

X: En met wat voor een digitale dreiging heb jij op een normale dag te maken?

Y: Persoonlijk bedoel je?

X: Ja.

Y: Ik vind dreiging wel echt een heel groot woord. Eh, bij dreiging denk ik gelijk aan [0:53:51 until 0:53:54 has been omitted]. Eh, ja, wat ik zie langskomen is bijvoorbeeld spam, met, eh, ja, advertenties erin of weet ik veel wat erin. Of links die leiden tot eh, malafide websites. Ja, phishing is natuurlijk echt een ding. Eh, ik denk dat dat vanuit een persoonlijk perspectief, of bedoel je vanuit een klant perspectief? Wat ik eh, ik zie-

X: Ja, of vanuit [the professional services firm] perspectief?

Y: Ja, kijk, ik kan alleen maar gissen, wat daadwerkelijke dreigingen zijn, worden niet door mij gemeten, die worden niet door mij ingezien. Ik krijg ook geen bericht van oké, jij bent slachtoffer geweest van. He, dus heel veel wordt natuurlijk al uitgefilterd door e-mail systemen of door eh, ja andere dingen van [the professional services firm]. [The professional services firm] heeft natuurlijk heel veel software die ons helpen, om, om veiliger te zijn. Dus, ja, ik kan eigenlijk geen goed beeld geven van de dreigingen die ik op dagelijkse basis zie. Behalve dan dat ik kan raden wat het is. He, als je, als je zelf een server hebt, eh, en die zet je op het Internet en die zet je op je external facing netwerk, ja, geheid dat jij constant rare verzoeken krijgt. He, dus daar wordt wel constant scanning op gedaan, op het moment dat jij publiek beschikbaar bent op het Internet. He, want dat is natuurlijk geen ingang voor eh, aanvallers om op het netwerk te komen. Daar zie je het wel heel duidelijk. Als je het eenmaal open zet voor het Internet, wat er allemaal voor gespuist langskomt om te kijken hoe het allemaal zit.

X: En verandert de soort dreiging dan door een VPN-verbinding?

Y: Ik denk niet dat de soort dreiging verandert, maar dat je de maatregelen in ieder geval neemt om de dreiging af te dekken. Dus je hebt onveilig, he, verkeer over het Internet heen. Ja dat, daar geef je iets meer zekerheid over. He, dat jij kan Internetbankieren bijvoorbeeld is toch, ja, fijn als je een VPN-verbinding gebruikt, maar dat hoeft niet. Kijk, als ik [the professional services firm] gebruik voor Internet bankieren, eh, ja, dat doe ik dus niet. Maar dan weet ik ook dat de data gaat gewoon via [the professional services

firm] resources, nou dat wil ik ook niet. He, dus er zit ook een stukje zelfbescherming in. He, maar, eh, kijk op persoonlijke basis gebruik ik geen VPN voor Internetbankieren. Ik vertrouw wel op HTTPS protocollen, he, TLS, om een beveiligde verbinding te maken met mijn bank. Daar gebruik ik geen VPN voor.

X: Dit ging dan over digitale dreiging. Maar heb jij ook nog te maken met een sociale dreiging?

Y: Sociale dreiging, wat bedoel je met sociale dreiging?

X: Eigenlijk alles wat niet digitaal is.

Y: Eh. Wat is niet digitaal tegenwoordig.

X: Eerder bijvoorbeeld had je het over Internet bankieren en dergelijke. Dus dat is dan allemaal duidelijk digitaal, maar zit hier ook nog een sociaal aspect aan?

Y: Eh, ja, ik kan die twee dingen bijna niet los van elkaar zien tegenwoordig. He, dus, kijk, als je het hebt over bijvoorbeeld advertenties ontvangen, of als je het hebt over de overheid kan eh, inzien op wat jij doet, of wat dan ook, ja, die impact is er zeker. Als je daar om drukt maakt, dan moet je andere maatregelen nemen.

X: Heeft een VPN-verbinding hier invloed op?

Y: Eh, nee. Helemaal niet. Ik heb juist het idee dat ik ook een beetje gevaar loop als ik een VPN-verbinding gebruik. He, want ja, je dekt misschien wat verkeer af. Het gaat nog steeds via je VPN-verbinding, he, daar moet je maar vertrouwen in hebben, dat is een. Eh, het tweede is, ja, als een overheid op, he, dat is, wat mij betreft is dat het allerhoogste niveau van, eh, van persoonlijke dreiging, eh, zijn overheden. Nou, ik vertrouw de overheid op zich wel, maar ik weet ook wel waartoe ze in staat zijn. En daar gaat een VPN niet bij helpen. He, als zij willen dat jouw VPN-verbinder of aanbieder toegang geeft tot data, dan vraag ik mij af of zij hun poot stijf houden. Ik geloof dat eigenlijk niet eens.

X: Biedt een VPN dan in enige vorm wel bescherming? Want je zegt als ze data vrijgeven, wat bedoel je daarmee?

Y: Nou ja, kijk, een VPN-verbinding heeft, he, zo lang zij hun werk doen, zo lang zij doen wat zij beloven, dan ben je veilig. Voor in ieder geval je netwerk, eh, je verkeer. Dus hetgeen wat jij verstuurt tussen A en B en weer terugkrijgt van punt B naar A. Eh, ja dus dat is de bescherming die ze bieden. Eh, maar, zoals alles, nou alles, veel in beveiliging is het toch heel erg afhankelijk van, eh, het vertrouwen dat je hebt met de aanbieder. Dus als de aanbieder, kijk, als jij een gratis VPN gaat gebruiken, nou dan, dan doe je dat waarschijnlijk niet omdat je echt iets beschermt wilt hebben. Dan doe je dat waarschijnlijk om binnen [company] Amerikaanse series te kunnen kijken of eh, een ander land. He, dat is de kracht van VPN natuurlijk ook. Je maakt verbinding met eh, een ander netwerk of een ander apparaat in een andere regio, he, zodat je kunt doen alsof je in Amerika zit. He, dus als je zegt ik ben privacy aware en ik wil eh, eh, he, ik wil via andere punten connecten, zodat ze in ieder geval een, of twee, of drie stapjes meer moeten nemen zodat ze bij mij komen, eh, dat kan. Maar dan zou ik eerder een ander mechanisme gebruiken.

X: Op wat voor manier draagt een VPN bij aan privacy?

Y: Nou het draagt zeker bij aan privacy tot op zekere hoogte. He, dus het zorgt er in ieder geval voor dat als jij bijvoorbeeld eh, veel eh, wil inloggen, eh, in ieder geval gewoon browsed of Internet gebruikt, weet ik veel wat, en eh, dan, dan kunnen ze niet direct zien wie jij was. Dus zij zien dan niet een IP-adres, dat, dat kan op een server namelijk, dat wordt gewoon allemaal gelogd. He, dat wordt gewoon, ja, keihard wordt daar gewoon opgeschreven wie toegang probeert te krijgen op jouw eh, resources. He, als je technisch aangelegd bent, kun je de logs inzien en dan kun je zien dat jij of ik dat gedaan heeft. Niet op persoonlijke basis, maar wel jouw computer. Dus in ieder geval kun je heel erg pinpointen. Kijk als jij in een huishouden zit met, eh, vier personen en je weet het IP-adres, ja, dan kun je dus met redelijke mate van zekerheid vaststellen wie het is. Tot op vier personen. Je kunt natuurlijk gasten hebben, familieleden, wat dan ook, maar daar gaat het niet om. En, eh, een VPN kan daar hulp bij bieden om, om, om in ieder geval te doen alsof je vanuit een ander punt komt. He, want zij zien natuurlijk het laatste punt dat probeert, geprobeerd heeft te connecten. En natuurlijk gaat dat ook altijd- Kijk, hoe het technisch werkt, je hebt natuurlijk hops he, dus tussen jou en mij zitten denk ik minstens vier hops. Dus ik, eh, ga naar mijn, eh, een kastje hier en het kastje hier gaat naar het Internet, en dat Internet dat wordt een beetje gescrambled, of er komen meerdere dingen bij elkaar en dat komt weer bij jouw Internetprovider terecht en dat komt weer bij jouw modem terecht. Dus uiteindelijk zitten er best wel wat hopjes tussen. En wat jij dan, stel je zou onze

verbinding inzien, dan zie je een paar laatste, he, dat laatste stapje zie je. Maar wat je ook zelf kan doen is ping trace. He, dat is gewoon dat jij als pakketje volgt. Dus dan zie je precies welke hops ertussen zitten, met uitzondering van een paar private die ertussen zitten. Dan zie je dus ook bijvoorbeeld, ja, dat je zes stappen hebt genomen voordat je bij eh, je eindpunt eh, komt. Het is niet allemaal- Ik zeg maar- Ik simplificeer heel veel dingen hoor, er zit toch best wel wat complexiteit tussen. Dus, ja, eh, helpt het echt met privacy, ligt eraan hoe veel vraagtekens je hebt. Als je veel vraagtekens hebt, dan is het vaak nee. In de vorm van hoeveel kritische vragen stel je voordat jij tevreden bent met je privacy. Als jij een vraag hebt, dan ja. Als jij vijftien vragen hebt, dan is het hoogstwaarschijnlijk dat die niet gaat bieden wat jij wilt.

X: En je zegt het laatste punt die ziet dat dan, wat ziet die?

Y: Sorry, kun je dat herhalen?

X: Ja. Je zei dat je springt naar allemaal hops, en het laatste punt ziet dan alleen het laatste, of alleen het een na laatste punt. Wat ziet dat laatste punt?

Y: Wat dat laatste punt is?

X: Nee, zeg maar, jou naar mij, dan gaat het via allemaal punten-

Y: Ja.

X: En met een VPN-verbinding zie je alleen het laatste punt, zei je.

Y: Nee, nee, dan verander je het laatste punt natuurlijk. He, dan in je log-

X: En wat verander je dan?

Y: Ja, bijvoorbeeld je locatie, of je server, of wat, eh, je verandert niets aan de feitelijkheid, alleen eh, waarom het ook zo traag is, is dat er hops tussen zitten. He, er zitten dus dingen, als we weer teruggaan naar de tekening bijvoorbeeld, dan eh, is er hoogstwaarschijnlijk deze externe aanbieder of wat dan ook, dan, he, is dan een stap tussen, he, tussen jou, het moet eerst naar het Internet komen, dus jouw modem, het Internet, dan naar de externe VPN-aanbieder, die heeft waarschijnlijk ook allemaal servers, he, en die zorgt ervoor dat je weer naar DMZ gaat, en alles gaat weer terug, he. Dus alles stapjes worden teruggenomen, omdat elk pakketje wordt eigenlijk uitgepakt, he, dus eh, hm, het Internetprotocol is opgebouwd uit meerdere lagen zeg maar, segmenten, zeven volgens mij in totaal. Nou, elk stukje zorgt eh, die verpakt, eh, dat vorige stukje en voegt een stukje, eh, toe. Dus wat er gebeurt is dat steeds meer data wordt toegevoegd aan een pakketje. En dat pakketje wordt, eh, bij het doorsturen wordt die dus weer ja, krijgt het weer een afzender en een, eh, target. Target blijft redelijk hetzelfde, omdat je altijd weet waar je uiteindelijk naar toe wilt. Er zit er eentje tussen, maar de, maar als die uitpakt dan ziet die, oké, hij kwam van dit punt, dus daar moet die ook weer naar toe. He, en zo onthoud je de hele tijd, eh, he, dus er hoeven geen actieve verbindingen te blijven bestaan om die connectie te laten, eh, leven zeg maar. Dus die data zit eigenlijk in het pakketje. Dus doordat de data in het pakketje zit, weet hetgeen wat het ontvangt of verwerkt of wat dan ook, waar die weer naar toe moet ofwel naar teruggestuurd moet worden.

X: En we hadden het eerder dan over digitale en sociale dreigingen en je noemde het al kort even, maar wie of wat is de aanvaller die achter een eventuele dreiging zit?

Y: Hm, wat is zijn motief bedoel je? Ik hoorde niet helemaal het laatste stukje.

X: Wie of wat is de aanvaller die achter een dreiging zit?

Y: Ja, dat is heel afhankelijk van eh, waar je bent in de wereld. Ik denk overal eigenlijk wel, maar eh, ja, je hebt gewoon verschillende vormen van, van, ja, actoren zagezegd, en, eh, die kunnen heel erg verschillen. Het kan je buurman zijn, maar het kan ook een, een kwaadwillend bedrijf zijn. Of het kan ook een bedrijf zijn die geld wil verdienen over jouw rug heen, denk aan [social media platform] bijvoorbeeld. Eh, maar het kan ook een lokale of eh, een wat grotere overheid zijn. Eh, of een criminele bende. Dus dat zijn echt verschillende vormen die, die dreiging kunnen geven.

X: Verandert de soort aanvaller ook door gebruik te maken van een VPN-verbinding?

Y: Hm, nou de soort verandert niet, maar ik denk dat eh, eh, dat het niveau, he, de kennis en kunde van de aanvaller, moet hoger zijn. En dat, dat geldt denk ik voor alles binnen informatiebeveiliging, alle maatregelen die je treft, verhogen de drempel voor een aanvaller om het effectief uit te voeren. He, en hoe moeilijker je het maakt, hoe meer middelen je nodig hebt, hoe meer tijd je nodig hebt en de kunde die je nodig hebt om een aanval uit te voeren.

X: Kan je daar een voorbeeld van geven?

Y: Eh, nou ja, je, stel je zou dus, en ik ga weer terug naar het [example of restaurant] voorbeeld, voor het gemak, omdat ook VPN als onderwerp hebben, eh, stel je zou geen VPN gebruiken en je maakt gewoon direct gebruik van het netwerk van [example of restaurant] dat onbeveiligd is, ja, dan is het voor iedereen mogelijk om jouw data in te zien. Dat kan ik, ik loop nu naar de [example of restaurant] ik kan dat. En ik kan jou dat uitleggen in een uur en dan kun je dat. Niet dat ik jou wil aansporen, dat zeg ik niet. Eh, maar het is redelijk makkelijk. Gebruik je VPN, he, dan heb je die dreiging, dan heb je die actoren al uit het veld. Nou, heb je echt goede mensen die snappen hoe het Internet werkt, ja, dan wordt het al, dan is je bescherming toch wel iets minder. He, en stel je zou vanuit je thuisnetwerk gebruik maken van [the VPN of the professional services firm] om je diensten, eh, ja, om het Internet te gebruiken. Ja, dan heb je toch wel echt meer, meer kennis en kunde nodig, kijk en misschien wel meer macht. He, dus wat heb je dan nodig? Misschien een kwetsbaarheid in de VPN-oplossing, of, of toegang bij de VPN-aanbieder, of weet ik veel wat. Ja, daar heb je echt wel wat macht voor nodig. En dat zijn wat mij betreft vaak de, de nationale overheden die dat eh, die dat gewoon kunnen. Zij kunnen ons nu ook afluisteren denk ik. Eh, ja, dat denk ik qua mogelijkheid is dat zekerheid. Of ze dat doen, dat is weer een andere vraag.

X: En wat zou de motivatie van een aanvaller kunnen zijn?

Y: Hm. Ja, dat, ik denk dat dat verschillend is. Als jij- Je hebt natuurlijk persoonlijk motief, he, dus dat jij, ja, stel je bent een publiek figuur en iemand wilt jou eh, iets aandoen. Of je hoeft niet eens- Iemand wilt jou gewoon iets aandoen, dan is dat al een motief op zichzelf denk ik. Als je buurman boos is en die weet iets van computers af, dan zou die jou best kunnen targeten. Eh, dat geldt voor een overheid, als die jou in de smiezen wilt houden of wat dan ook, dan eh, dan, dan kan die jou targeten. Eh, als een criminele organisatie iets in jou ziet, qua geld, he, dat kan ook, dat is vaak meer een wat bredere approach, dan ben jij waarschijnlijk niet de enige, ja, dan ben jij gewoon of makkelijk te vinden, dat kan, of je hebt gewoon- Ze hebben gewoon een bepaalde specifieke interesse. Bijvoorbeeld als je directeur bent van een bedrijf met macht over geldstromen bijvoorbeeld.

X: En vanuit het perspectief van [the professional services firm]?

Y: Wat zei je?

X: Als je denkt vanuit het perspectief van [the professional services firm].

Y: Ja, dat kunnen ook heel veel dingen zijn, bedrijfsspionage bijvoorbeeld. Eh, concurrenten, eh, overheden willen misschien in de gaten houden wat je afsprekt met een klant. Eh, of je, ja, iemand waar je zaken mee doet. Ik denk dat er wel veel dingen zijn. Ik denk dat we niet helemaal onze zeg maar, dat, eh, dat, dat je helemaal de beveiligingen naar beneden moet stellen omdat je denkt dat dat niet gaat gebeuren.

X: Wat zou de impact van een aanval kunnen zijn?

Y: De impact van een aanval. Hebben we het dan over [the professional services firm] specifiek?

X: Ja.

Y: Ik denk, het is echt reputatie in dit geval. Zeg maar, feitelijk, dus stel iemand he, een derde partij leest of ziet iets gevoelig van een ja, van [the professional services firm], op zichzelf is dat niet zo boeiend. Eh, alleen wat je wilt voorkomen is dat er dingen uitlekken die ervoor zorgen dat je geen bedrijfsvoering meer kan doen. He, en we gaan er natuurlijk altijd vanuit dat, dat, he, we doen gewoon altijd iets goeds, he, we gaan er gewoon vanuit dat wij altijd goed handelen, he, maar wat voor de ene partij goed handelen is, is voor de andere partij misschien helemaal niet goed. He, zo zijn er natuurlijk veel belangen die spelen. He, en op het moment dat jij [1:13:40 until 1:13:49 has been omitted]. En aan de andere kant, als een overheid eh, ziet dat er iets, ja, niet volgens, eh, eh, ja, een bepaalde interesse heeft zeg maar, je wilt natuurlijk altijd spelen volgens het boekje en dat soort dingen, dus dat doe je dan ook. Maar eh, stel iets komt op straat wat, eh, ja, misschien niet helemaal eh, goed is voor hun, naar hun mening, dan kan dat ook gevolgen hebben voor de licenties die je hebt, he, dat je je bedrijfsvoering niet mag doen. En dat is natuurlijk, he, op het moment dat er iets fout gaat, maar ook denk ik dingen die binnen de regels goed zijn en niet binnen de publieke opinie vallen bijvoorbeeld, weet je, [1:14:40 until 1:14:53 has been omitted]. He, en ook al blijven we binnen de boekjes van de wet, we overtreden daarmee soms helemaal geen wetten, kan dat soms nog steeds verkeerd vallen bij de publieke opinie. En dat soort dingen wil je niet op straat hebben liggen.

X: Is dit ook wat je bedoelde met gevoelige informatie?

Y: Ja, absoluut, ja. Ja, en kijk ik heb het niet eens over de GDPR he, ik heb het echt eigenlijk alleen over puur confidential informatie. Tussen ons en de klant. He, we hebben ook gewoon, eh, onze verplichtingen om de, de vertrouwelijkheid te bewaken.

X: En je zei er eerder al iets over, maar hoe veilig is een VPN-verbinding?

Y: Eh, een VPN-verbinding is zo veilig als je het maakt. En dat is een heel vaag antwoord, maar in principe hangt het er heel erg van af hoe je hem inricht. Hoe richt je hem in en wat is punt A, wat is punt B, welke, eh, eh, protocollen gebruik je, welk beveiligingsalgoritme gebruik je, en heb je vertrouwen in je aanbieder, eh, waar heeft de aanbieder zijn server staan, wie heeft er allemaal toegang toe, he, wat, en dat hele stukje vertrouwen is heel belangrijk hierin. Is, he, wie heeft controle over het bedrijf, eh, ja, wie is de uiteindelijke eigenaar, wie, ja, hoe hebben zij hun interne beveiligingsmaatregelen getroffen. Er zijn heel veel vragen die je moet beantwoorden en waar je due diligence op moet doen, voordat je besluit op welke VPN je gaat gebruiken. En veel van dat soort IT-beslissingen op zichzelf zijn niet zo moeilijk. He, zijnde, we gaan een VPN gebruiken, maar daadwerkelijk het idee hebben dat je, dat je iets goed, he, neemt of koopt, daar gaat best wel wat werk, moeite en due diligence inzitten.

X: Als je deze onveiligheden opnoemt, veranderen jouw handelingen dan ook daardoor?

Y: Ik heb hier natuurlijk minder directe invloed op he, omdat [the professional services firm] als groot bedrijf hebben zij gekozen voor een bepaalde oplossing, om welke redenen dan ook. Eh, en hierbij ga ik er echt vanuit dat [the professional services firm] de juiste stappen heeft genomen om een partner in de hand te nemen. Eh, mijn handelingen veranderen daarom niet, maar ik heb natuurlijk zelf wel een soort van basis, basisprincipes van privacy en security en zeker als security professional, he, noem het maar zo, dan, ja, dan, dan, weet je in ieder geval hoe het in elkaar zit. En kun je niet blindelings vertrouwen op eh, keuzes die gemaakt zijn. He, dus ik zou niet 100% vertrouwen op keuzes die [the professional services firm] altijd maakt.

X: Als je dan basismaatregelen treft, kan je een voorbeeld geven van deze maatregelen?

Y: Die ik tref?

X: Ja.

Y: Ja, ik scheid bijvoorbeeld privé en werk scheid ik echt. Dus ik, ik gebruik geen, ik heb bepaalde apparaten voor bepaalde doeleinden, dat klinkt heel panisch, maar goed, ik ken nog, ik ken nog wel gevallen waarin mensen bijvoorbeeld een hele operating system in een USB-stick met zich meedragen, zodat er geen hardware bij betrokken is, nou dat vind ik te ver gaan. Eh, en ja ik kijk wel uit, he, in dat opzicht, ik weet in ieder geval wat, eh, wat ik wel en niet met de apparaten moet doen van [the professional services firm]. He, wetende ook bijvoorbeeld dat je e-mailbox eh, ten alle tijden kan worden geconfisqueerd, maar ook worden ingezien door alles en iedereen, nou, niet alles en iedereen, maar in ieder geval- Je zou denken van niet, maar iemand heeft natuurlijk toegang tot jouw e-mailbox, dus als er, dus als iemand zeg maar de wil heeft om erin te kijken, dan kan die dat, he, dat moet je altijd weten. En dat is, dat is natuurlijk van belang om in je achterhoofd te houden. Dus dat jij niet dingen erin zet waarvan jij denkt oké, dat hoeft mijn bedrijf niet te weten. Persoonlijke zaken moeten dus weggelaten worden uit je professionele e-mailbox. Zelfde voor [Softwareprovider], he, zelfde voor [Softwareprovider], maar je verlaagt natuurlijk het risico door dingen te spreiden. Dus niet al je gegevens op straat liggen op het moment dat een e-mailbox wordt gecompromitteerd.

X: Zijn er nog andere maatregelen die jij treft?

Y: Hm, ja, ligt eraan waarvoor. He, wat is het doel, weet je wel.

X: Ja, maatregelen die jij treft vanwege eventuele onveiligheden in de VPN.

Y: Nee, ik tref verder geen eh, maatregelen.

X: Dan waren dit tot zo ver mijn vragen. Heb jij nog iets wat niet ter sprake is gekomen over VPN?

Y: Oeh. Ik heb het idee dat ik heel veel heb gezegd over VPN. Ik denk jij ook. Eh, ik heb verder niet echt vragen.

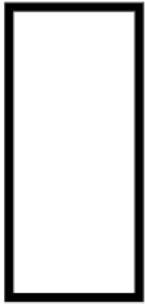


Figure C.1.1: Drawing 1_1

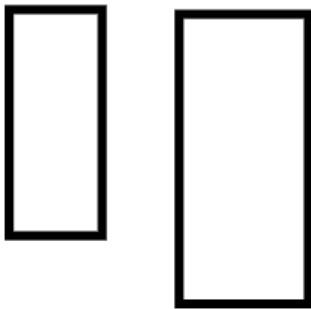


Figure C.1.2: Drawing 1_2

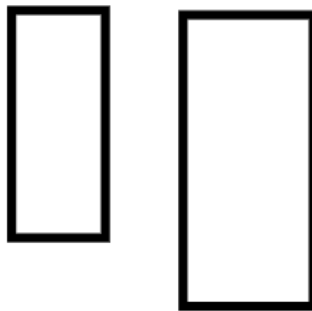


Figure C.1.3: Drawing 1_3

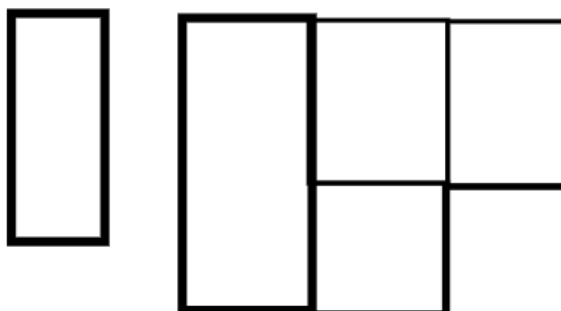


Figure C.1.4: Drawing 1_4

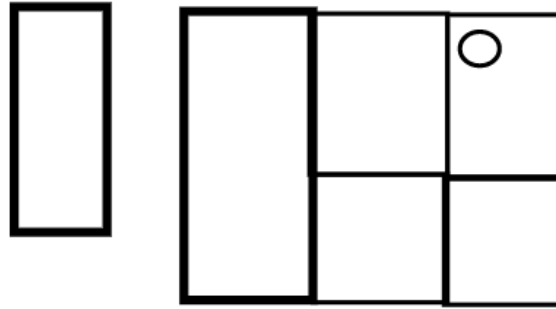


Figure C.1.5: Drawing 1_5



DMZ (external facing network)

Internal facing network

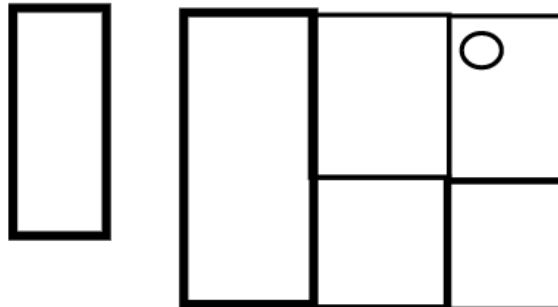


Figure C.1.6: Drawing 1_6



DMZ (external facing network)

Internal facing network

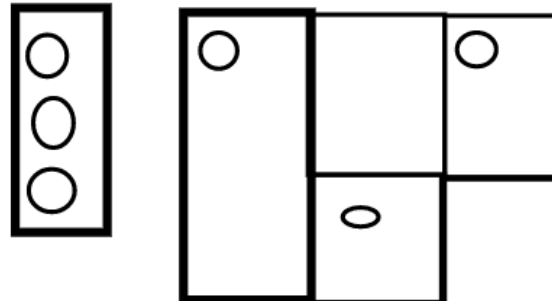


Figure C.1.7: Drawing 1_7



DMZ (external facing network)

Internal facing network

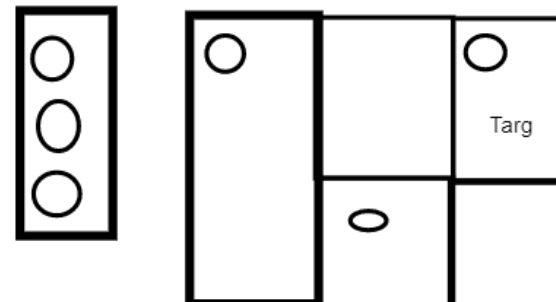


Figure C.1.8: Drawing 1_8

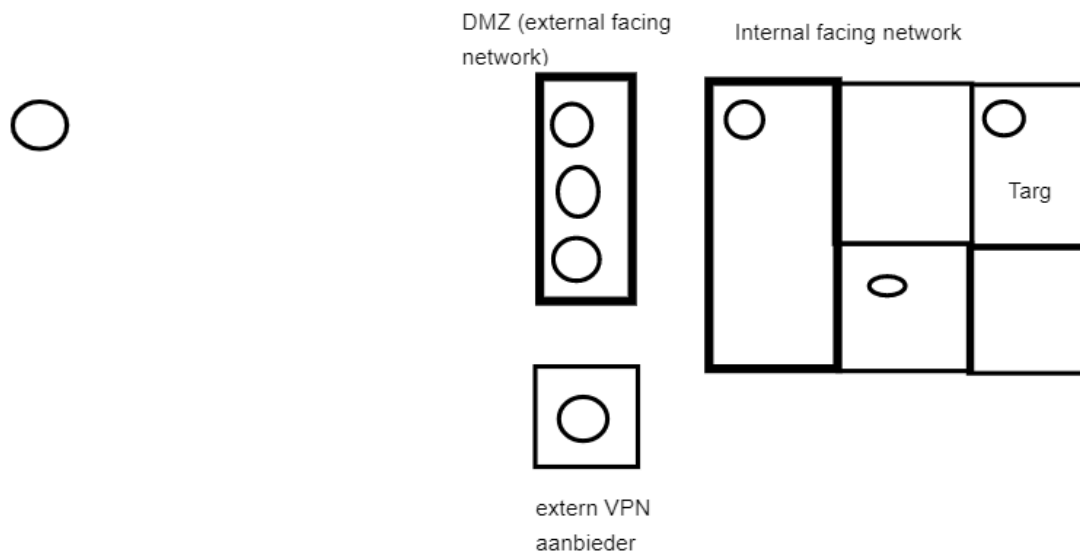


Figure C.1.9: Drawing 1_9

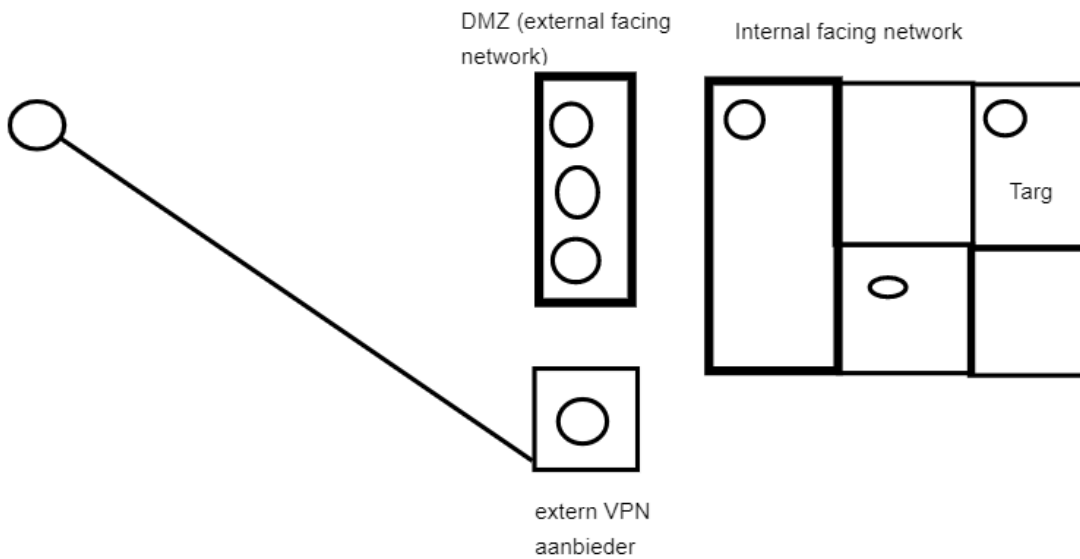


Figure C.1.10: Drawing 1_10

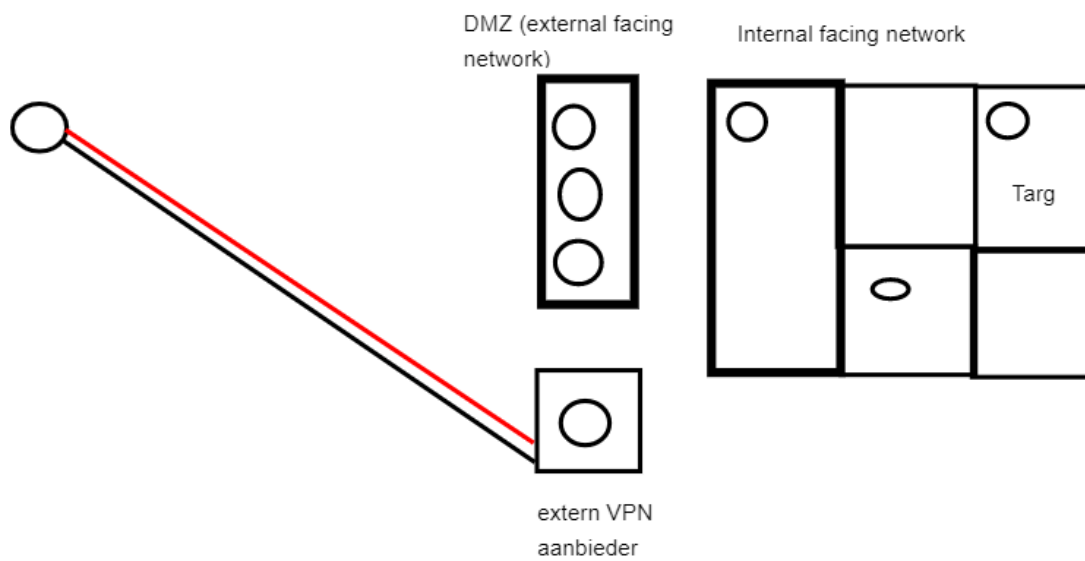


Figure C.1.12: Drawing 1_12

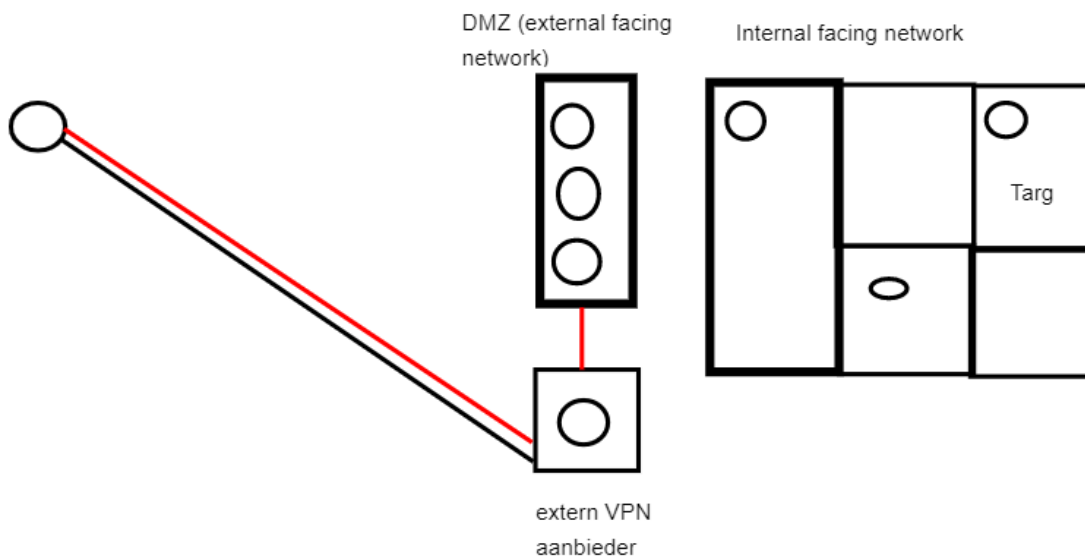


Figure C.1.13: Drawing 1_13

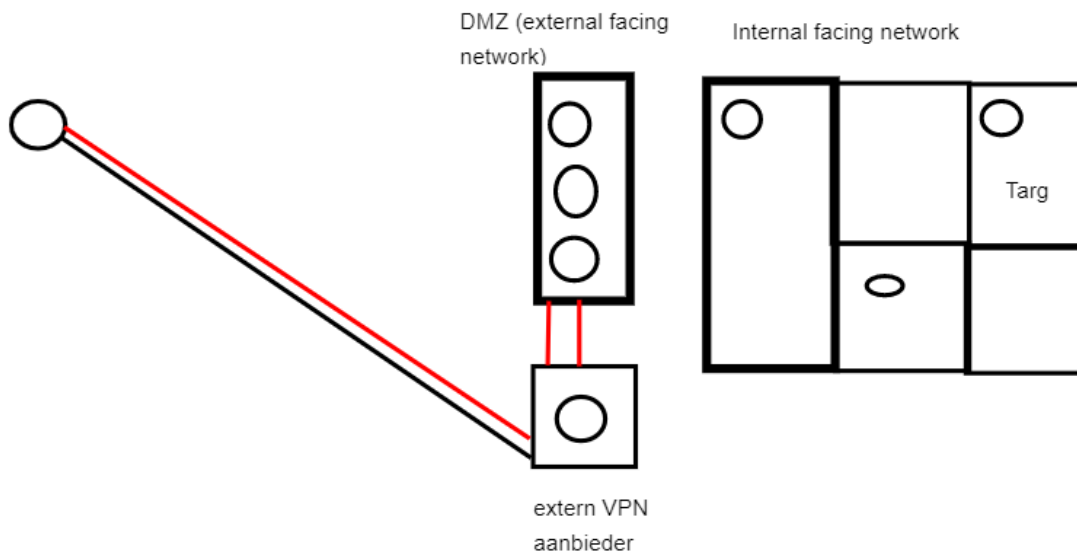


Figure C.1.14: Drawing 1_14

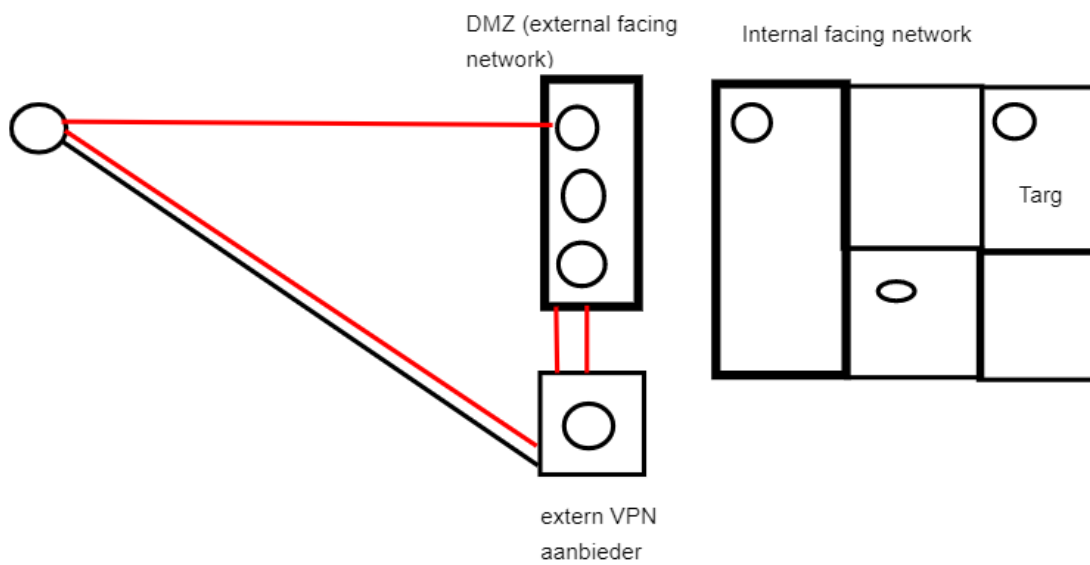


Figure C.1.15: Drawing 1_15

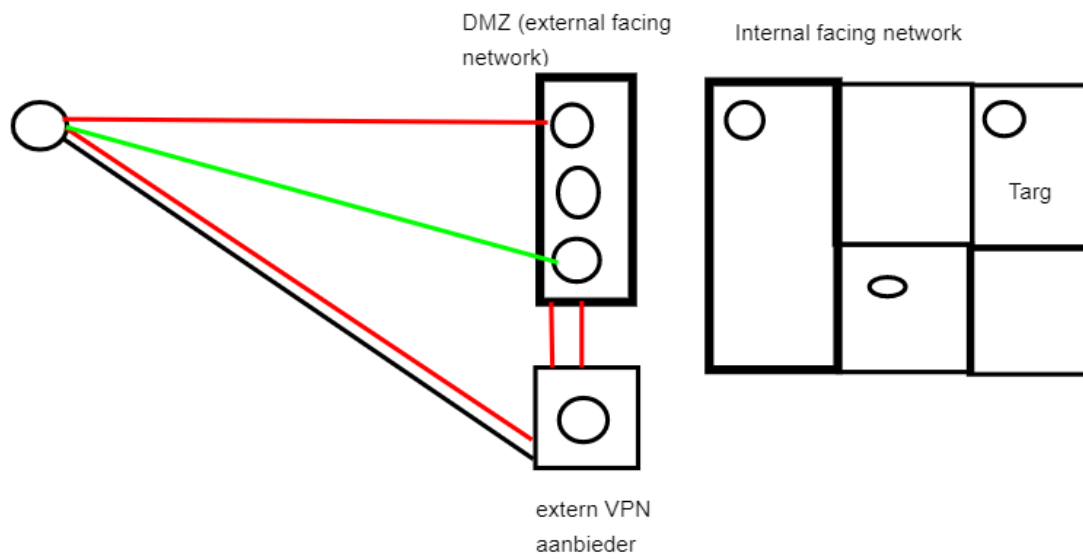


Figure C.1.16: Drawing 1_16

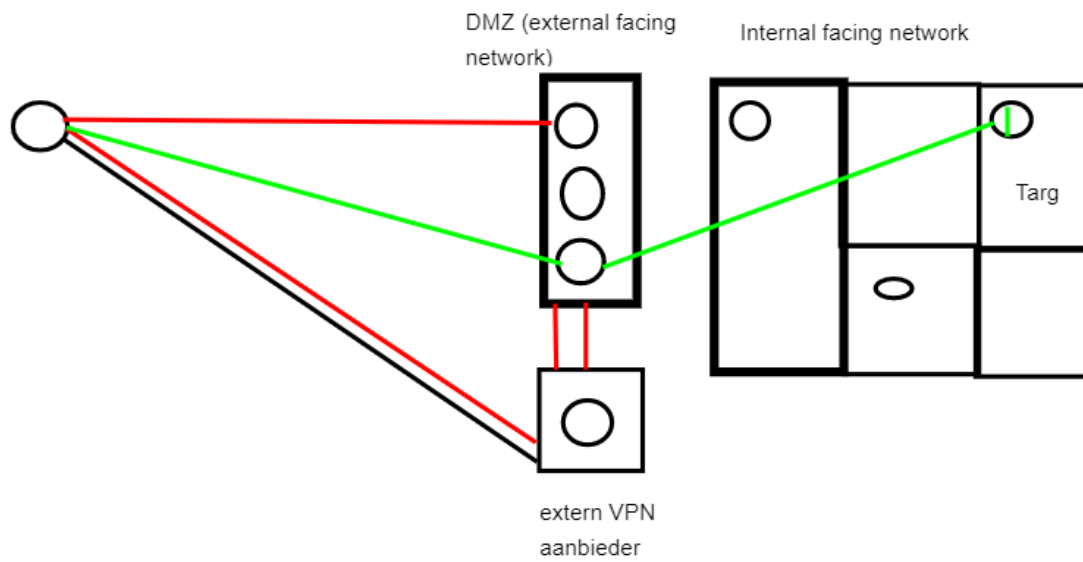


Figure C.1.17: Drawing 1_17

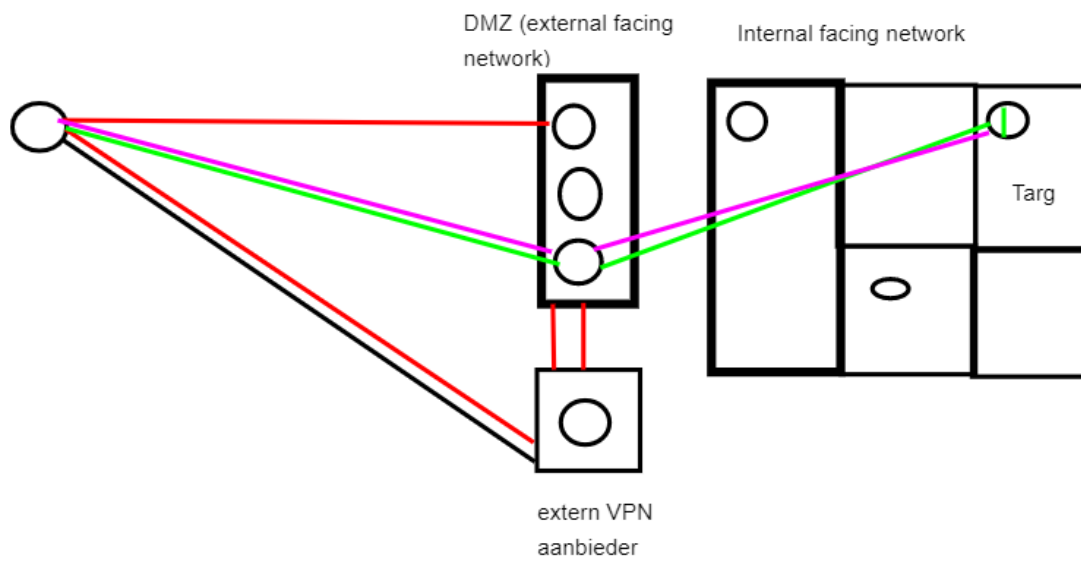


Figure C.1.18: Drawing 1_18

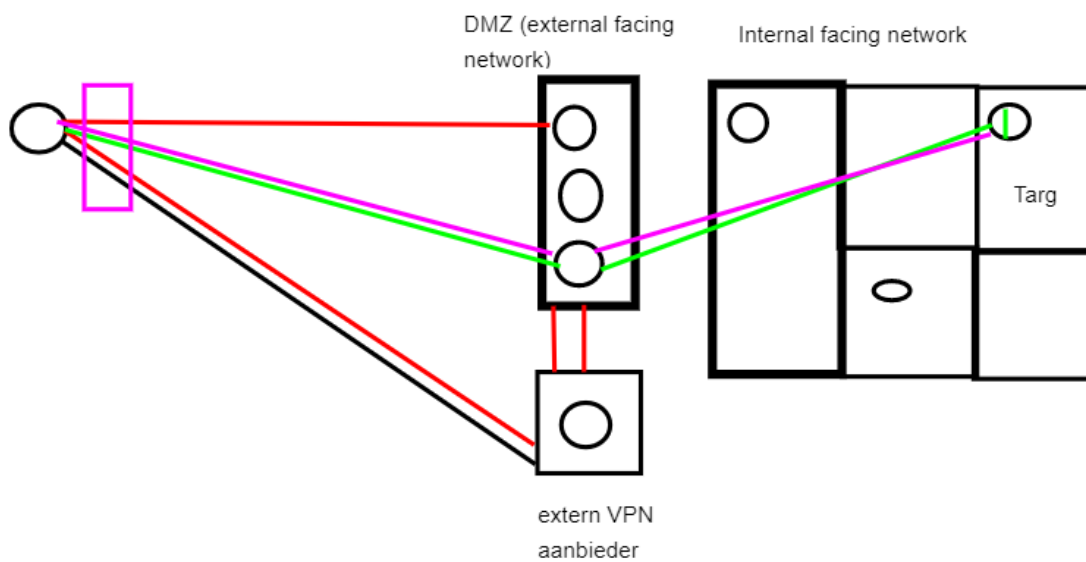


Figure C.1.19: Drawing 1_19

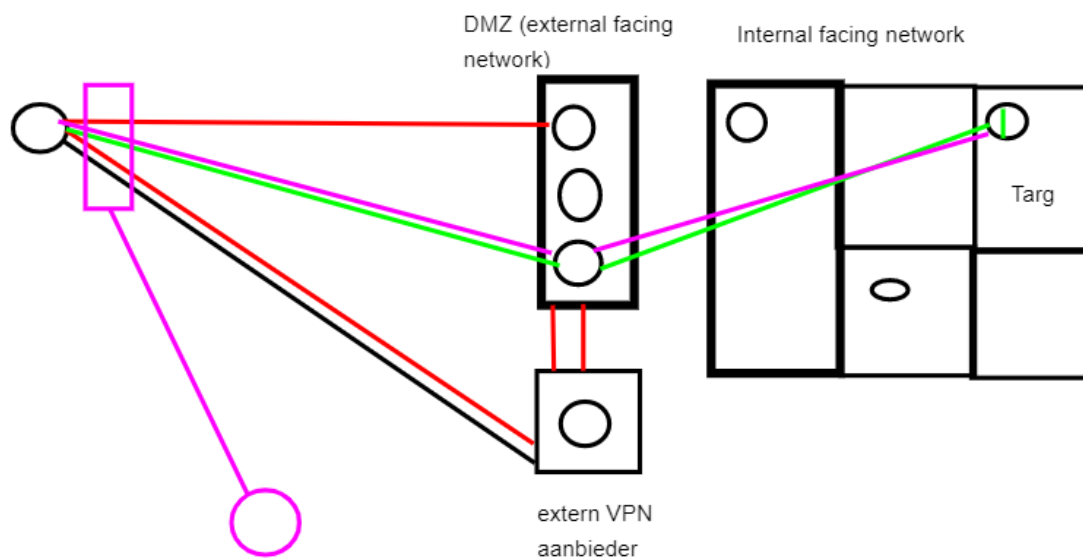


Figure C.1.20: Drawing 1_20

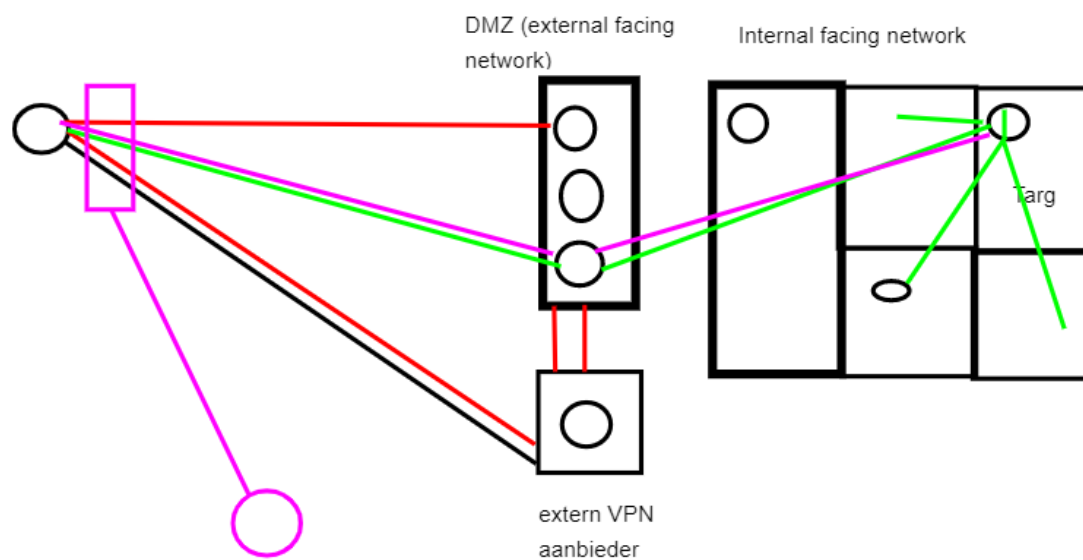


Figure C.1.21: Drawing 1_21

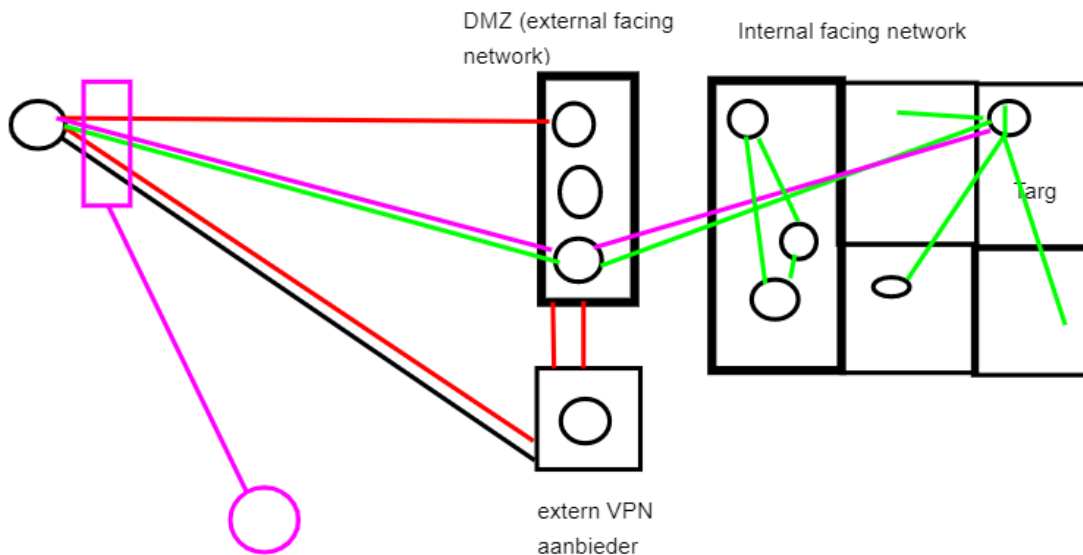


Figure C.1.22: Drawing 1_22

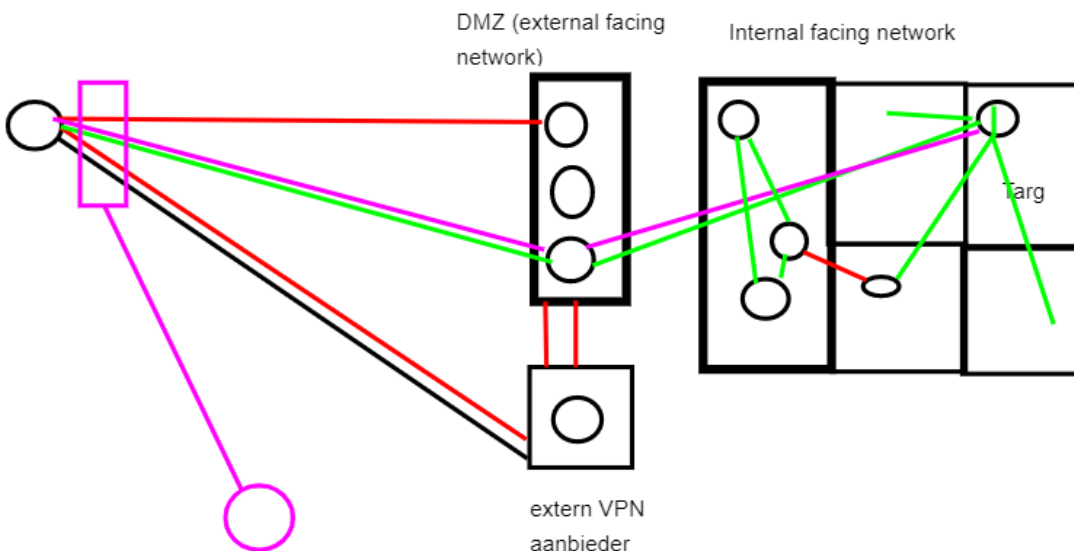


Figure C.1.23: Drawing 1_23

C.2: Transcript Expert 2

Duration: 30 minutes

Language: Dutch

Number of drawings: 1

X: Kan jij aan mij uitleggen wat een VPN is?

Y: Nou, van wat ik weet, een VPN is een Virtual Private Network en het beveilgd de verbinding als je bijvoorbeeld, eh, off-site werkt. Dat je toegang hebt tot, eh, bijvoorbeeld je bedrijfsgegevens of wat voor gegevens dan ook, maar op een beveiligde verbinding. Een beetje encrypted verbinding, waardoor je gegevens niet zomaar gelekt kunnen worden. Dat je toegang hebt tot eh, bepaalde webpagina's die gewoon via de Internet niet eh, toegankelijk zijn.

X: En hoe zijn deze niet toegankelijk normaal?

Y: Hoe zijn ze niet toegankelijk normaal?

X: Ja.

Y: Eh, gezien het in het interne netwerk is van je bedrijf of waar je het ook opzet. Maar meestal- Ik ken het alleen in het bedrijfsleven. Gezien het in het bedrijfsleven in het interne netwerk bevindt, dan is het eh, afgesloten van eh, ja, het Internet, dus de buitenwereld. En met een VPN kan je wel toegang krijgen tot eh, ja, alles wat in het interne netwerk is van je bedrijf.

X: Oké, en je zet dat het een beveiligde verbinding is. Kan je meer vertellen over deze verbinding?

Y: Nou, het enige wat ik weet is dat het geencrypt wordt, maar verder weet ik niet veel van VPN, dus het technische deel van hoe het precies in elkaar zit.

X: En wordt de hele verbinding encrypted?

Y: Dat hoop ik wel. Wat ik vermoed, niet zeker, maar wat ik vermoed is dat het eh, op het moment dat je het opzet dat alles wat eh, van jouw laptop, of jouw telefoon, of mobiele device, dat die dan geencrypt wordt naar het interne netwerk van je bedrijf.

X: En je zegt laptop en mobiele device. Gebruik jij ook op allebei deze apparaten een VPN-verbinding?

Y: Eh, ja en nee. Voor werk gebruik ik alleen op mijn laptop, eh, voor eh, voor mijn mobiele device, dus mijn telefoon, mijn mobiele telefoon daar zit het al, eh, ik weet niet hoe de applicatie heet, maar [example of mobile application], en ik vermoed dat dat ook eh, op een of andere manier beveiligd is.

X: Bedoel je ook beveiligd via een VPN-verbinding of op een andere manier?

Y: Dat weet ik eigenlijk niet. Is een beetje raar als security expert dat ik dat niet weet, maar je verwacht wel dat werk het goed geregeld heeft. Maar je krijgt wel dat dat ervoor zorgt dat je applicaties die je binnen de [example of mobile application] download, dus je [example of mobile application], je [example of mobile application], en al die, zulke, [example of mobile application], je krijgt wel een melding dat het geencrypt wordt. Dus ik verwacht wel dat het, ja, ik weet niet of het echt VPN is, maar ik verwacht wel dat ze het op een of andere manier eh, beveiligd is.

X: Op je mobiel dan bedoel je.

Y: Ja, mobiel.

X: En je zegt dat jij een VPN-verbinding off-site gebruikt. Op wat voor plaatsen gebruik jij een VPN?

Y: Eh, thuis. Of ja, waar ik mijn laptop ook gebruik eigenlijk. Want als ik [0:04:36 until 0:04:37 has been omitted], dan zet ik ook mijn VPN aan om gewoon bij [the professional services firm] dingen te komen, documenten of je mail of wat dan ook.

X: Zijn er nog andere redenen waarom jij een VPN-verbinding gebruikt?

Y: Nou, in principe niet, in principe is het meer om je, ja, je weet eh, dan dat je gewoon bij alle gegevens kan komen. Als ik het niet nodig heb zet ik het ook niet aan. Maar dat is eh, als je buiten werkt is het eh, het handigste om dat te gebruiken, want dan weet je zeker dat het ook eh, beveiligd is. Dus voor het zekere voor het onzekere zet ik het altijd aan als ik, zeker als ik [0:05:14 until 0:05:15 has been omitted], eh, thuis zet ik het aan als ik bijvoorbeeld bij een [the professional services firm] applicatie moet zijn, maar dat moet, want anders kom je er niet bij. Maar e-mail, als ik alleen bij e-mail en [cloud software] moet zijn, dan laat ik de VPN uit, want dan is het niet nodig. Maar dat is alleen als ik thuis ben. Op het moment dat ik buiten zit bij een café of eh, ergens, dan zet ik altijd, ja, voor de zekerheid zet ik de VPN toch aan.

X: De VPN aan.

Y: Ja.

X: Waarom zet je dan de VPN aan?

Y: Dat geeft een gevoel van vertrouwen. Maar, in principe, ik weet weinig van VPN, maar het is gewoon een gevoel van vertrouwen dat je hebt, dat het eh, je communicatie die je op dat moment bezig mee bent, dat dat wel op een veilige manier gebeurt.

X: En op wat voor manier gebeurt dat veilig?

Y: Nou de encryptie die je toepast. Die ja, toegepast wordt door VPN.

X: De verbinding dan bedoel je?

Y: Ja, precies.

X: En welke handelingen voer jij uit om een VPN-verbinding te maken?

Y: Eh, de eh, [the VPN of the professional services firm] openzetten, nou, eerst mijn wifi van waar ik ook zit aan te eh, connecten. Daarna de [the VPN of the professional services firm], mijn zes-cijferige pincode invoeren en dan de eh, vier- of vijf-cijferige code van eh, [access token provider], en dan connect, dan heb

je hem. Dus dat is simpel, maar daarom heb ik ook nooit achter gezocht van eh, wat allemaal precies doet op technisch niveau.

X: Je voegt een extra code toe naast je pincode, waar haal je die code vandaan?

Y: Van [access token provider] eh, [access token provider] is de token. Van [access token provider].

X: Oké, dat is een token. Wat voor een token?

Y: Het is een eh, software token dat je krijgt van [the professional services firm], de applicatie heet [example of mobile application] en daarop krijg je een zescijferige code is het en het heet een [the professional services firm] software token. Dus als je- En het verandert met de minuut krijg je een nieuwe code.

X: Zijn er nog andere manieren, eh, andere soort tokens?

Y: Eh, ja, je hebt zeg maar de ene die je in je hand gewoon al, ja het is echt een token, het lijkt op zo een klein dingetje, ovaal dingetje, en daarin, maar het is hetzelfde principe, dus het verandert de code om de minuut.

X: Zou je mij kunnen uitleggen hoe een VPN-verbinding werkt? Je kan hiervoor ook het whiteboard gebruiken als je dat fijn vindt.

Y: Ja, ik zou het wat kunnen tekenen, maar, oké. Eh, even kijken, hoe kan ik tekenen. Moet ik het naar mijn scherm, nee, ik kan het niet gebruiken. O, ja, ik heb hem. [\[start drawing 2_1\]](#). Dus stel je hebt hier je laptop, zo, ik ben niet heel goed met tekenen, maar oké. Denk dat het wel duidelijk is. Zo, je laptop, en dan heb je hier ergens de VPN. En hier heb je de server van eh, [the professional services firm]. En dan heb je zeg maar hierachter Internet en dan is de VPN-tunnel, die loopt zo. En dat weet ik wel dat het een tunnel heet, maar dan gaat het via het Internet, maar dan via een beveiligde verbinding naar de server van [the professional services firm].

X: Kan je dan meer specifiek uitleggen over de VPN die je hebt getekend?

Y: Dit?

X: Ja.

Y: Nee, nee, daar weet ik niet meer van inhoudelijk of technisch gebied.

X: Want de VPN zit dus in het Internet?

Y: Nee, het is niet echt in het Internet, maar het gaat over het Internet heen via de tunnel. Maar ik zou niet weten hoe ik het anders moet tekenen. Maar niet dat het in het Internet zit nee.

X: En wat bedoel je met een tunnel?

Y: Eh, ja, de tunnel is eigenlijk alles wat door de tunnel heen gaat, encrypted is. Dus alles wat hierdoorheen gaat is gescheiden van het echte Internet.

X: Maakt het voor deze tekening nog uit waar je bent als fysieke locatie?

Y: Nee. Nee, maakt niet uit. Zo lang je een mobiele device hebt en je verbindt met de VPN dan gaat alle gegeven die je hier hebt heen en weer.

X: Stel je voor dat je dan een e-mail stuurt, hoe zou dat in dit proces verlopen?

Y: Dat weet ik niet. Ik vermoed gewoon dat alles wat je hier doet, via de VPN gaat hiernaartoe. Maar, technisch weet ik niet meer dan dat.

X: En wat is de invloed van een VPN-verbinding op jouw computerbeveiliging?

Y: Een goede vraag. Ik denk eh, als je verbindt met een VPN of eh, als je computer verbonden is met een VPN van [the professional services firm] bedoel je.

X: Ja.

Y: Kan ik me zoiets voorstellen dat er dan eh, bijvoorbeeld automatisch updates uitstuurt. Nee, ik heb eh, eerlijk gezegd eh, weinig idee over hoe het allemaal technisch gaat.

X: Oké. En hoe zouden de automatische updates gestuurd worden?

Y: Dat wordt als het goed is gepushed naar je laptop via de admin. Dus dat zou- Waarschijnlijk gaat dat ook via VPN, want zolang je geen VPN aanzet, heb ik meegemaakt toen [0:11:54 until 0:11:55 has been omitted], dat er ook geen updates gebeurt. Dus je moet een keer per week ongeveer moet je VPN even verbinden en dan krijg je ook die eh, worden die updates automatisch gepushed en ook automatisch bijgewerkt. Daar hoeven wij als medewerkers weinig mee te doen.

X: En met wat voor digitale dreiging heb jij op een normale dag te maken?

Y: Ik denk de meest voorkomende zijn sms'jes. Ik heb weinig last van spam e-mails, maar sms'jes die krijg ik wel van een of andere partij die zegt bijvoorbeeld je [company] krediet wacht op je goedkeuring, log hier in. Of je, je krijgt een sms'je van CJIB dat je een boete nog moet betalen. Maar voor werk heb ik zelf nog niet meegemaakt dat ik eh, een spam e-mail krijg waar klik op een link of iets dergelijks.

X: Heb je met nog meer digitale dreigingen te maken?

Y: Eh, voor mij niet. Eh, enige waar ik gewoon zorg eh, als ik bijvoorbeeld klaar ben met een klant, dat ik die gegevens ook van mijn harde schijf verwijder, zodat ze echt op het interne netwerk van [the professional services firm] zitten. Maar nee, ik heb geen dreiging meegemaakt eh, in mijn carrière.

X: Verandert de soort dreiging door een VPN-verbinding?

Y: Eh, ik denk het wel. Zou wel logisch moeten zijn. Want op het moment dat je een encrypted verbinding opzet, dan is het niet, of ik kan niet zeggen niet mogelijk, maar het is minder moeilijk, of minder makkelijk om bij je interne gegevens te komen.

X: Hoe bedoel je dat?

Y: Wat zeg je?

X: Hoe bedoel je dat?

Y: Nou, gezien de gegevens geencrypt gaan via de VPN, dan vermoed ik dat het onmogelijk is, of bijna onmogelijk is om bij die gegevens te komen. Voor een externe persoon. Dus ook al heeft die toegang tot jouw Internet of tot jouw laptop, op eh, op een slechte manier. Dan vermoed ik dat alles toch wat je communiceert via de VPN wel veilig blijft.

X: En met wat voor sociale dreiging heb jij op een dag te maken?

Y: Eh, weinig, omdat ik eh, geen social media gebruiker ben. Ik heb wel accounts maar eh, ja, er is weinig te halen eruit, omdat ik niet echt eh, gebruik van maak.

X: En heb je nog te maken met andere sociale dreigingen?

Y: Ik de enige die ik te maken mee zou kunnen hebben is het hacken. Dat als iemand mijn laptop hackt of mijn mobiele device hackt, maar that's it. En zelfs als dat gebeurt dan heb ik eh, op afstand dat ik alles kan verwijderen. Dus als ik eh, zie dat iets gebeurt, kijk dat heb je sowieso met de werklaptop, vanuit je mobiele telefoon eh, kan je zowel met de eh, kan ik de IT-service desk bellen verwijder alles en ook eh, ook van mijn eigen [mobile phone], omdat ik mijn privé [mobile phone] gebruik voor werk, kan ik het ook zelf verwijderen. Dus het enige wat ik kan bedenken wat een dreiging voor mij is dat mijn laptop of mijn mobiele device gehackt wordt, maar er is niet veel te halen eruit.

X: Verandert deze soort dreiging door een VPN-verbinding?

Y: Eh, ja. Want als ik iets moet delen dan is het wel via een beveiligde verbinding. Dus dan is de kans dat het gebeurt veel kleiner dan als je zonder VPN iets gaat delen. Bijvoorbeeld [cloud software] zit niet verbonden aan de VPN. Daar kan je altijd iets uploaden en downloaden zonder VPN te gebruiken. Als je hele gevoelige gegevens moet gaan delen, dan niet via [cloud software], maar eh, alles wat wij delen met de klant dat gevoelig is, dat wordt eerst geencrypt eh, dus dat zit op de [cloud software], of eh [cloud software] niet, [an internal page] gebruikte ik altijd, dat is ook via met VPN te verbinden. Via [an internal page] wordt dat gedeeld met de klant. Dus we doen heel weinig delen via eh, e-mail als het heel gevoelige gegevens is.

X: Eh, en wie of wat is de aanvaller die de dreiging veroorzaakt?

Y: Eh, als ik kijk naar wat ik deel, dan zou ik me kunnen bedenken dat het een competitor is, dus iemand die graag die gegevens van een andere eh, partij in handen wil hebben om daar zijn eh, voordeel uit te halen. Misschien is het ook handig om wat achtergrond te geven daarbij. [0:17:12 until 0:17:25 has been omitted]. Dus als ik kijk naar wie die gegevens zou willen hebben, dan zou het een competitor zijn, maar that's it.

X: Zouden er nog andere aanvallers kunnen zijn?

Y: Ja. Het zou gewoon eh, een random persoon kunnen zijn ook, die gewoon zegt oké, laat me even kijken wat voor gegevens ik kan halen uit [the professional services firm]. Om financiële schade te eh, niet financieel maar, eh, hoe noem je dat. O, jee, ik ben het woord even kwijt. Een schade aan het bedrijf, dus eh, momentje. Even het woord opzoeken, sorry.

X: Geen probleem.

Y: O, wauw, ik ben het woord gewoon even kwijt.

X: Je kan het ook omschrijven anders.

Y: Eh, ja, schade aan je bedrijf, dus dat je in de krant of eh, in het nieuws met slechte naam komt.

X: Reputatie?

Y: Reputatieschade, precies.

X: Dus dat is ook de motivatie van een aanvaller dan, motivatie-

Y: Ik denk dat dat de grootste motivatie zou zijn om eh, als ik kijk naar mij specifiek, om mij specifiek aan te vallen, dan zou het echt reputatieschade of om eh, ja, om te zeggen ja kijk, [the professional services firm] beveiligd niet goed of eh, zo makkelijk is het om bij gegevens van [the professional services firm] te komen. Bij mij persoonlijk valt er niet veel te halen.

X: En wat zou de achtergrond van een aanvaller kunnen zijn?

Y: Achtergrond, ja. Eh, ja, ik heb eerlijk gezegd eh, geen idee. Misschien moet ik breder denken dan alleen aan mij, wat ik op mijn laptop heb. Eh, nee. Ik kom even niet op een goed antwoord.

X: Want je noemde eerder een ander bedrijf of een random persoon-

Y: Ja.

X: Wat moet zo iemand kunnen om een aanval succesvol te laten zijn?

Y: In principe niet veel, want eh, wat ik heb meegemaakt is dat met social engineering al genoeg kan eh, uithalen. Dus dat qua technisch heb je misschien helemaal geen kennis nodig om bij alle gegevens te komen, maar als je social engineering goed kan toepassen en dan gewoon toegang krijgt bijvoorbeeld tot USB-sticks, kijk gelukkig gebruiken wij dat niet, of ik niet. Maar dat zou ook een eh, manier kunnen zijn om bij gegevens te kunnen komen van [the professional services firm].

X: Bedoel je-

Y: Maar als je gewoon goed wilt kijken naar eh, ja, dan heb je wel de technische kennis nodig om te kunnen hacken bijvoorbeeld.

X: Hoe bedoel je dan social engineering?

Y: Eh, social engineering is bijvoorbeeld dat je eh, via spam een link stuurt, dat ik dan op die link klik. Dan moet het wel een goed opgezette e-mail zijn die betrouwbaar overkomt. Eh, tweede is dat je eh, eh, persoonlijk eh, tot, toegang krijgt tot mijn laptop, maar dat is ook niet waarschijnlijk, maar als iemand bijvoorbeeld achter je rug staat, stel [0:21:23 until 0:21:25 has been omitted] en iemand staat achter mijn rug te kijken hoe ik mijn wachtwoord invoer, dan is dat ook een manier om bij mijn, bij [the professional services firm] gegevens te komen. [0:21:35 until 0:21:36 has been omitted], die persoon kijkt naar je wachtwoord, je gaat even lunchen, ja dan heeft die wel een half uurtje zeker de tijd om bij alle gegevens te komen, als die je wachtwoord weet. En dat heeft ook een beetje met VPN te maken, want stel die persoon krijgt toegang tot mijn wachtwoord en ik ga even lunchen, mijn VPN blijft aan, een VPN is voor de hele dag bijna geldig, je moet dat een keer in de ochtend aanzetten en dan is die voor de rest van de dag geldig als je op hetzelfde netwerk blijft, dus op dezelfde wifi blijft. Dus dan heeft die wel toegang tot alle gegevens.

X: Maakt het daarbij nog uit of je je computer in slaapstand zet bijvoorbeeld?

Y: Nee, want dat ene wachtwoord gebruik je voor alles. Dat is single sign-on.

X: Dan blijft je VPN verbonden.

Y: Ja. Als je met de VPN verbonden blijft, ja, dan heeft die toegang tot alle [the professional services firm] gegevens. [0:22:37 until 0:22:41 has been omitted]. Zeker als de VPN verbonden is.

X: Wat zou de impact van een aanval kunnen zijn?

Y: Eh, bij mij persoonlijk of bij iemand van [the professional services firm]?

X: Bij iemand van [the professional services firm].

Y: Ik denk dat het afhangt van hoeveel gevoelige gegevens je op je laptop hebt, maar dan zou het eh, best wel een financiële en reputatieschade kunnen brengen. Als iemand met heel veel, ja, we werken met heel veel gevoelige gegevens van klanten, [0:23:20 until 0:23:30 has been omitted], ja, dan, dan zit je echt in de hoogste risicoklasse.

X: Is er naast financiële schade en reputatieschade nog meer schade?

Y: Eh, ik denk dat eh, qua informatie, die twee wel het belangrijkste zijn.

X: En dan over de VPN-verbinding zelf, hoe veilig is een VPN-verbinding?

Y: Eh, ja, als je er goed mee omgaat dan denk ik wel dat het veilig genoeg is. Want eh, je hebt zeg maar de code die je moet invoeren en je [access token provider] token, dus het is een persoonlijke code en de [access token provider] token en dan pas kom je erbij. Dus ik vind het wel veilig genoeg. Het is ook een manier van two-factor authentication, want je hebt zowel eh, je persoonlijke code op je laptop en dan op je mobiele device een andere code, dus het is niet ook niet op hetzelfde eh, mobiele device dat je beiden hebt. Dus dan zou iemand eh, zo bij je laptop moeten hebben, je mobiele device, wachtwoord van je laptop, wachtwoord van je mobiele device en je persoonlijke code. Dus er is best wel veel die je tegenhoudt om bij de VPN te komen. Om de VPN op te zetten bedoel ik.

X: En de VPN-verbinding zelf, is die ook 100% veilig?

Y: Dat weet ik niet. Dit is het technische deel dat ik dus geen kennis over heb.

X: En je zegt als je er goed mee omgaat dat het dan veilig is, wat bedoel je daarmee?

Y: Nou, het is het voorbeeld dat ik net gaf, als je je VPN eenmaal verbonden hebt dat het de hele dag verbonden blijft, zolang je op dezelfde wifi blijft. Dus, ik vind dat je daarmee wel voorzichtig mee moet omgaan, vooral als je bij, ja, buiten kantoor zit. Eigenlijk ook op kantoor gewoon, zorgen dat je altijd je laptop locked en eh, dat mensen niet zomaar bij je gegevens kunnen komen. Dus je moet je wel voorstellen eenmaal staat die VPN aan dan kan iedereen die toegang heeft tot je laptop bij alle [the professional services firm] gegevens komen waar jij ook toegang toe hebt.

X: Maakt het dan nog uit of je zelf op [the professional services firm] kantoor bent?

Y: Kijk, [the professional services firm] kantoor is een vertrouwde omgeving, maar eh, het, we ontvangen ook klanten, we ontvangen ook bezoekers, dus je weet nooit wie daar rondloopt. Ik vind eerlijk gezegd thuis veiliger, omdat ik thuis hier alleen zit. [0:26:13 until 0:26:16 has been omitted]. Maar thuis is sowieso veiliger dan op kantoor. Bijvoorbeeld ik durf thuis gewoon naar de wc te gaan zonder mijn laptop eh, te locken, maar op kantoor zou ik dat nooit doen. En niet omdat ik mijn collega's niet vertrouw, maar omdat je nooit weet wie langs kan lopen.

X: Wat is de rol van een VPN-verbinding hierin?

Y: Eh, de rol van VPN hierin is dat eh, eenmaal krijgt iemand toegang tot je laptop dat die dan ook gelijk, als je VPN aanstaat, bij alle [the professional services firm] gegevens kan waar jij ook bij kan. Dan is de beveiliging dan niet meer wat het hoort te zijn. Dan heb je liever dat de VPN uitstaat op dat moment.

X: Dat geldt zowel thuis als op kantoor?

Y: Ja.

X: En veranderen jouw handelingen hierdoor?

Y: Hoe bedoel je?

X: Jouw handelingen, want je omschrijft mogelijke aanvallen, hoe je daar zelf rekening mee houdt, zijn er nog meer handelingen die jij uitvoert om een aanval te voorkomen?

Y: Ja, zeker. Als ik bijvoorbeeld [0:27:39 until 0:27:50 has been omitted], eh, thuis eh, gaat mijn laptop ook altijd uit als ik hem niet gebruik. Dus, ja, en sowieso, [0:27:59 until 0:27:59 has been omitted], is het ook eh, een kwestie van als je laptop niet met slot achtergelaten kan worden, neem het gewoon mee met lunch.

X: Wat voor slot bedoel je?

Y: Wat zeg je?

X: Wat voor slot bedoel je?

Y: Eh, [0:28:27 until 0:28:29 has been omitted] en je gebruikt dezelfde kamer de hele dag, dan eh, als je gaat lunchen de kamer openblijft, ja, dan gaat mijn laptop mee. Maar als de kamer, eh, de deur op slot gaat, dan kan ik mijn laptop daar achterlaten, maar dan staat die wel uit.

X: Zijn er nog meer dingen die belangrijk zijn om te vertellen over een VPN-verbinding?

Y: Eh, voor mijn kennis niet nee. Ik zou graag meer willen weten over VPN hoe het technisch werkt, maar gezien dat niet mijn expertisegebied is of waar ik eh, technisch heel veel over hoeft te weten dan eh, heb ik nooit iets eh, achter eh, verder over, heb ik nooit meer eh, achter eh, verder over gezocht. Wat ik moet weten erover vind ik eh, nu genoeg, maar het is altijd interessant om meer te weten.

X: Oké, eh, heb jij zelf nog vragen verder?

Y: Ja, ik vraag eh, ja, ik ben benieuwd, tenminste als je het kan beantwoorden, waarom dit eh, waarom VPN gekozen is als onderwerp.

X: Oké, ik zal eerst de opname uitschakelen.

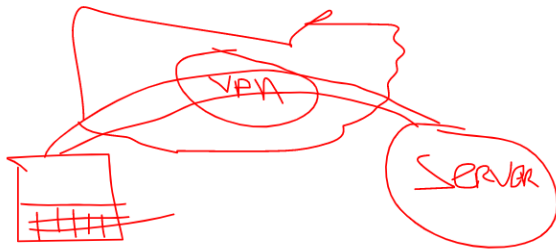


Figure C.2.1: Drawing 2_1

C.3: Transcript Expert 3

Duration: 60 minutes

Language: English

Number of drawings: 6

X: Could you explain to me what a VPN is?

Y: Yes, so you're gonna cold call me out. VPN, in essence, it stands for Virtual Private Network. So, it is a way of, of getting access to a private network. For instance, if you look at our company as [the professional services firm], to our, eh, corporate private network. And that way of getting access is not dependent on physical location. So, I do not need to be at the office and connect through the eh, Wi-Fi connection there to be able to access the VPN. I can make that connection to our [the VPN of the professional services firm] from anywhere in the world.

X: Could you tell more about the private network?

Y: The private network, so, do you mean- Because you mentioned in the beginning of our introduction that it is more about [the professional services firm]. So, are we talking about corporate VPN or also how you might use it as a private person?

X: Yes, how you use the [VPN of the professional services firm].

Y: Okay, all right, so in a corporate setting. Essentially it, it, eh, the way that it, the way that I use it is that there are certain eh, applications that are only accessible when you are within the [the professional services firm] network. So, eh, a very simple example of that is [an internal page], but also other business supporting core applications. And due to security reasons, these are not accessible just from any public Wi-Fi point. And you need to first establish eh, the VPN connection, so that the traffic is, is properly secured and encrypted, to then be able to basically use it as if you were just connecting to the office Wi-Fi. So, it allows you to feel or act as if you were connected to the office Wi-Fi and using all of the appropriate business applications irrespective of your geographic location, that is how I use it.

X: Do you use the VPN for any other purposes?

X: No, not the, not the corporate VPN.

Y: Or what other purposes are you thinking of?

X: Eh, I don't know, just getting a feel of what people use the VPN for.

Y: Yeah, so for me it is, from a business perspective, it is more to make sure that I can access whether it is [an internal page] or other type of applications, eh, [0:04:26 until 0:04:28 has been omitted], you can't get to it unless you are on the VPN, or the office network. Eh, just means that I can work.

X: Yes. And you said the connection was secured, can you tell more about how it is secured.

Y: Yeah, let me think, I don't think I can recall all the different protocols. Well essentially, VPN is like a tunneling system, right. So, you, you connect to the VPN server instead of just connecting directly to a website through an Internet gateway. And that means that that tunnel needs to be set-up, it needs to be protected, and that also, and I know this is not the same for, for every eh, VPN, the type of protocols that they use and the type of security that they use in terms of encrypting the traffic within the tunnel, et cetera.

So, there are several configurations, but it is ultimately about setting up the secure tunnel. Where your traffic goes through.

X: What do you mean with a tunnel?

Y: You can imagine it like an actual tunnel, I think that's- At least that's how I always learned it. So that your connection, so let's say your eh, I'm now dialing in from home, all of us are working from home, that I'm not connecting directly to a website, but I first set up a secure connection, eh, to a VPN server. That in our case is provided by [the professional services firm]. And that means that that connection basically forms a tunnel with the appropriate eh, protocols and ensuring the encryption of the traffic. Which then, to an outside viewer, or let's assume I was dialing in from you know, a [example of restaurant], and I was using their Wi-Fi, but then to make sure the traffic is not readable to everyone around us, using the VPN to shield off and basically wrap-up the traffic in a format that they can't read it.

X: Okay, is there a difference between home and the [example of a restaurant], in how you use the VPN?

Y: From a business perspective no. I connect as soon as I eh, use the Wi-Fi. Depending on where I am, you know this is a really practical situation, but I have travelled a lot for work, but if I am travelling in Europe, I probably wouldn't even use a public Wi-Fi spot, and just use my mobile data to create a hotspot. Eh, if I'm travelling somewhere where I know using my mobile data will cost [the professional services firm] 500 euros within the first five minutes of me using it, yeah, I would use it differently and would be more inclined to connect to, you know, whether that's hotel Wi-Fi or whatever it is, before connecting to the [VPN of the professional services firm].

X: Do you also use the VPN with the mobile data hotspot?

Y: Yes. That then just form the layer of first having the Internet access to be able to establish the connection to the VPN server.

X: And what is a VPN server?

Y: That's basically the server that allows you- So, you know how I said that normally, normally if you, if you use Internet it would be just routed through a regular eh, Internet gateway. It's the same if I use Internet privately at my home. And the VPN eh, server, basically sits between that and is the one that then allows us to connect to, for instance, the corporate applications.

X: Could you maybe use the whiteboard to draw how a VPN works?

Y: Anything specific? Cause that is quite a broad question.

X: Yes. Let's see that you connect from home and how does that look like.

Y: Okay. Let me see if I can find a pen. I'm hovering over the presentation, but I still don't- O, there we go. Now it's coming up. Eh, I am working from home. [\[start drawing 3_1\]](#). Okay, let's say this is me. Does this work. No, it's not the most- Can I turn, can I make the other one bigger. No.

X: You can undo an action or draw it again.

Y: Okay, let me see if I can do that. I am trying to redo- O, now it has taken everything away, great. And I want to try and type in it. So, you wanted to see connection from home, right? So, let's see, we do have a Wi-Fi connection here. Wow, this is looking like a child's drawing. And we would be connecting- Normally we would be connecting through a gateway, but eh, okay. O, god, can you still read that?

X: Yes, I can.

Y: And then from here, and I am simplifying it now, right. But eh, you would be accessing whatever resources you want, whether you want to go to [social media platform] or a different one. Now, the important thing here is I think, and I know you ask specifically about VPN in a corporate setting, but of course it is also important to mention that eh, this access, so me being able to access [social media platform], [social media platform] whatever it is, eh, is not possible anywhere you are in the world right. [\[start drawing 3_2\]](#). So, if I am trying to make this connection from say [country], then it is quite likely that there is a firewall here, that does not allow me to connect to this resource. But that is the other use case for VPN, that's not really looking at eh, the corporate perspective of it. [\[start drawing 3_3\]](#). But let's assume the corporate perspective, means that essentially, instead of going directly here, I would be, so I am just gonna mirror this from above, I would be connecting to a VPN service. Where we are setting up- Basically like a tunnel here, for our traffic to go through. So, this is again me from home, and then this would form the basis of connecting. So, it would all be routed through the VPN server. And then, in a corporate setting, here behind

this VPN, so this Virtual Private Network, would sit the eh, the private corporate network. So, this would be the resources that I mentioned, like [an internal page] that I would not be able to access eh, without using a VPN. If we're talking about you know, the example that I mentioned, if you live in a country that is eh, where the Internet is severely restricted, then it would allow you to actually circumvent eh, using that gateway, or rather it would allow you to connect to the VPN here and then connect to all the other resources. I hope I got that right, it has been a while since I studied VPNs.

X: No problem. How does it work if you can eh, access applications in a restricted area, like you said if you go outside of Europe and you have geographical restrictions?

Y: So, you're thinking something like [country] now?

X: Yes, for example.

Y: Yeah, so let's assume, you know, this firewall here is, is not allowing you to get to [social media platform], then VPN, and it does depend on what type of VPN you, you use, because you of course still first need to establish a connection with the VPN to then use it to be able to access the other resources through it, right. That first connection point requires the VPN server to not be blocked by the country. And I know that eh, that depending on- Cause there are a lots of companies as well that are offering subscription based VPN, some of them have been blocked in the past, but in general it means that you first ping the VPN server, and then you know, basically that's becoming your Internet gateway. So first you need to make it through here, make sure the VPN connection isn't blocked and then once you have been able to establish this, this sits behind it, that allows you to connect to all of those resources as if you weren't even in [country].

X: How is your location determined?

Y: Based on your IP-address.

X: Sorry, can you repeat that?

Y: Based on your IP-address.

X: Okay. And could you explain to me what a server is?

Y: What a server is. So, it's part of the infrastructure that you're using to connect. It's basically eh, and it can be you know a virtual server or an actual server somewhere, it's, it's, it's well, what is the best way of describing a server. It's a connection point that facilitates the way you connect for instance with a specific web resource, a website.

X: Okay, and could you explain what a gateway is? What do you mean with a gateway?

Y: Almost like a, like a division keeper, asked to what eh, what can go where. So what are you allowed to access and it's, it's like a, you know, at school in the past when you'd cross a road and it's like telling you yes you can go here, yes you cannot go here. And normally, and that's the reason I'm mentioning it in response to restricted countries, where, you know, that it usually flows from the Internet service provider in that country, so there is an element of eh, state-oversight that can be, eh, that can be applied here.

X: Okay, and on what devices do you use a VPN, the corporate VPN.

Y: We use it on our corporate laptop.

X: Only on the laptop?

Y: Yeah, I think there is actually, on the phone as well, but that is part of the eh, mobile device management. Yes, there is a VPN configuration that we can add here.

X: And what actions do you take to create a VPN connection?

Y: As a user or as eh, the IT team setting it up?

X: As a user.

Y: I first, so on the laptop, I first need to make sure eh, one second, I'm getting pinged by so many people. Okay, sorry, responded on [conferencing software]. What actions do I take. Okay, so I first establish connection to the Internet, because if you recall, we first need to be able to, to establish that connection with the server, right. So, there is an element of first setting up that connection and that requires me on my corporate laptop to have eh, Internet. I either use my home Wi-Fi or if I'm travelling I'd create a mobile hotspot, which essentially acts the same. Eh, and then as soon as I'm successfully connected to eh, the Internet, I open up the [the VPN of the professional services firm], click on the connect button, and then there has been some security measures built into this, eh, and what that means specifically is that it connects to a soft [access token provider] token on my phone, which provides a, I think it is an eight digit,

no it's a six digit code. Which I need to enter and it is regenerated every, I think 60 seconds. So, it is constantly updated, and I need to enter that on top of entering a, that's an eight-digit personal code that only I know. And once I have successfully entered that, and it verifies that I have provided the right eh, software token, so the [access token provider], then it will allow me to connect. And it will give me an icon that says connected and then from that moment onwards I am able to use [the professional services firm] internal resources.

X: Okay. And you say you use a software token. Are there any other possibilities?

Y: Yeah, you can also use a hard token. So, we used to- We have always worked with [access token provider] as a provider at [the professional services firm], at least since I joined. In the beginning we had a physical token, which you just carried on your key chain. It had essentially the same functionality. So, it was showing the, the digits eh, I think it was also a six-digit code at the time. Which would automatically refresh at timed intervals, but that for me was a little bit more complicated, because [0:20:08 until 0:20:25 has been omitted], so I was happy when I could move my [the professional services firm] token to a soft token, [0:20:31 until 0:20:35 has been omitted].

X: I can imagine that. Is there still a possibility to have a hardware token in [the professional services firm]?

Y: That's a good question. I handed mine in when I switched to a soft token. I know at the time it was eh, optional to switch to a soft token, and I would imagine, because this was already a couple of years ago, that they would have transitioned everything to a soft token by now. Eh, but I don't know that for sure. It is maybe possible that they, that they still use some hard tokens. No clue.

X: And why would they switch to a software token?

Y: I don't know what prompted that decision specifically.

X: And eh, earlier you also mentioned that you do not use [the VPN of the professional services firm] when you connect to the office Wi-Fi, why is that?

Y: Because then you're actually part of the, the local area network that [the professional services firm] has set up in the office. And that does not require you to, to use the VPN server. So, if I am logging in from the office directly, it has all been configured that I connect to a specific Wi-Fi, I think it is the [the Wi-Fi of the professional services firm]. And that's essentially, so that's the Wi-Fi that you then just connect to directly. And VPN mimics as if you were connected to that Wi-Fi from the office, but from, eh, from a distance. So, it is not necessary to connect to VPN from the, from the office, since you're already part of the eh, the trusted private corporate network when you connect to the, to the dedicated Wi-Fi connection.

X: And what is the influence of a VPN connection on your computer security?

Y: On my computer security. Well, it means that eh, you know, since we do have a tunnel set up, which is, and you know I mentioned there are different protocols eh, for securing this, but it is- It already applies security measures to set up this, this path that we're taking to connect eh, to the, to the private corporate network, and it also provides eh, to encrypt the traffic that is going through the tunnel. And the level of security of course depends on the configuration of the specific VPN. The idea is that eh, you're encrypting the traffic and sending it through a secured channel. So that is the additional security measure that you take.

X: You say different protocols, could you explain a bit more about that?

Y: Yeah, I am, let me see, you might need to help me out with remembering some of them. I know there are some protocols that work, they are like an all-inclusive package essentially, that take care of both of the setting up the connection point as well as the security measures that are applied to the traffic. And then there are others that work in combination, so you'd have one protocol that allows you to create the point-to-point connection and then you would put something like IPsec on top of it to secure the traffic, and encrypt it.

X: So, you create a point-to-point connection.

Y: Hmhm.

X: What does that entail?

Y: So, you wanna connect your own connection point to the VPN server, right. This is the tunnel. So, it has a start and has an end, and it allows traffic to go back and forth. That is the point-to-point connection you're setting up.

X: And what kind of digital threats do you deal with on a normal day?

Y: What type of what threats, sorry?

X: What kind of digital threats.

Y: In a specific setting or, what do you mean when you say on a normal basis?

X: So, yes, in a normal day what kind of digital threats do you encounter?

Y: Well, that's a very, eh, there is so much, that's a very broad question. Do you mean specifically when you're not using a VPN or eh, if I'm working, if I'm looking at myself as a private individual eh, just wanna make sure that I scope the question correctly.

X: Yes, in a general sense. So, you mention there are a lot, could you give a couple of examples.

Y: Yeah, of course, and let me know, I won't be able to cover everything because it is so broad, but happy to go into more depth. Eh, so I think you know digital threats eh- We have, o god, that's such a broad question. So, anything that starts from eh, someone assuming your identity, you know whether that's the typical example of you know, a grandma being send an e-mail to provide their banking information, or, you know in the US if you look at social security eh, numbers that have been stolen, or the BSN number in The Netherlands, so there is always a threat of someone eh, assuming your identity, pretending they are you in a digital space and using that for their benefit. Whether that benefit is, if you take the example of a social security number, that they are able to maybe apply for eh, social benefits or a loan in your name, without you having to do anything to do with it. Or if you take the more extreme example of getting access to certain payment applications or even your banking account, it means that they are able to steal money from you. So that would be eh, threat eh, that I think that eh, is quite relevant to lots of people. Depending on, on where you live, of course also, you know I mention here that certain restrictive countries might not allow you to access certain resources, but on top of that also eh, and that is a connection to the VPN connection, that you might be eh, you might be victim to someone you know, sniffing on your traffic and actually reading everything that you send through the web. Which can serve you know, multiple purposes. Eh, intentions of attackers I think are as wide as there are eh, different attack scenarios. So, whether that's with the objective of eh, getting to personal data, which we all know is a very high sought-after currency and, and can be monetized quite easily. So if I would wanna sniff the traffic to actually you know, what log in credentials you use to a specific resource, but it can also be, and this is where we are looking at different motivations, if you are severely restricted state, you might also surveil your eh, your fellow country women or men and we know the NSA scandal of mass scale surveillance, but we also certainly know that countries that are subject to a lot of restrictions eh, in terms of freedom of press, human rights et cetera, they are actually finding out information, personal information about someone, whether that reveals their political affiliation or sexual orientation, eh, can so far as costing people's lives. So, we are looking at something that goes way beyond stealing money eh, in that specific scenario. But those are just you know some very, very high level eh, examples. There are million more.

X: And from an [the professional services firm] perspective, does the threat change because of the VPN connection?

Y: Does the, does the what change, sorry?

X: Does the threat change because of the VPN connection?

Y: Eh, well some of the threats change, so when we talk about eh, sniffing traffic etcetera, you know, using the VPN as a security measure to, basically wrap up and encrypt the traffic certainly makes it way less likely, or it is associated with way more effort to get to that traffic. Eh, there are other types of threats that are not directly eh, mitigated by the eh, VPN connection, which are also you know, some of them are definitely prone to human error. So, for instance, for us always a big risk factor is eh, us accidentally sharing files with the wrong recipient or making it accessible to the wrong recipient. So, that has nothing to do with the VPN connection, that's how we behave. And also, because we have a lot of e-mail contact eh, outside of the organization, whether that's clients or vendors or other third parties, of course there's always a risk of a phishing attack or so. Which you know, whether it is human error or those types of attacks, we have different eh, security controls and measures in place, to more specifically target those.

X: Clear. And this is about digital threats, do you also deal with social threats on a normal day?

Y: Social threats?

X: Yes.

Y: Eh, is that something like looking at something like a social engineering attack or do you mean something else with a social threat? A social threat also, I mean, can also be look at socio-economic circumstances somewhere, that I would see as a much bigger threat than anything that stems from cyber or from digital devices.

X: I mean all threats that are non-digital.

Y: Then, are you looking at politics or-

X: If you imagine these kinds of non-digital threats, can you describe how those non-digital threats change because of the VPN connection?

Y: Eh, I am still trying to understand eh, the example of a non-digital social threat.

X: For example, you mentioned social engineering-

Y: Yeah.

X: That would be a social threat.

Y: Okay, but we're still looking at threats specifically looking at eh, at cyber space?

X: Not necessarily cyber space, eh, all kinds of social threats that stem from the perspective of [the professional services firm].

Y: Okay, cause I would also argue that what's going on in [country] at the moment around racism is a huge social threat, but that's not what you're looking at.

X: Not necessarily, but it can definitely be a social threat. If you see it as a social threat as well from the perspective of [the professional services firm], then yes, it is-

Y: No, it's more a broader societal thing. Yeah, but correct me if I'm not going in the direction that you're looking for, because I don't think I fully understand the question. I am using the example of social engineering, so here eh, in the example that I will talk about, VPN has very little, or very, basically a negligible role to play. So, let's talk about eh, one of our office locations, we might use the [place] office as an example, we have implemented physical security controls, we need to restrict physical access to the building, that involves [0:32:36 until 0:34:06 has been omitted], but let's assume for arguments sake, an outside person with malicious intent has managed to get into the [the professional services firm] office. [0:34:15 until 0:34:17 has been omitted], and is able to walk around freely. than they might use that to try and find a connection point into the Wi-Fi or maybe find a device that has been unlocked and not eh, secured correctly to try and get access to resources on the [the professional services firm] network. That would you know, if you were to try and do this attack from abroad, also be accessible through the VPN, but it is much more likely to be successful at an office location.

X: You mentioned shortly VPN. How does VPN, does it have a role in this?

Y: No, if we're looking at the specific example of a, of an office. And we already spoke about the fact that we do not connect to VPN, [the VPN of the professional services firm] when we're at the office. So, in that specific configuration, no.

X: Okay. And from a different location?

Y: Yeah, from a different location. So, I think, you know, hacking the VPN server is quite a momentous task, we only, this is also not a very likely scenario, but the only scenario I can think of is let's assume I'm with my laptop eh, in [country], I was working from it somewhere in a hotel lobby, I am connected to the [the VPN of the professional services firm] and then the, the easiest point of attack would be to distract me, so that I leave my laptop unattended and that I haven't locked it. So, then someone would be able to exploit the fact that I am already connected to the VPN, so I have virtual access to the private corporate network. And use the resources, at least the resources that are accessible to me in that scenario. Because I am not an admin, I don't have access to all files and resources at [the professional services firm] either, to try and obtain that data.

X: What do you mean with you do not have access to all eh, files because you're not an admin?

Y: Yes, so as any organization, we have identity and access management controls implemented. What that means is that in line with your, in our case it is a role-based access system, eh, in line with your business role, which needs to be validated upon hiring and also is in line with your eh, functional role. You only get

access to the eh, the minimum of resources that you require. And you do not by default get access to every resource the way that a system administrator would, absolutely not.

X: How would that look like in the drawing you made?

Y: Eh, don't know if we can add it here. Can I just add something new? Or do you need me to add it to this one?

X: O, a new slide you mean?

Y: Yeah.

X: Yes, that's possible.

Y: Let's see. [\[start drawing 3_4\]](#). So, the way that it works is, let's assume something like this. Eh, that person is a little bit ill-shaped, but that's okay. We all look different. Let's assume this is me, so this is [role], this is an admin, and we are all connecting to the different resources, and- Slowly getting the hang of the drawing. Okay. I spoke to early, should connect here. All right. So eh, let's assume, you know, we wanna connect to the different resources, whether that's [an internal page] or just a general office eh, core business applications that we're are using as [the professional services firm]. Eh, but we are different people connecting to this. And if we are on a, you know, at [the professional services firm] office, this would allow us to do that directly from the office Wi-Fi that has been configured. If not, it will go through the VPN. But it's the same process. So based on your role, you will have different access privileges. So, for instance, we discussed I'm a [role], which means I need certain access to applications. So, for instance, I will just give you an example of that, I need edit or write access to eh, I can't think of the perfect example, but I'll just use [an internal page] for now. This is not the best example, but just for argument sake, right. Eh, then we have [role], who needs no access to [an internal page], and then we might have, and bear in mind, this is not how [an internal page] works, but I just wanna illustrate how it works. Then we might have a third person from a business perspective, that could be eh, someone from I don't know, maybe another function, another team or so, that only requires- [\[start drawing 3_5\]](#). The idea behind this is that depending on our access profiles, so these here, are our roles, no that's not working yet, for instance, if [role] were to try based on their business role and their access profile to connect to whether that's through the office Wi-Fi or a VPN, to let's assume it is this one, that we're trying to connect to. [\[start drawing 3_6\]](#). I'm sorry Veroniek, there are so many people pinging me and trying to call me. Eh, let's assume this is the resource we wanna get to. So, this is [an internal page] in this, this hypothetical example. Depending on the business role that you have, this person would only require read-only access, so they would not see the same that I see as the one that needs to be able to edit and write, [0:42:20 until 0:42:23 has been omitted]. And since that's a business process [role] is not involved with, [role] doesn't need any access at all and thereby we are implementing the principle of you know, least privilege, and ensuring that only the people who really need have access to it.

X: And then eh, all lines go to the circle in the middle-

Y: You mean the yellow one or this one?

X: Yes, this one.

Y: This one?

X: Yes, this one.

Y: Yeah, so this one would be eh, you know, whether it's the connection which has been facilitated through the Wi-Fi that has been configured at the office, or, you know, the VPN is first giving us access to that virtual private eh, the virtual private corporate network.

X: And then going back to the attacks we mentioned, who or what could be an attacker behind it?

Y: Eh, are you thinking of a specific threat?

X: For example, social engineering you mentioned.

Y: Hmhm. Well, I think the threat remains the same, that it's a malicious actor trying to get access, eh, so that's not a variable that is, is changed by this. However, of course as an attacker you're trying to maximize the access that you will have, to maximize the impact you will have. So, if I manage to get access to [role] and let's assume my ultimate target is to see [an internal page], that would be no good. Because from [role] account, there is actually no associated business role and rights to access that. So of course, from that perspective, you'd try and go for a business role that has access. So, [0:44:37 until 0:44:37 has been

omitted], to be able to get to it, and ultimately the goal of any attacker is to try and elevate their access and their privileges to the point that they can take over a system. Eh, so that they can freely navigate and find whatever they are after.

X: What kind of malicious actors are we talking about?

Y: We're talking about a lot of different of them. So you can think of eh, in a corporate setting, eh, you know, maybe it's a disgruntled ex-employee, maybe it's corporate espionage, eh, but many, many more, I mean there are as many motivations and actors that you can think of, but these are probably eh, the most relevant in this context.

X: Could you give examples of their motivation?

Y: Well, disgruntled ex-employee, I think that's eh, the clue is in the title, so if they feel they haven't been treated fairly, they might try and get access to be able to expose certain files that they feel would be damaging to the company, or that they would wanna use in building up a law case against them for instance. Corporate espionage, I think again, the clue is kind of in the title, so trying to access any type of information that would give you eh, a competitive advantage going up against that company. That's probably less so relevant for us, but if you're imagining you working for a big pharmaceutical company, that has eh, you know, eh, proprietary recipes, you know, that have not yet, that are still patented, so you haven't released the formula et cetera, than getting your hands on that eh, would give you a huge advantage in being able to tackle that company's, maybe even monopoly on producing that specific drug.

X: What would be an attacker's capability?

Y: Capability?

X: Yes.

Y: Their capability, that's looking at their own eh, I think capability mainly looks at your own expertise. And your own- So, your starting point. So are you skilled at hacking, do you have any social connections to the company that might allow you to sneak your way in, eh, do you have access to people that will pay you to do this job, or maybe on the flip side, are you the one who has lots of money and you can hire a big group to do this for you. All of this are examples eh, but not exhaustive in terms of capability.

X: Okay. Does the kind of attacker change because of the VPN connection?

Y: The kind of attacker?

X: Yes. So, the sort of attacker.

Y: Eh, well, I, I, yes, do you mean change in, in what sense specifically? Cause of course our attack scenarios don't really have a VPN connection at the center of them. So eh, disgruntled employee, so what might happen, you know, what, this is, this is not something that's really relevant in this scenario, but let's assume hypothetically the company has very poor of boarding of employees, so the leaver part of the join and leave process which is a core aspect of your identity and access management doesn't function properly and they do not remove your access on time, so they don't disable your account, so the account that would be associated with your business role and the profile that you'd get with it and on top of that, not only do they don't do that, but they also don't ask you to eh, return the token, so we're using the example that we, that we used earlier that you require those levels of access controls to it. Then in theory you'd still be able to access company resources, even after having been terminated. So, you're still able to get to the VPN connections, because your user credentials as whatever else you might need, so in this instance a token hasn't been taken away from you. And then you're able to access company confidential information, even after having been terminated.

X: Very clear example. And if you look at an attacker's motivation or skill level, would that change because of the VPN connection? If you use a VPN connection?

Y: Eh, that's quite broad to answer definitively, so I'll try and make it example based. So, in this example that I just mentioned I don't think capabilities have a lot to do with it. Its more that a person doesn't need to understand how a VPN works from a technical point of view to be able to take advantage of the fact that their access hasn't been disabled on time. They just need to you know figure out that they can still get access. Eh, and then use that to get to whatever information they want to. If we using an attack scenario which has not got a disgruntled ex-employee with insufficiently terminated access rights, so someone who's starting, you know, completely outside of the company, then yes, and let's assume you're not trying to

orchestrate a social engineering attack, which means getting physical access to the building. But you actually wanna try and hack the VPN connection, yes of course. Because there are additional security levels, thus, to be able to actually break the VPN, that eh, requires tremendous abilities and capabilities. If you look at the example like the one I mentioned earlier, that I am working from the hotel lobby in [country] and someone tries to distract me to make sure that I don't lock my laptop and its connected to the VPN at that point, that doesn't require a lot of capabilities. But it does mean that you'd only see whatever I have access to and then being able to elevate those rights and jump around and ultimately try and get admin access, yes, that's again of course requiring a lot of capabilities.

X: What could be the impact of an attack for [the professional services firm]?

Y: So, let's go smallest to biggest. So if we assume that in one of those two examples, so disgruntled ex-employee or someone manages to get my laptop unlocked while I'm already connected to VPN, they would be able to access any information that I am allowed to see, based on my business role. So they would be able to see all my files with client confidential information, they would also be able to see confidential commercial data that I have access to, which eh, they would be able to, you know, take copies of or extract from the system, and then be able to use to whatever advantage eh, they might want. Depending of course on the individual eh, motivation. If you take worse case and someone uses the connection into the system, whether that's on premise or through a virtual VPN connection to try and elevate and escalate their privileges, then you could be looking at them getting access to even more data. But ultimately, it's about, at least from the type of scenarios that we're dealing with, its mainly about getting access to confidential data and being able to use that.

X: What could be a consequence if they get access to that confidential data?

Y: Well, it's a breach right, it's a data breach at that moment. And it needs to be investigated and followed appropriately to determine the impact and could be subject to, you know, having to notify the data protection authorities, could even possibly lead to fines if we're found to be negligent or depending on the impact and we also need to look at notification chains with anyone that's affected, which of course if you imagine that that's a client, will not necessarily help our relationship with them and might even bring with it legal consequences in terms of lawsuits.

X: Okay. And if we look at the VPN connection itself, how secure is the VPN connection?

Y: Yes, so this is where I mentioned earlier that eh, just because it says VPN, there are still varying levels of security within that connection, because it ultimately depends on how you set it up and which protocols you use. And I know that some of the initial protocols that were used have been, you know, the encryption behind them has been broken, eh, so yes, it offers you an extra level of security in terms of security and keeping data confidential and setting up the, the connection to the private network so that you're not spied on essentially as you're, as you're connecting. But ultimately if you want to have a definitive conclusion on how secure it is, you need to look at the specific configuration of the VPN. You can't make a default blanked statement.

X: And do your actions change because of these insecurities?

Y: My actions change based on the insecurity?

X: Yes. So, do you handle differently, because you know there might be vulnerabilities in the VPN connection?

Y: No, they don't, because ultimately, I need to work, I need to get access to it. It's still way more secure than if I was able to all company resources from [example of restaurant] Wi-Fi. Eh, the reason that I emphasize that it depends on it is that in, as with any you know, security mechanism that you deployed, always depends on the specific configuration. But eh, having said that, having a VPN to access the corporate private network is from a security point of view way more preferable than not having one. But that doesn't mean, and that is I think in general with security, that you're never gonna have a 100%.

X: Okay, I think that is a nice notion to end this on. Do you have anything about VPN that was not said right now?

Y: Eh, no nothing from my side. I know it has been quite free format in terms of covering topics, so I don't know if we've covered everything that you wanted to get into.

X: Yes, we did. All questions I have are answered.

Y: Cool.

X: So yes, if you can think of anything that we did not speak about and that you think is important to mention-

Y: Let me see, well the only thing that, but this is not, this is really not from a corporate point of view, but more a, eh, societal view, because I do think that, you know, how I said in that previous drawing I said well you first need to establish a connection to the VPN server.

X: Yes.

Y: Which I know in certain countries also, if it's a recognized VPN service, they might actually disable that eh, that connection. So, I know that, I think the NSA did that as well, that they actually were scanning for people using a VPN or you know, using their search terms to connect to a VPN and then put them on a list of people requiring, eh, more surveillance, because they felt that was by default suspicious, that someone would try and, and keep their web traffic and those connections private. So, I think that's more a political point of view. And from an individual perspective of course I feel like we're all entitled to not be surveilled by a state, but then there is also the flip side of it, if you look at it more eh, from a law enforcement point of view, then of course eh, privatizing, or not privatizing, but keeping information private and allowing people the freedom that comes with it, of you know, either using a VPN service or even setting up their own VPN does mean that, of course it can offer those people with malicious intent and criminals also a way to hide from law enforcement or make it significantly more difficult eh, to get to them. So, I think that's just one, it, it's not related to VPN in corporate use, but more from broader societal perspective. It's something to be aware of that what we're gaining from it is also avoiding eh, more privacy and freedom to those with definitely not the right intent.

X: From an [the professional services firm] perspective, is the NSA for example, taken into account searching for a VPN connection or making a VPN connection eh, and placing the [the professional services firm] employees on extra surveillance, would that pose a risk?

Y: Yeah, I don't know how likely that is, because of course you also see what kind of VPN service you connect to, and if it of a very reputable firm, that's definitely something different than you know a guy from Minnesota that has suspicious spikes in web traffic anyway, using a eh, a custom built VPN. So I am, yes of course you could argue that this is also important in a corporate setting eh, but I think this is more, and that's why I say for me it is more a societal point of view, this is probably something that proportionally will affect individuals or you know groups of political activist more than it would a corporate. That's just a personal gut feeling, I don't have any stats to back that up.

X: Okay. Thank you very much-

Y: You're welcome.

X: I think that was everything from my side.

Y: Cool, hope it's helpful.

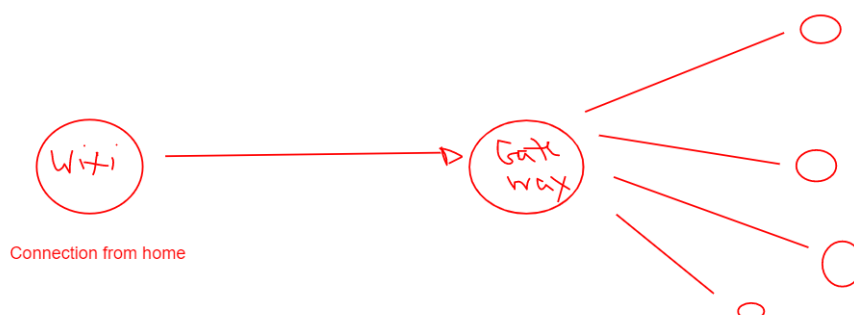


Figure C.3.1: Drawing 3_1

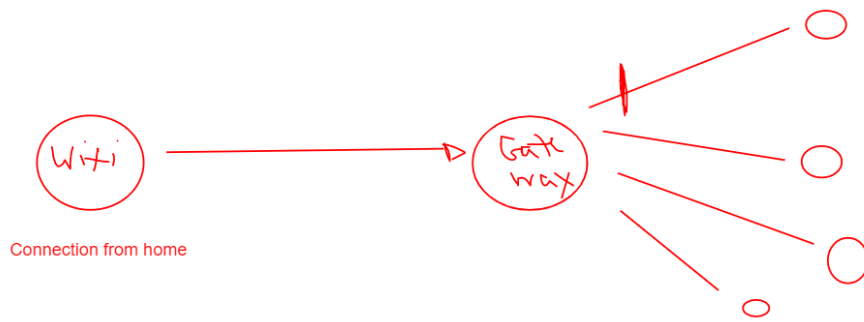


Figure C.3.2: Drawing 3_2

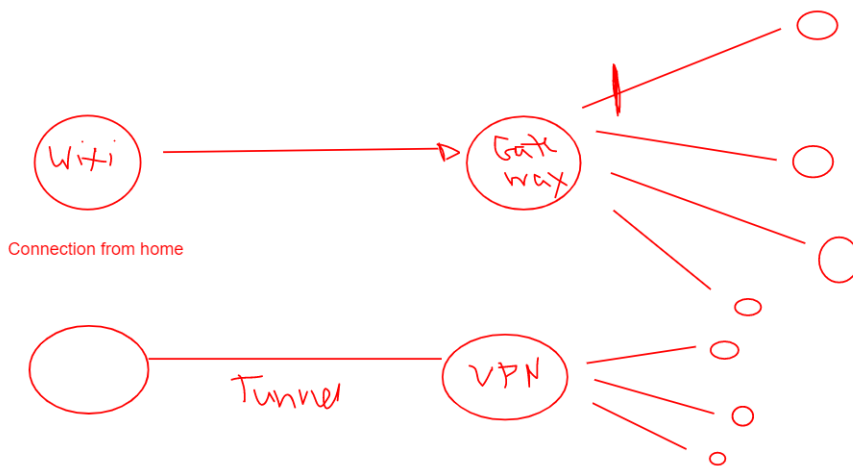


Figure C.3.3: Drawing 3_3

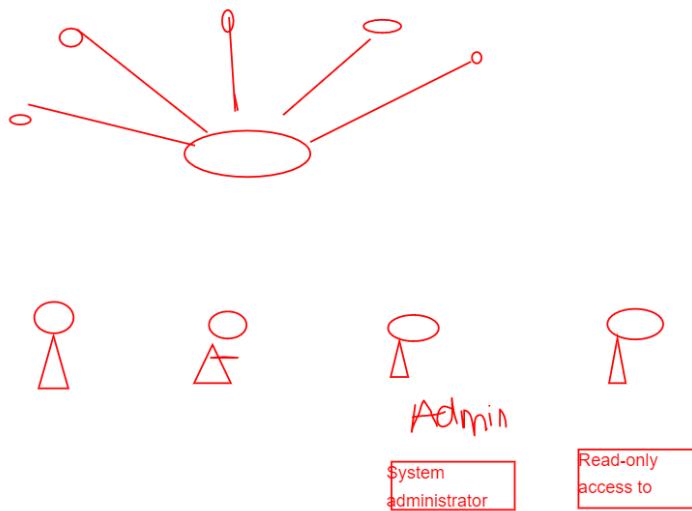


Figure C.3.4: Drawing 3_4

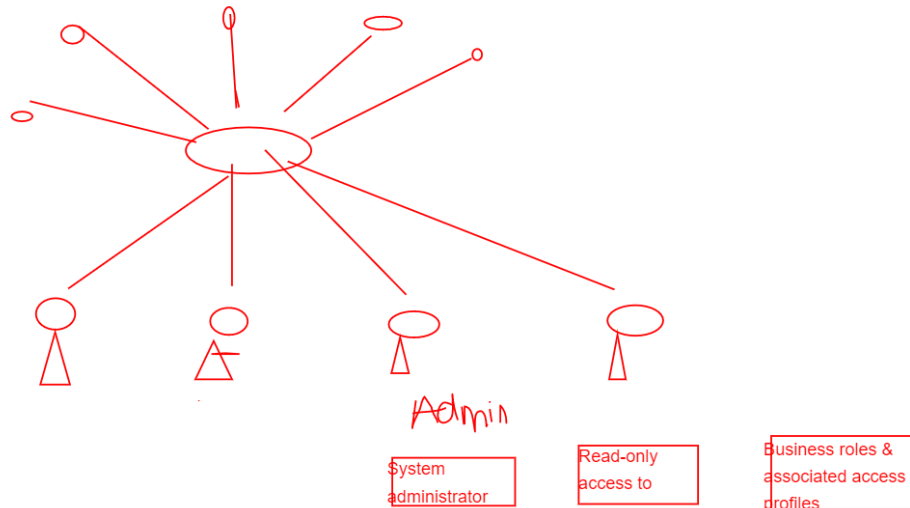


Figure C.3.5: Drawing 3_5

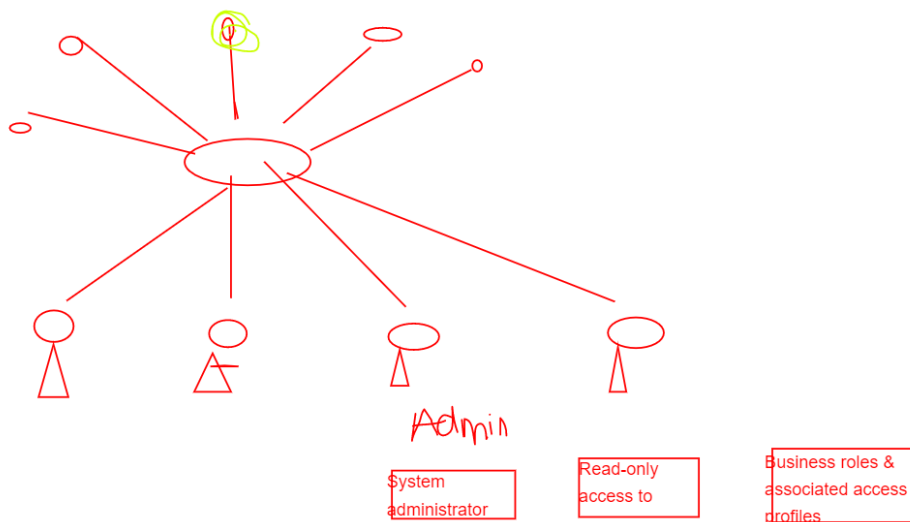


Figure C.3.6: Drawing 3_6

C.4: Transcript Expert 4

Duration: 88 minutes

Language: English

Number of drawings: 18

X: Could you explain to me what a VPN is?

Y: A VPN is used to reroute your connection through the server. Eh, this is used for security purposes or to eh, be able to mask your eh, location while using the Internet.

X: Okay. You say to reroute your connection, how is your connection rerouted?

Y: So, you are using it as a door to the Internet instead of connecting to the Internet through eh, your eh, connection, your IP, your computer you are accessing this server and from that server you are sending your requests and receiving your data and then it is routed from the server to your computer.

X: Okay. And could you explain to me what a server is?

Y: Eh, basically a server is just another computer that you're connecting to. A server is of course eh, bigger, stronger computer, this is eh, eh, let's say industrial or something. This is a computer that is eh, eh, used for multiple users. This is a mainframe like a, as you can see in the movies eh, a cabinet closet, that eh, has

the, the, eh, supercomputer, the stronger computer than normal. And you are using it as a connection. You are connecting to it and the server itself, that computer itself is sending and receiving requests from all over the Internet.

X: Okay. And you said you can use VPN for security purposes, could you say more about what these security purposes entail?

Y: Eh, so, eh, you can think of it again as a computer. In your computer, you have your own eh, antivirus computer eh, software, you have your own malware, you have your own eh, eh, security applications all of those are eh, eh, embedded within the server with the highest level and with the eh, latest updates. So, from eh, eh, the threat of being eh, infected with viruses, breaches, or eh, being hacked, using VPN is an extra layer to eh, safe, to make you a bit safer than searching the Internet. So, when you are accessing a website eh, which is eh, suspicious or eh, that can eh, trigger a virus, this server, this VPN server, can act as a first layer of, of eh, of, of defense. So, this is one. The second one is security from the eyes of everyone else. So, from the people who are tracking your requests, tracking your eh, eh, browsing history let's say. While using VPN, no one can see what are the request that you are sending, they can only see the IP of the server itself. So, you are also shielded from being tracked.

X: Okay. And your first security purpose, how does the server act as a first layer of defense?

Y: Imagine that eh, this server is eh, your PC. And you are connected to this PC. Imagine that it is in your home, in your room, so this server eh, has the latest version and the strongest version of antivirus, it has the strongest version of anti-hacking or malware, as they call it. So, the malware is software that people can use to eh, obtain information from your laptop or your computer. So, using this server can provide this extra layer whenever there is virus that is coming to your eh, browser, coming to your PC, coming to your laptop. Through this server, the server should act as a, a, firewall, a defense layer, that's stopping this virus. So, eh, yeah, for example when using a VPN, sometimes you are trying to access a website and you will not be eh, directed to the website, instead you will get a screen that this website that you have requested is not secure, using this connection you will not be able to access this website. Eh, we recommend you to look into eh, eh, this website as it is reported as a threat to your PC. So, it either stops you from entering the website, or stops the intended threat, so it can stop the attachment or stops an e-mail from coming to you if it is eh, eh, including any threat to your data or to yourself, your PC.

X: Okay. And eh, you also said it protects you against the eyes of everyone else-

Y: Hmhm.

X: How does this protect you against the eyes of everyone else?

Y: Okay. I'll give an example eh, outside of our environment. Then I'll give another example from, from work perspective. So, from eh, countries that are at war, for example [country], is someone who can speak against eh, eh, a certain party. There is a possibility for them to be detained or eh, held accountable to what they are saying. So those people use the VPN and through the VPN they can post, they can send files, they can use accounts, without these parties being able to track them or to know who is the actual person responsible for those information. The VPN, using the IP of the VPN, everyone else on the Internet is they can track an account or an article or a video on [social media platform], they can track the IP that has posted this. And this IP is one of the IPs of the server itself, of the VPN server, but if the VPN is secure, which is, should be the case, you cannot get the IPs of the people using this server, you can only see the actual IP of the server itself, not for the users who are using this, this server. So, this is one of the uses of masking your own IP. Hiding it through the use of the VPN server. Is this clear?

X: This is clear. Thank you.

Y: Of course, another application from, from work perspective eh, when you are working with eh, multiple clients and international clients, sometimes there are some limitations to accessing their data. [0:09:25 until 0:09:36 has been omitted]. And I can only access this information if I have an account that can allows me to do that. So, using the VPN connection masks my ID, of course this is in a legal way, I mask my ID through their VPN, so that I can access their secure eh, location. Using this VPN can give them the comfort that I am not an intruder or someone who is not authorized if I have this VPN access it means I have the permission to go to their secure eh, cloud, and access their files.

X: Could you perhaps use the whiteboard to draw for me how such a connection would work? You are for example working from your home situation and you connect to eh, [the VPN of the professional services firm].

Y: Eh, I, I don't know how to create this eh, let me try to see if I can eh, interpret this in a simple way. [\[start drawing 4_1\]](#). So, instead of connecting to the Internet immediately, we can use the server, let's use this IP. This is my PC. This is the VPN. And this is the eh, Internet or if we can say the, o, wrong button. [\[start drawing 4_2\]](#). O, let's quickly draw it eh, this is [the professional services firm], this is the VPN. Eh. Normally I would connect to [the professional services firm] using my IP, which is my Internet name. [example IP-address], so the IP is the name of my connection, you can consider it the name of my eh, eh laptop. The Internet knows me as, as this number. So, when I go to [the professional services firm], [the professional services firm] sees me as this and it will not allow me to enter this, their server, to access their services. For example, to go into my e-mail account, my [the professional services firm] e-mail account. Eh, or my eh, eh, work eh, workspace. So, I need to have a secure connection because this can be copied easily, this is a public IP, so anyone can use this public IP. Of course, I can combine this with a password or with another authenticator, but it still is eh, a bit eh, vulnerable. So, people can hack or can eh, use this, another combination to hack my account. [\[start drawing 4_3\]](#). So, [the professional services firm], they have installed another layer, this layer, means that access from outside is eh, access from outside is not allowed eh, unless it is secured. [\[start drawing 4_4\]](#). So, how can we make this secured connection is to have eh, for example a number of secure eh, IPs, let's consider [example IP-address] until [example IP-address]. Yeah. So, this is an example. Of course, it is a bit more complicated than this, but this is the concept that they have private IPs that are only known between the server and [the professional services firm]. [\[start drawing 4_5\]](#). Then, if I want a secure connection I can connect to the VPN, using my IP-address. Using this address. And then from the VPN, when I connect to [the professional services firm], I would use one of those secure eh, IPs. [\[start drawing 4_6\]](#). So, [example IP-address] for example. So, [the professional services firm] can only see this IP and because it is an IP that is eh, in their database they can allow it to enter. So here in the database, [the professional services firm] should have the list of those secure IPs. So, [example IP-address], for example. So they are saved here, so, they crosscheck those IPs with their list, and eh, this is the eh, let's say the contract between this VPN and [the professional services firm] to allow those IPs and then I can enter their eh, secure application and eh, do the work. Is that eh, good, is it okay.

X: Yes, very clear. You told earlier about a firewall as well-

Y: Hmhm.

X: Where in this picture would you find a firewall?

Y: So, here, within the VPN, now I send my request, now let's consider another scenario, where here, instead of [the professional services firm] I am visiting unknown website. So, if I am, let's say eh, using instead of [the professional services firm], am logging to on unknown. [\[start drawing 4_7\]](#). Let's call it- So if I want to go to this website, I send the request with a secure eh, IP. [\[start drawing 4_8\]](#). This website sends back eh, a packet data, a picture for example or a sort of data, that has a virus in it. Let's say virus, a virus here. So, this is a virus. [\[start drawing 4_9\]](#). Now, within the VPN, they have the applications that should eh, scan all coming packages eh, and for example, anti-virus, anti-ware, eh, firewall- So, all of this is within the VPN, so the server, this computer, is equipped with all of the state-of-the-art applications that scan those packages and either remove eh, here, either stop, eh, wait- [\[start drawing 4_10\]](#). Either stop this here, at this border, or for example only allow the secure part of the package and will not, so for example you are receiving an e-mail from an unknown source, you will get the e-mail, but you will not be able to open the attachment. So, the attachment is deactivated for example. So, using the, the software is within the server, you eh, make sure you have a more secure connection with only eh, known eh, sources or known objects to be received. Is that clear?

X: Yes. You also said-

Y: So, it is-

X: Yes, sorry.

Y: Yeah, so, it is similar to what you could have on your own eh, device, so for example you are using eh, eh, some kind of an anti-virus, [software provider] eh, [software provider] anti-virus. But what you have on

your PC, you have the personal version, because if you want to have the corporate version, you will need to pay a lot of money. So, this company, the one that has the VPN server, they pay for the highest level of security so that you are using this very expensive and up-to-date application for, for your personal use. So, you are using the technology with only fraction of the cost.

X: Do you need to pay yourself you mean, or the company pays it for you?

Y: Exactly. So, if you want to for example, if you want to install five applications, if you want to install one application for antivirus, if you want to install one application for secure browsing, if you want to install an application for anti-malware, eh, if you want to install eh, a firewall, so, in the end you will need to pay for example a hundred euro per month, but the VPN pays a thousand per month, because they have the updated version, the up-to-grade version and then they only ask you, or they ask your company, for example in my situation [the professional services firm], they ask for ten euros per user, so they get back their investment and the user herself, the user himself, doesn't really pay for the total cost of the application, they only pay for the monthly subscription to the VPN itself and use the software.

X: Okay. And you also mentioned that sometimes a page, a webpage is unsafe, and your browser blocks it. What is-

Y: So, it is the same, it is the same, sorry, it is the same with this if you are going to an unsafe eh, website, it doesn't wait until you get back the virus and stop it, the VPN has also a list eh, let's say here. [\[start drawing 4_11\]](#). So, it could have a list of secure websites, or a list of unsecure websites. So, the VPN server, they have a list and they compare every request. So, every time you type www.google.com for example, this request goes through this filter, the filter looks if this is one of the secure websites, it immediately allows it to go, if it is one of the list of the unsecure websites, it immediately stops this request and sends it back to you and inform you that this is not secure, because this has been reported for example earlier. So, your request is not send or the third option is your request is not being recorded on either list, then the eh, request is send and then the response will be eh, eh, scanned for any viruses or any attacks, and then it's stopped if it is the case.

X: Okay. And what would happen if you go to the same website, but you are not, eh, you did not enable a VPN?

Y: So, now, if you are bypassing this, if you are going immediately through the normal connection, then your request will get to the website and the website have the ability to send you eh, a virus or spyware or malware, and it is up to your device, laptop or PC, to stop this attack. So, do you have up-to-date antivirus, do you have an up-to-date spyware, then it will catch this eh, this attack. If it doesn't have it, you will receive it, for example an e-mail with an attachment, an e-mail with a link that can install a virus. So, the laptop or the computer didn't catch this attack and you received the e-mail, then it is up to you to open this e-mail and see okay, I see this e-mail, it doesn't look phishy, I click on the link and then I am eh, infected, my laptop is infected with a virus. But then, the other option is I notice this is an attack, I notice this is not secure e-mail and I delete it. So, if I am not using the VPN, I am depending 100% on my eh, self and my device.

X: So, there is no other mechanism that prevents eh, e-mails like that being send to you?

Y: [\[start drawing 4_12\]](#). So, as I said, the mechanism is either one eh, let's say, VPN or paid apps or free apps and then your knowledge and eh, eh, your knowledge and eh, let's say, common knowledge more or less. Eh, so eh, the most secure option is to use a VPN. The second option is to pay yourself for the applications that the VPN is using, sometimes it is not at the same level, but a paid eh, antispysware or antivirus is also an option, if not, you can install a free version. So, this is partially protecting your PC. Of course, it is not protecting it from eh, from the latest eh, applications. Because the latest ones are always covered by the paid version. If you don't rely on those free apps, then you are relying on your knowledge. So eh, last month, I received eh, an e-mail from my account from [e-mail], asking that eh, there is an attack and you need to click on the link to change your password. I immediately saw that this e-mail is not from [e-mail], it is an attack that looks like a [e-mail] page, but if you focus on the eh, e-mail that this e-mail was send from, this is eh, not @[e-mail].com, but eh, gibberish, something else. So, when I saw this e-mail, I understood that this is an attack and I e-mailed immediately reported this e-mail instead of opening the link. Instead if I had opened the link and I got to a website asking me write down your old password and new password, they would get my old password and they will open my account and get inside my account. And eh, eh, get my

information. So, eh, the VPN is the most secure way to browse the Internet, but it is not the only option, it is the most secure option.

X: This is for your corporate laptop?

Y: I am now talking in general, either for corporate or eh, personal laptop, but this is a good question, because within a VPN you have multiple eh, types of VPN. So, you have the commercial VPN, some company who bought a server, put it online and ask people to pay subscriptions to use this VPN server. So, this would be secure, but it would not be highly secure. Then you have an, another VPN server which is from a well-known corporate, so for example using secure [company] server. So, this [company] server, they have a name they need to maintain so they use a really state-of-the-art server. So, this is the second level. The third level, which is the highest level, is that a VPN that is provided from your corporate, from eh, for example from, where I work at [the professional services firm], they have provide their own eh, VPN, this is known, this is the highest level. Because, then here, you are not using the IP from the VPN, you are using a VPN that is pre-approved by the company, so you have two-way handshake as they call it. So, the VPN communicates to [the professional services firm], and [the professional services firm] communicate to the VPN and they open a secure connection. So, this is the highest eh, the highest level. There is no way of anyone intervening in the middle. No third party.

X: What do you mean with interfering by a third party?

Y: Eh, the VPN company for example. So, the VPN company, if you look at the Internet, there is a lot of eh, eh, third parties, there is a lot of companies who eh, yeah, sell you the service of VPN. But are they themselves secure, you don't know them. You need to do your own research to make sure that those companies add service are secure. They have the latest update of the antivirus and they have a good secure connection. Because sometimes a VPN does not mask your ID, the IP-address. It allows your IP-address to go through, but it scans the package. This is not a hundred percent secure. But if you are using a VPN that is pre-approved with the websites that you are visiting, then it makes it, eh, another layer of security.

X: Okay. Clear.

Y: Okay, good.

X: What do you mean with a secure connection between the VPN server and [the professional services firm]?

Y: So, the, what I mean by secure connection is what I just mentioned. So, the secure connection is that no one else is between you and your target application. So, if this VPN is provided by [the professional services firm], so you have immediately from connecting from your PC, you have [the professional services firm] channel. So, I don't have any other company that could be a weak link. So, I have a secure pass. So, for example now in this pandemic, in Corona. So, I have, I go from my home to my car, to my office. Which is, I am the only one who is using this office, so I know all of the steps that secure, no one could eh, infect me with this disease. But, if instead of using my car, I am using public transport, there is, here, this connection in between, is not secure. I am not using an eh, corporate VPN, I am using an open connection. So, there is a big change of being infected if I myself, not being vigilant, I don't have the knowledge of protecting myself. Of course, instead of going in the public transport, I can use eh, my neighbor's car, my brother's car, I can use a taxi company. It is eh, less public, but again I don't have the 100% assurance that this is eh, risk free. So, using a VPN is like using your own service. You know how secure it is. But using any other option can present more risk.

X: You mean you know how secure the [the professional services firm] VPN is.

Y: Eh, of course, in this situation it is not me who need to be afraid, it is [the professional services firm] who needs to be afraid. And they know that this VPN is secure. Me, as a user, I don't know. But because [the professional services firm], who is the, let's say the organization or the site that need to secure their files, they are the people who eh, take the measures to make sure that this VPN provider is secure. And they do that by, for example, a strong contract with eh, a penalty clause, if there is any eh, issues eh, with doing an audit. So, the IT-audit itself is one of the ways to make sure that the eh, service that is provided is according to the standard that it is mentioned.

X: So, [the professional services firm] uses an external VPN supplier you mean?

Y: Eh, so [the professional services firm] is using a VPN supplier. I cannot eh, I don't have the knowledge if this eh, for example a company or an application owned by [the professional services firm] or this a contract being eh, extended by, with a third party. The only thing is, I know that, the [the professional services firm] VPN is a service eh, like [the professional services firm] e-mail address. This is service that is provided by [the professional services firm] to its employees and it is managed and overseen by the corporate itself.

X: Okay, thank you. On what devices do you use the [the professional services firm] VPN?

Y: Eh, so, the VPN itself is only used on eh, [the professional services firm] laptops. But of course, there is other measures on other devices. So, if you are using your mobile phone to access [the professional services firm] location, you need to have another service. Not a VPN, but a service that eh, checks for eh, your connection and your requests. So, it is not a VPN, but some sort of eh, check, like an antivirus for example. It is not an antivirus, but it is eh, a service to check for, for threats.

X: Eh, why do you use a VPN? For what purposes?

Y: The purposes of using a VPN. Is that your question?

X: Yes.

Y: So, as a [the professional services firm] employee, I use VPN to eh, first of all, have a secure connection eh, to, eh, to have the eh, I'm trying to find the right word. So, eh, to, provide my clients with the assurance that their data, which I am working on, is still secure. So, no one from outside my organization, my team can have access to their data, which is on my devices. So, using a VPN eh, provides the assurance that the client data is secure.

X: Are there any other purposes for which you use a VPN?

Y: Eh, for my personal use I could use a VPN for example to access the [company] server on the UK, because the server on the UK provides broader content than the content on the Netherlands, but- And of course, I am stating this a legal way of using the VPN. Other people can mask their eh, their, their IP to eh, access eh, other websites that can track their eh, usage of the VPN. So we are going back to the first question eh, the usage of the VPN is either to mask your presence, your name, your IP from anyone else on the Internet or to have a secure connection to be able to access any website without being afraid of being hacked or eh, having a virus on your device. Eh, or to have a secure connection with no one else being able to steal your data.

X: Do you mean no one else can steal your data because you use the VPN of [the professional services firm] and not another VPN server?

Y: Because I used a secure VPN, not an unverified VPN. Because other VPN services could be secure, but again, here in my situation, [the professional services firm] did the work for me. So, [the professional services firm] have provided the assurance that this is a trusted service. I don't need to do the work myself. But with other services, I do need to do my research, I need to review the contract, which 99.9% of the people don't review. So, when you are subscribing to any contract, you get approve and do not approve, most people press on approve without even reading what they are approving on. So, this is something that, when I am using the VPN of [the professional services firm], I know for a fact that [the professional services firm] has the legal team to make sure that eh, using this service has been reviewed and eh, approved by the company.

X: And as a user, what actions do you take to create a VPN connection?

Y: Eh, as a user, I only open the application that is provided by [the professional services firm]. I make sure that I have the Internet connection activated. I put my username and password a click on connect.

X: Okay. And what is the influence of a VPN connection on your computer security?

Y: [start drawing 4_13]. If the VPN connection is on, I know for a fact that here I have this connection protected. So, whenever the VPN connection is on, I know for a fact that I won't, most of the time, I won't get any threats from this side. [start drawing 4_14]. The only problem is that when I turn off my VPN connection, I could get a risk or a threat from this side. [start drawing 4_15]. And if I use a, a USB for example, a USB stick, in my device, this is a threat that the VPN is not covering. So, the VPN is only covering the risks from the Internet, as long as the VPN is activated.

X: Okay. And does it matter where you create the VPN connection?

Y: Sorry?

X: Does it matter where you create a VPN connection, so for example at home or at a different location?

Y: No. It doesn't matter, because, no matter where I am, immediately when I am activating my VPN, I am doing this two-way handshake. So, I am sending a packet to the VPN server and the VPN server approves my connection. When it approves my connection, this connection is encrypted, so no one can access this connection, and this connection is protected by eh, the VPN server itself. I don't know if you can see my mouse when I am moving it.

X: Yes, I can. Can you tell a bit more about the encryption of the connection?

Y: Eh, this is another layer of protection. So, a VPN could provide encryption. This encryption means that like when we are talking in a different language, the VPN is using another language. So the letter, or the number one in the eh, computer language is eh, sevens zero's and a one, so it's eh, in the computer language, in the language of zero one, eh, number one is zero, zero, zero, zero, zero, zero, zero, one. With an encryption eh, the VPN could be using a different language, which eh, cannot be read by an outsider who doesn't have this eh, list of decoding of the encryption. So, using the encryption, the information is sent and received between me and the VPN server in a way that is not being read by anyone else. Even if they were able to tap into this connection.

X: The connection between the VPN server and the [the professional services firm] server?

Y: Between the VPN server and [the professional services firm] if this is like for example in this case, this connection is a private connection, then I would expect that here, there is also an encryption. The encryption only works if the two parties are eh, known to each other. So, they have the let's say, decoding list. So, if I speak to you in Spanish, and you don't know, you don't have the dictionary of Spanish, you cannot understand me. But in this case, all of the parties have the contract, so they could have the decryption list, therefore I would expect that all of this connection is being encrypted.

X: Clear, thank you. And then in a bit of a broader sense, what kind of digital threats do you deal with on a normal day?

Y: Sorry, I did not get the question.

X: What kind of digital threats do you deal with on a normal day?

Y: Eh, may I ask you, can we take a break for eh, couple of minutes?

X: Sure.

Y: Okay, I will keep the connection on, I'll just eh, come back within three-four minutes.

X: Okay, that's fine.

Y: Okay.

[break from 0:54:01 until 0:58:25]

Y: Hello.

X: Hi.

Y: Hi, I'm back.

X: Are you ready to take on where we left off?

Y: Yes. Yes. So, your question was, was what are the type of threats that I am facing in my work, right?

X: What kind of digital threats do you deal with on a normal day.

Y: Okay. So, the first threat is that we are working with, with the high-profile clients, so there are a lot of people who would like to obtain this kind of information from any way and they could try to obtain this from, from our laptop or our connection or our devices. So, the first threat is people trying to hack and steal the data of the clients. Eh, the second, eh, level, the second type of threat is the people who would eh, try to steal eh, any data without any discrimination. So, any type of data to eh, blackmail and ask for ransom, eh ask for money. So, it doesn't really make any, any difference if the data is personal for the client or the organization itself. And of course, the third eh, the third party, the third threat is people who would like to harm eh, eh [the professional services firm] as an organization. So, those three threats that eh, eh, we could deal with eh, using, yeah, digital connection.

X: And how would information be obtained from your laptop?

Y: Eh, by one of the eh, ways eh, eh, shown here in this drawing. So, either by sending eh, spyware and malware, where eh, unknowingly I am opening a connection with this person or this organization and they could steal from my laptop without me knowing. So, they install this application that open this connection. Or by me thinking that I am uploading the files to [the professional services firm], but in fact I am uploading it to a different location. So, eh, as I said before, an e-mail with a link that I think it leads me to a certain website, but in fact it's leading me to a different one. Eh, what else. Eh, sometimes it could be eh, with infecting a computer with a virus that you cannot eh, deactivate until they, you pay this person a certain amount of money, so that he can activate, deactivate it for you, so this is the ransomware. It happened with eh, unknown virus where the data on, on the computer were held hostage, so you cannot access your own data until you eh, had to pay eh, certain amount of money to the hacker, so that he can eh, deactivate the eh, virus and you can access your data. And if you don't eh, some viruses keep your files locked, some viruses delete your files and some viruses even, cause your device to malfunction. Sometimes stop the fan in the laptop to stop, heating the laptop, which destroys the hardware itself.

X: Okay. And you also said that information can be obtained from the connection. How would that be?

Y: Sorry, I didn't get the question.

X: Yes, you also said that information can be obtained from the connection. How would that be?

Y: Eh, the information can be obtained from eh, like, masking the connection, so it's not from, from just listening to the connection itself, but from eh, being in the middle. So, instead of eh, visiting the service or the website that you are thinking you are going to, eh, you are using fake eh, a fake website. This website is being created eh, more or less like a VPN, used to show you what you want to see, but in fact you are not getting to your connection. You are getting to your, a fake, yeah, a fake website in the middle.

X: Okay. And how does the threat change because of the VPN connection?

Y: How, sorry?

X: How does the threat change because of the VPN connection?

Y: Eh, I don't understand the, the connection.

X: Okay. You mentioned there could be a fake website-

Y: Hmhm.

X: Does the VPN connection influence that threat?

Y: Yes. So, the VPN does not stop your connection. It only makes sure that you are as secure as possible. [start drawing 4_16]. So, if this website that, the fake website that is created, eh, if this is a new website, and it doesn't have any eh, eh, any eh, people eh, how to say, reporting it. So, no one has reported this website yet, and you have requested an access to this specific website, eh, the VPN search it list, it doesn't find anything, so it makes the connection to this website. If the website is not sending any eh, suspicious files, then the VPN eh, is making this connection. So, the VPN is only stopping eh, suspicious links and suspicious packages, but this is not a common threat, then the VPN is not stopping it. So, the VPN is not 100% eh, risk proof, but it is the most secure way. So, coming back to your question, how, if I have this website, if I am using a VPN, most likely, this request will be stopped here after being checked against the list that are within the VPN. So, if this request if being checked, stopped here, if it is not sent, the request is sent, but getting any suspicious information back, it will be stopped here, and it will not be sent back to the PC.

X: And you say the VPN connection for the VPN server is not 100% secure, what do you mean with that?

Y: Eh, so, one thing that I have learned when I started working on eh, computers, is that if someone wants to hack you, he will be able to hack you. The only thing that you can do is to make his job harder. So, you can install more applications, more, more layers, you can use advanced, more advanced technologies, but in the end if the hacker is experienced and determined to get the information, they will be able to. Eh, the only thing is that you are making it harder and more expensive and more dangerous for the hacker to do so. Eh, so this is for example the difference between using eh, public VPN versus using the corporate VPN. So, if I am using the corporate VPN, I am having a higher level of security. But there is a lot of eh, situations that companies have used secure connections and eh, non the less, there was an attack on them. Of course, the attacks will be less, the losses will be less, but in the end, the VPN cannot stop everything. As I just said, this is one clear example, if this website is created new, there is no report, so this website is not used on

any of the lists here. So, my request will be sent. If I have sent in this request any private information, this private information is already known to the hacker. So, there is always a risk and that's why I said the VPN is not the only layer of protection, you need to have your own knowledge and common sense to stop any phishing e-mail, any eh, virus that could be eh, uploaded to your device.

X: Can you think of any other reasons why a VPN is not secure or not 100% secure?

Y: Eh, no. I believe the, yeah, this, this could be the, the eh, the biggest reason. Just that, just the fact that any smart person who put some eh, defensive measures, there is a smarter person who can defeat those measures. The only way to be 100% secure is not to have an Internet connection. And that's what some of the companies do, they always have servers that are not connected to the Internet. They have their private information on those servers, and keep them offline.

X: You mentioned that there are always smarter persons than you, who or what could be those smarter persons?

Y: Eh, yeah, anyone. So, eh, when I started eh, working in my eh, profession, I had little information, I gained my experience because I have the eh, passion, I have the drive to do so, and I have done the courses, I have obtained the knowledge, I have developed my eh, eh, experience. So, that now I am way better than I was five years ago. The same way goes for hackers. So, there are people who are fully dedicated to break those types of walls. So, no matter how secure and sophisticated, there will be people who are, whose sole purpose is to break those type of eh, secure measures and they are eh, most times succeeding. But of course, the race is that the antivirus companies, the VPN companies, that they are immediately adapting and eh, eh, updating their eh, measures, so that this door is not open for eh, a long time.

X: Could you think of examples of attackers? What kind of categories do we need to think of?

Y: So, one of the most common attackers, known to, to eh, a lot of people are the people who eh, hack the iPhones, of course I am talking about personal use, not the corporate use. So, eh, there are people who break the eh, eh, let's say the, the seal of the company and they call it a jailbreak. A jailbreak is a way of hacking the eh, the iPhone software, so you can install eh, a non-approved applications on the iPhone. So, those people, no matter how many updates the eh, the iPhone company, Apple, is providing for the iPhone, immediately after one week or one month, the hackers are able to break the code and provide an update for this jailbreak. So, this is a clear eh, example of, because there is a need, cause there are people who always want to have eh, unauthorized applications into their iPhones, there are always people who are willing to put the effort to break this eh, code.

X: And does the kind of attacker change because you use a VPN connection?

Y: No, because now, what I am talking about is hacking eh, certain software, this is not related to a VPN connection. But if we are talking to, about hackers that want to hack a connection, or want to hack eh, location, a virtual or physical location, they want to get into your hard drive, then yes. A VPN is one of the best eh, best eh, measures to stop this hacker. Because the hacker here, he doesn't need to eh, break a code, he doesn't need to solve an equation. [\[start drawing 4_17\]](#). He only wants to find a way, a small way, a small door, so that he can access and get inside the VPN or get inside your device, within, through the VPN or outside the VPN. So, eh, this VPN, if it is strong, if it is secure, it is preventing 99% eh, or more of the attacks that could happen. The only eh, small percentage left is eh, reliant on the user himself. So, for- And that's why a company needs to always provide training, needs to always provide local services, antiviruses and anti-spyware services. So, on my laptop itself, I have a smaller version of the antivirus, even though I am using a VPN. I need to have an antivirus on my laptop as a second layer of protection. So, if a hacker was able to hack the VPN connection, he cannot access my laptop.

X: What would be the difference of the antivirus on your laptop and the antivirus in the VPN?

Y: Eh, it could be just a different version. So, the VPN could be using an antivirus of eh, a specific provider, for example [software provider], and I am using [software provider], so I am using a different provider and this could provide eh, just an additional, different list of, of eh, protection. This is similar to any other services in the world. So, when you are having service from two different providers, you are using different features, which provide a better experience.

X: And what would be an attacker's intention?

Y: So, the intention is either eh, let me try to remember, so either for fun, just people who would like to hack, because they want to get the eh, recognition that I was able to do so, or for money, they hack to sell the information or to ask for ransom. Eh, a third eh, party, would be hackers who would like to blackmail, eh, to do an espionage eh, for governmental reasons. For example, [the professional services firm] is doing eh, providing services for governmental organizations, eh, and, so, they are foreign countries could hack to gain those kind of information. Eh, there is eh, the corporate espionage, so eh, eh, competing company who would like to eh, get the information or change the information of competing company. And I believe the last one is just for sabotage. So, for people who would like to destroy eh, specific information.

X: Okay. And what would be an attacker's capability?

Y: It depend on the type of attacker. So, an amateur who would like to prove himself, he is just using his common tools, free tools that are on the Internet, but if we are talking about eh, a government who would like to, eh, for example eh, the example of the American election, where Russia hacked the voting machines or where they hacked the process of the election. So, they have eh, open capabilities. They can do anything that you can imagine. So, it depends on the type of the hacker, the purpose.

X: And what could be the impact of an attack?

Y: Again, it depends on-

X: For [the professional services firm].

Y: Yeah. It depends on the purpose of the attack, it could be just eh, losing eh, a client data. It could be disrupting the business, and it could reach to eh, complete eh, shake in the credibility of the company. So, if it is a small attack on one laptop eh, one part of the client data would be stolen or destroyed, if the eh, attack is on one of the services that [the professional services firm] provides, they can disrupt their work for a day, or a week, or a month, until they are able to resume the work. But if the attack was on one of the critical services, this can make [the professional services firm] lose their credibility against their clients, and their clients are not trusting them anymore. And therefore, the security, of the eh, digital security is one of the top eh, priorities for eh, corporations, including [the professional services firm].

X: Clear, thank you. And this was all about social, digital threats, can you also think of social threats you deal with on a normal day?

Y: Eh, yeah, of course, there is always a threat. The threat of the eh, physical device to be stolen in public transport in eh, my locked car, if someone broke the window, to steal from the house itself. So, there is always the, the eh, risk of eh, the information being physically stolen. There is eh, other risks that are related to the social interaction. And for this, there are always, there is always a training on how to eh, maintain, eh, the secure information for the company and the clients. You are not allowed to discuss eh, client information publicly, with relatives, or with friends eh, in public locations. So, there is always measures need to be applied to protect eh, your, your information.

X: Clear, thank you. That were my questions. Do you have anything about VPN that you think eh, was not spoken now?

Y: Eh, I am trying to think if there is any other threats. Again, at this time, the use of external storage is being limited at the moment. [\[start drawing 4_18\]](#). But there is always the threat of accessing the data from an external source. Eh, either by an external hard drive, eh, an external flash disk, a CD, eh, any type of external eh, device. This could be a threat to the application or the data itself. With the, eh, more and more use of smart devices, you are not able to always use the VPN connection through those devices. so, there is always other measures to provide a secure environment eh, as if it for example, an, an, the mobile connection, you need to install eh, a certain application. So, for example an authentication software, or an encryption software, where it provides an extra layer of protection.

X: Okay, and can you think of anything else about the VPN you want to discuss right now?

Y: No, not at the moment. No, I believe we have covered most of the important eh-

X: Okay, great.

Y: Aspects.

X: Do you have any questions for me at this point?

Y: No, not at the moment.

X: Okay, then so far the interview. I will stop the recording.

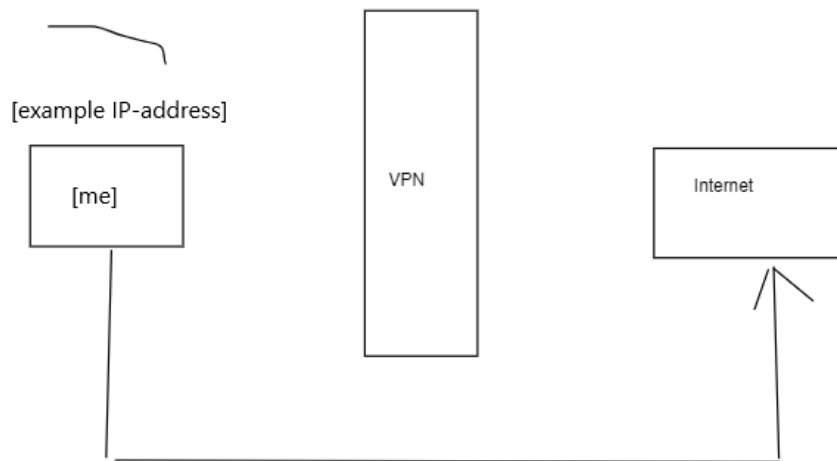


Figure C.4.1: Drawing 4_1

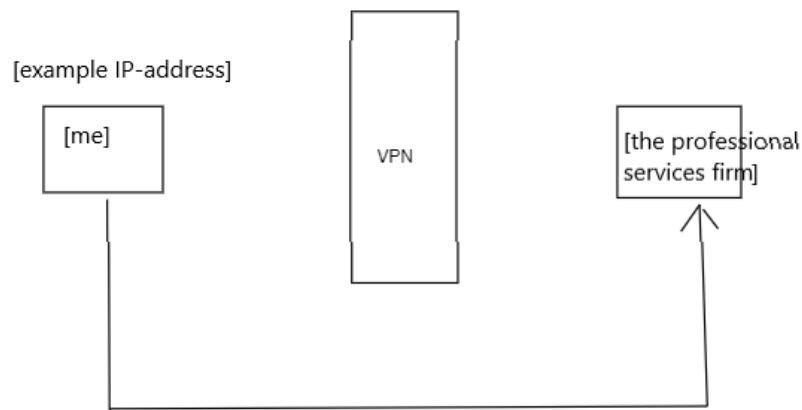


Figure C.4.2: Drawing 4_2

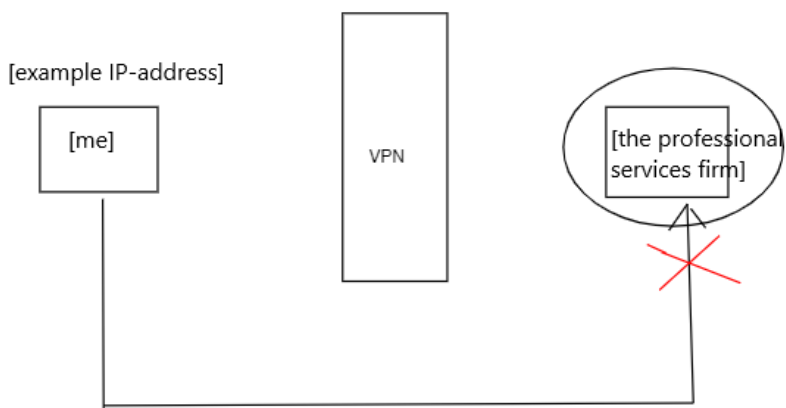


Figure C.4.3: Drawing 4_3

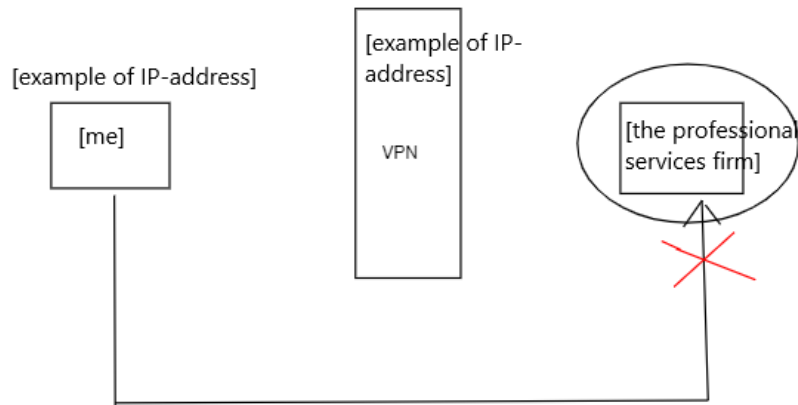


Figure C.4.4: Drawing 4_4

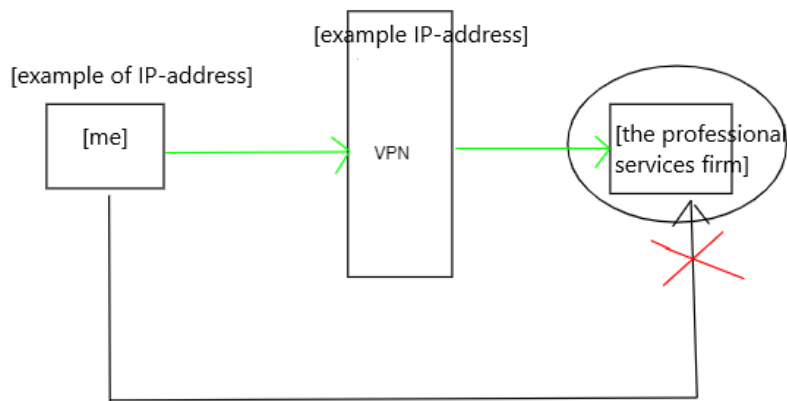


Figure C.4.5: Drawing 4_5

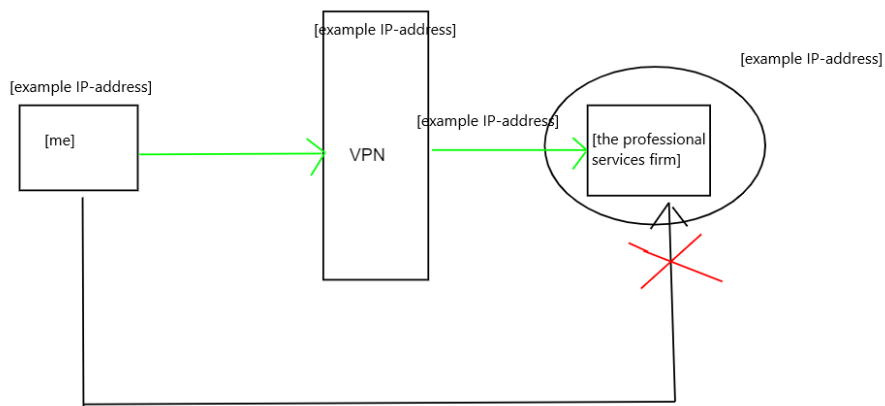


Figure C.4.6: Drawing 4_6

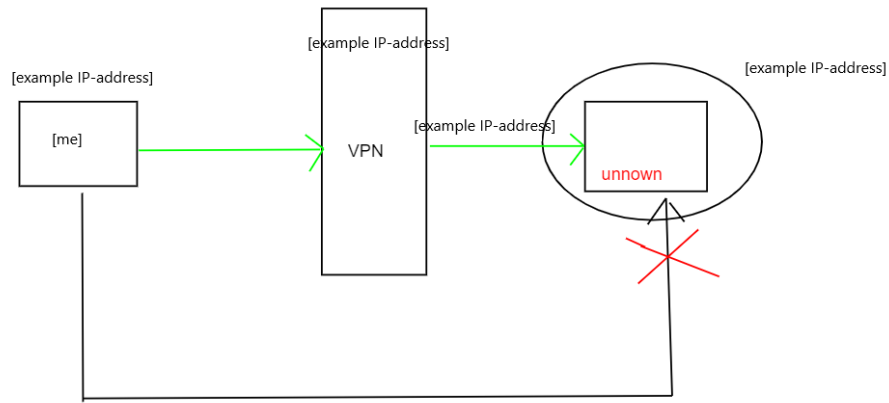


Figure C.4.7: Drawing 4_7

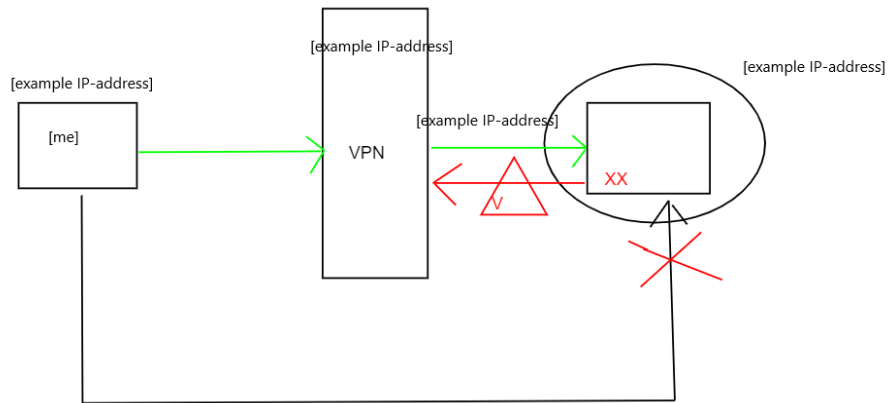


Figure C.4.8: Drawing 4_8

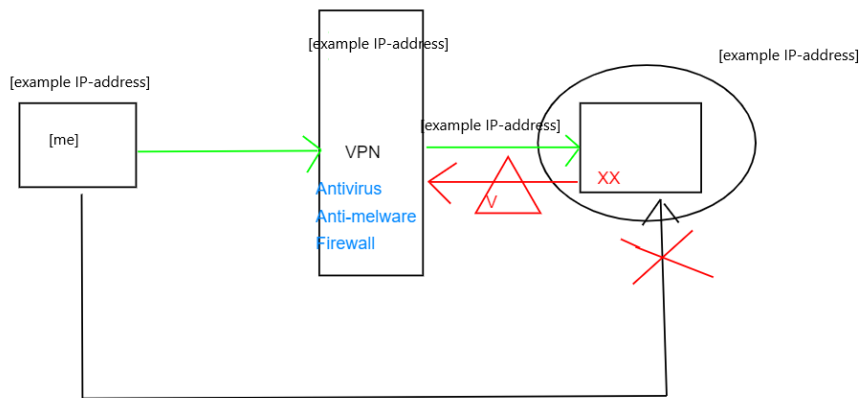


Figure C.4.9: Drawing 4_9

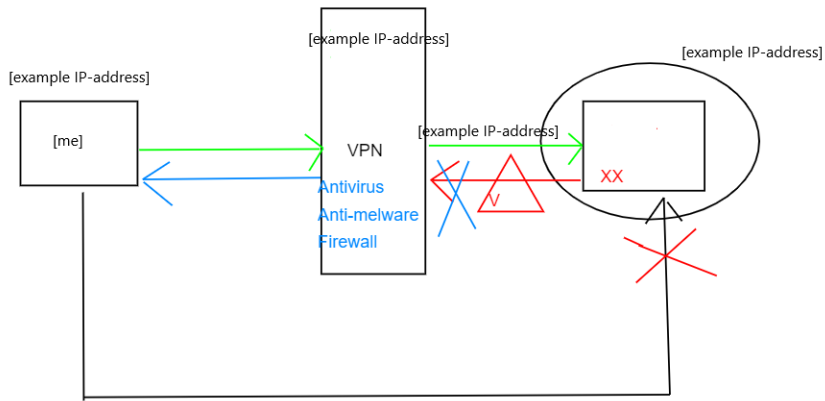


Figure C.4.10: Drawing 4_10

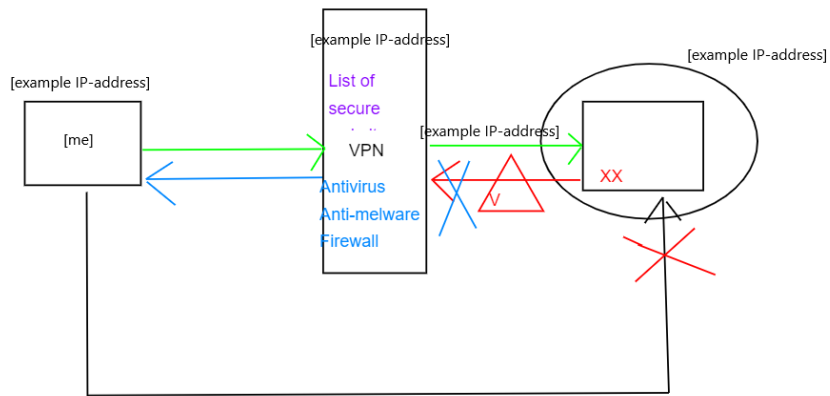


Figure C.4.11: Drawing 4_11

VPN or
Paid Apps
free Apps
your knowledge

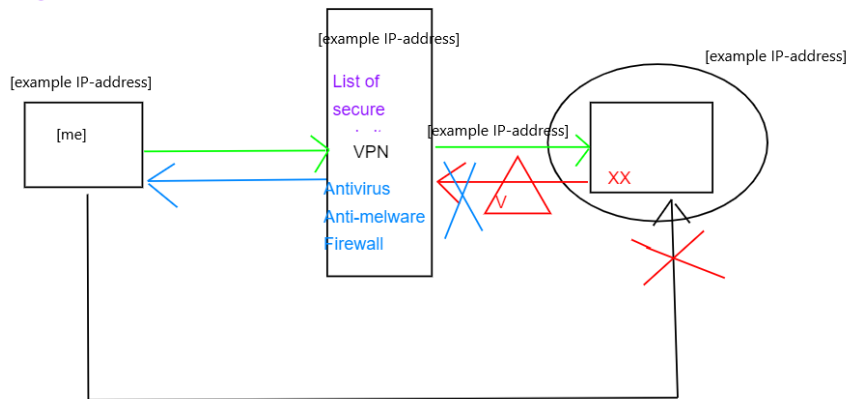


Figure C.4.12: Drawing 4_12

VPN or
Paid Apps
free Apps
your knowledge

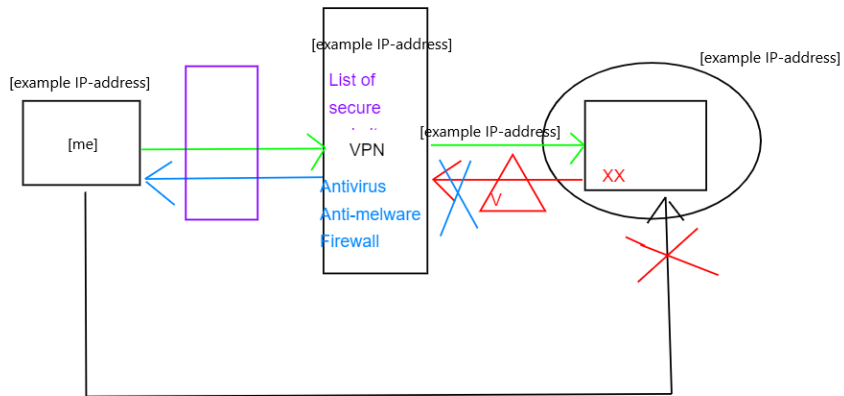


Figure C.4.13: Drawing 4_13

VPN or
Paid Apps
free Apps
your knowledge

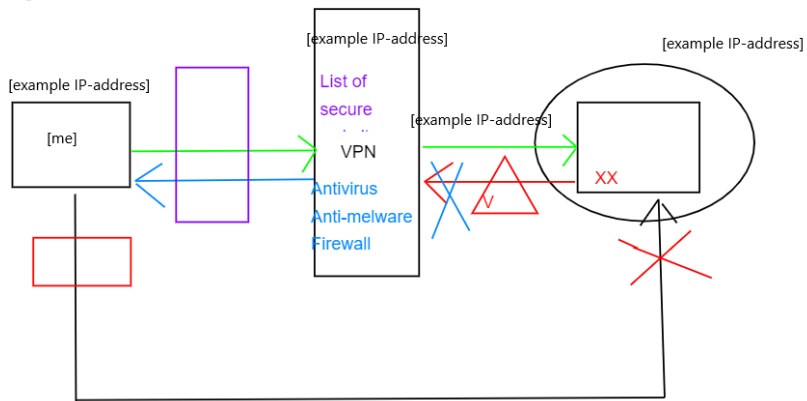


Figure C.4.14: Drawing 4_14

VPN or
Paid Apps
free Apps
your knowledge

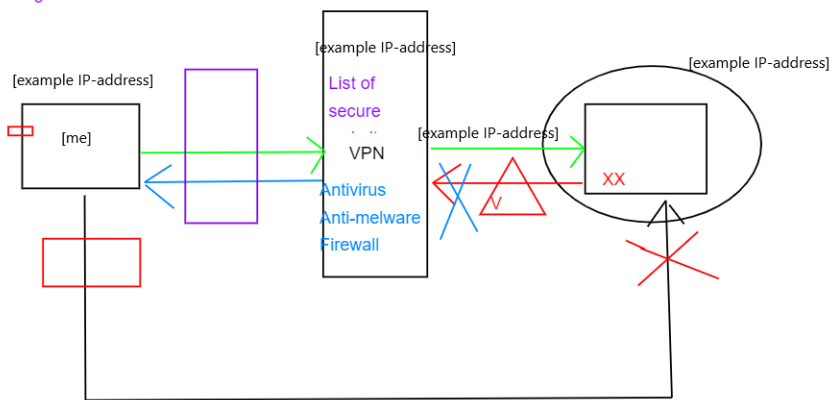


Figure C.4.15: Drawing 4_15

VPN or
Paid Apps
free Apps
your knowledge

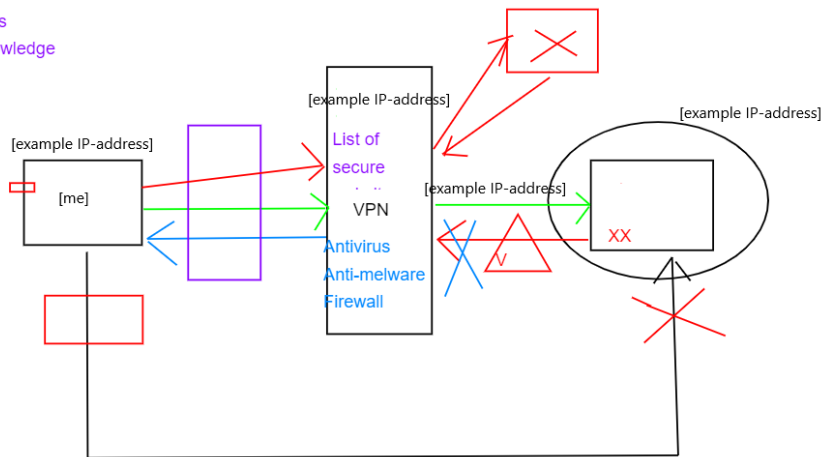


Figure C.4.16: Drawing 4_16

VPN or
Paid Apps
free Apps
your knowledge

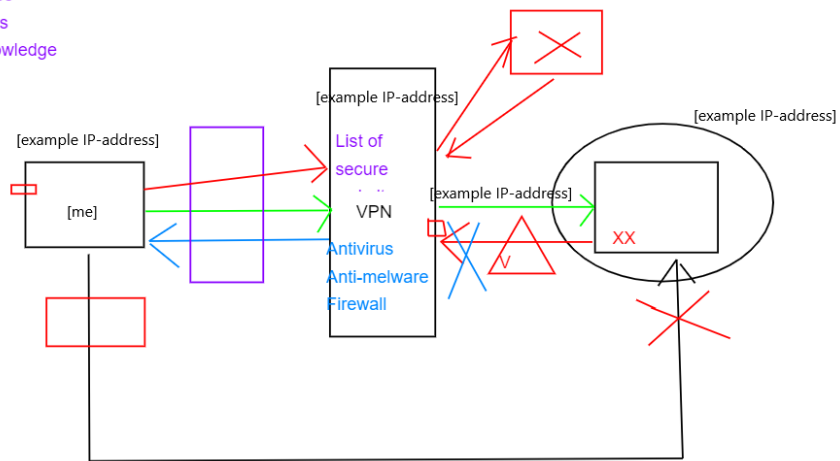


Figure C.4.17: Drawing 4_17

VPN or
Paid Apps
free Apps
your knowledge

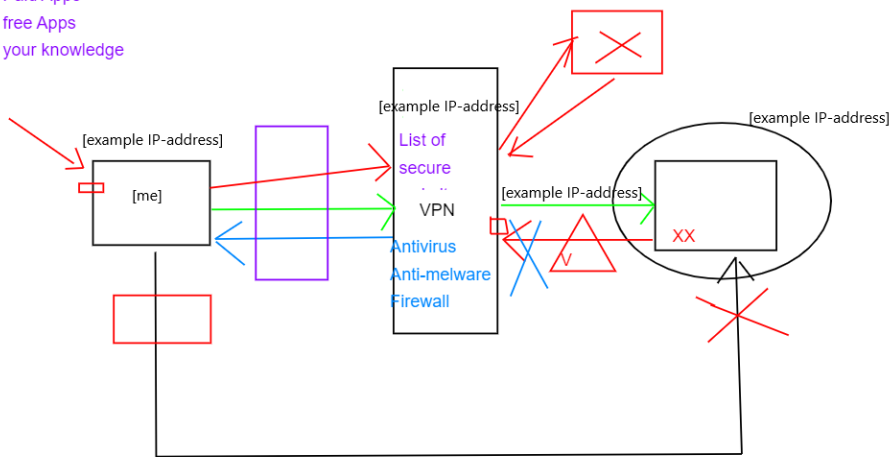


Figure C.4.18: Drawing 4_18

C.5: Transcript Expert 5

Duration: 58 minutes

Language: English
Number of drawings: 12

X: Could you explain to me what a VPN is?

Y: Okay. Eh, so, eh, I would not classify myself as an expert to know about VPN, but the way I understand VPN is like, a narrow, or more like secure tunnel to this Internet traffic online, where the provider and the receiver of information have a secured connection. So, it is like shielding a queue of tunnel through the rest of the Internet traffic. That is how I understand VPN.

X: Okay. And could you explain what you mean with a tunnel?

Y: Sorry, I am having a bit of- Okay, so, eh, let me try if I can draw something. [\[Start drawing 5_1\]](#). What I mean for example is here is the receiver, eh, there is a secured connection established between the receiver and let's say an organization that is providing their IT landscape. So, the people that are from external eh, yeah, environment who do not have access to this tunnel or environment, will not be able to decipher what is being transferred through this channel. This is what I am referring to as a tube. Eh, but it, it's like a way of isolating yourself from the rest of the environment of Internet, that we call like a broad entity where information is freely available. If you want to have a secure connection, then VPN is what most of the companies prefer to go for. But this is how I understand what a VPN should be. I am not familiar with the technical term, but I do understand how it works.

X: Okay. And you say it is secured. How is it secured?

Y: Eh, okay, that's quite a good question. So, I am not quite certain how it is secured in terms of technical terms. Eh, but I know that eh, for example the provider of VPN in this case is an entity, it identifies its provider based on certain parameters. [\[Start drawing 5_2\]](#). I don't know. Like the credentials for example eh, or there is two-factor identification for example. Eh, so, that kind of things. But I do not know what kind of encryption for example works to keep it isolated from other eh, eh, yeah, other attack, well not attack, but other actors. But this is how I understand it. Sorry, I cannot fill in much eh, here.

X: This is quite a lot actually.

Y: Okay.

X: And in what way does the encryption work?

Y: Eh, so, well, there are numerous ways of encrypting, but one of the ways is to obscure the information, or replace them with meaningless eh, how do you say, but eh, yeah, set of letters. [\[Start drawing 5_3\]](#). Let's say one, a, c, b, for example. Yeah, basically replacing a whole sentence with a short encrypted eh, 256-bit of this long strings of mindless characters. And then you have to have a key to decipher what this actually means. So, this is what I understand encryption is. So, if you want to transfer information, this would be one way of transferring to the tunnel.

X: Could you explain to me what this and this is in your drawing?

Y: So, in this case I will say this is me. Sorry I am very bad at writing in this. In this case this is [the professional services firm], who is offering let's say our VPN, that we call [the VPN of the professional services firm]. Eh, if I want to connect to [the VPN of the professional services firm], I will have to first access eh, yeah, the remote connect application where I have to identify myself, say this is my credentials. I think, once I enter those credentials, it also validates that these credentials are valid, only then I get access to this secure channel that is eh, VPN.

X: Okay. And earlier you also mentioned the IT-landscape, what do you mean with an IT-landscape?

Y: Well, so, let's say, [the professional services firm] has a bunch of applications in its landscape, let's say [an internal page], for example. [0:07:24 until 0:07:29 has been omitted]. These applications are not really accessible without a VPN. So, I can use Internet without connecting to VPN. So, I have a broader channel to the rest of the Internet, but if I want to access [the professional services firm] infrastructure, which is basically these applications, our clients' documents are there, [0:07:45 until 0:07:47 has been omitted], eh, mainly sensitive information. Then I have to access it through this channel. So, I was referring to this as the [the professional services firm] IT-landscape eh, where the applications offered by [the professional services firm] can only be accessed through this channel. If I am not located in [the professional services firm] network.

X: Are there purposes for which you use the VPN?

Y: Eh, I am not quite certain. While I personally do not use it for any other applications, because I only have eh, well, [the professional services firm] VPN, [0:08:21 until 0:08:31 has been omitted]. But I can imagine other applications, like yeah, if you want to access, let's say, eh, if you want to eh, yeah, mask yourself as being someone in a different location eh, ... applications, we can always do that eh, by replacing your eh, IP for example. Eh, I can imagine you can also use VPN for that purpose. Eh, by obscuring your location where you are located.

X: How would it work if you mask your IP?

Y: Eh, well, eh, okay, I do not know the specifics, but I will try. [Start drawing 5_4]. So, if, let's say, if I am located here in the Netherlands, eh, I have a specific IP assigned to it. A VPN will allow me to rout my access to the Internet to a different location, to let's say Malaysia, or to China, eh, I do not know if it's possible. Eh, to all these- And then I am able to access another connection, which I do not want them to track me back to The Netherlands, or I want to access eh, data, that is in this country specifically. Let's say [company] eh, in the US for example, it is only available to content in the US. An IP, then in that case, I might be able to access yeah, the network, or the content in the US, by masking an IP which is located in the US, or subsidiaries. But this is just in a very layman's term.

X: Thank you. And are there any other purposes for which you use the [the professional services firm] VPN?

Y: Eh, I am trying to think eh, no. So, that is the purpose, I do not use the [the professional services firm] VPN for any other purposes. I am not sure if you can use it for any other purposes though. Eh, so.

X: And is it location dependent or time dependent when you use VPN?

Y: So, it is not time dependent, but I think it can be location dependent, but not in a way that we might understand it. So, I think our [the professional services firm] server for Europe are located in [place]. So, generally when we connect to VPN, when you open Google, the first reference is [place], where our datacenter is located. So, I can imagine that the VPN is connecting us to the VPN in [place], and then we are able to access [the professional services firm], eh, [the professional services firm] infrastructure. Eh, but it doesn't depend on the country I am located in if I am able to connect. If I have my credentials with me, so, we generally have a [access token provider] token on our phone, which is a multi-factor authentication mechanism that [the professional services firm] uses, if I have my phone, I should be able to connect it to the [the professional services firm] VPN, even if I am in North-Korea for example. So, it is not really location dependent or time dependent.

X: Okay. And could you tell more about that token?

Y: Token, yes. So, eh, it is eh, well, right now I have a software version, but you can also get a physical version. But all it does, it spits out a six-digit number eh, which eh, I forgot the English, but it replenishes itself every one minute eh, that number is specific to my ID. Eh, I am not sure what kind of algorithm they use in that number eh, I think some combinations makes it recognizable that [me] in this case is trying to log in. And this is a number, is this number valid, yes, then it allows me to enter. So, if I am to log in using let's say my colleague's [access token provider] token, it will not work, because the user ID and the number that is entered using the [access token provider] token will not match. But I think this is, this is very specific for employee eh, that they configure the [access token provider] token per employee and the user ID.

X: And on what devices do you use [the VPN of the professional services firm]?

Y: Eh, I use [the VPN of the professional services firm] only on my laptop. Eh, if I have to access [the professional services firm] infrastructure like I said before, to my mobile phone, then we have a special application eh, yeah, I forgot the name, let me quickly look it up. Yeah, it's called [example of mobile application], [example of mobile application] is like a VPN for phone, but once you log into [example of mobile application], you are actually able to access [an internal page], etcetera, only to that portal. So, it doesn't work through web browsers, but there are specified browsers in there that are installed and connected to [example of mobile application]. The [example of mobile application] is like, yeah, it validates your ID and it validates the device on which it is running. Whether it is [the professional services firm] provided device, or it is a device for your own. Eh, if everything goes well, you are able to access it through your phone. If not, if it cannot validate your identity, it will not run. And then we have to use [example of mobile application] to authenticate ourselves on our phones, but it is only one-time process.

X: Okay, eh-

Y: Eh-

X: Sorry, is there anything else you want to add?

Y: No, no, sorry.

X: If we go back to your drawing-

Y: Yes.

X: You say this is you and this is [the professional services firm], could you tell a bit more about how that connection is established?

Y: Eh, can you be a bit more specific? How do you mean how is the connection established? Eh, so, what exactly should I elaborate on?

X: So, if you establish a connection, you said you use software, where in this drawing would we find that software?

Y: Okay, okay. Eh, okay. So, maybe I can try, draw a little bit over here.

X: Or I can provide a new slide if you would like.

Y: Okay, that's also great. Okay, thank you for that.

X: We can go back to the previous slide if you'd like as well.

Y: Okay. Eh, I can't draw anymore, eh-

X: One moment.

Y: Okay, yeah. [Start drawing 5_5]. So, yeah, this might be a very childish drawing, but let's say this is my laptop here eh, my laptop is connected to Wi-Fi that is in my house, eh, and [the professional services firm] is providing their services accessible to web- to a channel. In addition, I need to have my telephone, eh, the app is installed on the telephone. So, what I have to do is when I log into [the professional services firm] network, whenever I have to access the [the professional services firm] infrastructure. Eh, first I have to enter my user ID, after that I have to enter this token ID, that will be generated here, once I open the token it will give me a random number, the random number enters, presented here, and then the information is send over to the router, to [the professional services firm], saying this guy is [me], or whatever my ID is, and this is the token, [the professional services firm] performs some calculations or validates that the ID is correct, because it is the two-factor authentication and then it is send back he, this is okay. And then there is a message that pops up on my screen that says I am connected. And after that I should be able to access all the applications in here. So, this is how I am connecting myself. And this works, not just my home Wi-Fi, but also works with Wi-Fi at a cafe, or any other place. As long as I have an Internet access, I should be able to connect to [the professional services firm] eh, through the same procedure. Or there is an alternate way if people don't want it on their phone eh, or have dinosaur technology, it is also possible to have a token eh, this is a physical token. Eh, all it does, it has a small 16-bit display, like we used to have those in ... And it would do the same thing, it will display random numbers that will keep changing every one minute. If you have this token as well, this token is assigned to your name, you can enter the name here, sorry, enter the number here and then it works the same way.

X: Clear, thank you.

Y: You're welcome.

X: And now on a different topic-

Y: Okay.

X: What is the influence of a VPN on your computer security?

Y: Eh, well, I think eh, I am a bit scared to use VPN from public places eh, like, if I am sitting in a barista café like, [example of restaurant] for example, I am quite worried to use VPN eh, to their Wi-Fi network. Eh, but I am not sure whether that has any impact on my computer security. Well, in a way I am worried that someone tries to target my system, just because I have sensitive information and I am connected to a publicly accessible network, which may or may not be very secure. So, those are my top. So, what I always prefer to do is, I try to use the mobile phone Internet, that is provided by [the professional services firm], eh, to, by connecting to a hotspot. I think that calms my nerves a bit. Eh, I know there are a lot of hacks possible from a network which is not secure, especially when you're connecting VPN and that is eh, so,

yeah, so, it influences my thinking and my mind and how much I am worried to access it through public eh, publicly available network.

X: Why are you scared to use VPN in a public space?

Y: Eh, yeah, because I am partially aware of the kind of attacks that are possible. Eh, I do not know if someone will try to listen or look at the traffic that is going through the channel, if the, if the Internet that I am connecting to is not secure. I do not know how, for example, the cookie and the communication logs are stored. Eh, either way, I am not sure who the Internet Service Provider is for the café, how secure they are, what are their security measures, et cetera. So, all these things really make me worried a bit. I do not know the technical specifics of how a person can attack, but I know it is possible. And hence, the worry that, because I have sensitive information on my laptop, I prefer not to connect to a publicly available eh, network.

X: And then you connect to a hotspot you say.

Y: That is correct.

X: And what is the difference between a hotspot and a public network?

Y: Well, first, the hotspot is provided by eh, a network that is approved by [the professional services firm]. Eh, so, either way there are certain, let's say, contractual obligations, that are in place. I am not sure if for telecom providers it matters if they have a contract with let's say, [the professional services firm] or anyone else, the security will be different. Eh, but, yeah, so, the difference is, I have right now Internet connection through [company]. So, [company] is the preferred service provider for [the professional services firm]. I can imagine [company] taking extensive measures to make sure their, the Internet that they are providing through the phone is secure and it is not easily crackable. Because of their application and ... I do not know if a small café in a corner uses an Internet provider, a service provider that is not really very robust. They do not have proper architecture. Eh, are they, you know, just cheaping out and paying more, just to have a proper security and just making Internet available to people who want to do it. So, those kinds of things.

X: Okay. So, you mean in general you do never use eh-

Y: Publicly available Wi-Fi. Eh, yes. So, if I find Wi-Fi- Well, I mean, in dire need, when there is really nothing that is left, I generally know when the times are bad and you really have to get something done, your data on your phone is gone, than you have no other way. But, if I have an option, I will always tend to avoid it.

X: And you would definitely not use VPN if you're connected to the public Internet connection in that case?

Y: Eh, no. Then I will, well, in the past I have done that once or twice, when there was an emergency and my phone wasn't connecting properly. My Internet wasn't stable, so, at that point I just connected to the Internet, got some stuff done and immediately eh, I kept the amount of exposure time to eh, yeah, as less as possible.

X: Clear. Then for example, if you send an e-mail when you are connected to the public network-

Y: Yeah.

X: Could you explain how that process would go and where they could listen in as you say?

Y: Eh, yeah, so, eh, okay, so, I am not quite certain if they can refer to the e-mails in this case. Eh, yeah, because most of our mails are stored in [e-mail], we do not use web-based e-mail services. I am not able to access [the professional services firm] e-mail through web-based eh, or through browser services. If it was the case, then it is possible that some of the cookies are stored in the browser or yeah, somewhere different outside the [e-mail] environment, that is protected by [software provider]. Eh, then it is possible. But a lot of data that is uploaded to and downloaded from [an internal page] is through web-based services. So, my concerns or the worry- I am not sure if it is irrational or it is rational, but if I am using something through my browser, I can imagine a lot of cookies are being installed by the browser, because the cookie management is quite hectic and crowded. And if I am accessing it through a publicly available network, I am not certain if someone can get access to those cookies or some kind of logs that are registered in the system. That kind of situation. But I would not be worried about [e-mail], or at least that is my understanding, that it is secured in the portal, yeah, so ... client, like we call it. Eh, there is a client that is installed on the laptop, that you open it, and only then can you access the e-mails. So, that is how I understand it.

X: Okay. And if you were to upload information, how would that work?

Y: [\[Start drawing 5_6\]](#). Eh, if I have to upload information eh, okay, I have to first connect to VPN, like this, once my ID has been validated, I go to Internet browser, I type [an internal page] eh, the [an internal page] opens. There is a location where it says upload files, I click on it and then that establishes a connection between [an internal page] and my system. Where I have to look up the files that are located in a specific folder, I select that file and the file gets uploaded. So, there is, this is basically open, well, within the VPN, this is like an open connection, where you are uploading a file from the system to here. I can imagine that the browser through which I am accessing, the browser will store a cookie with certain files with certain information has been transferred, so it works properly, or some functionalities for this to work are stored in those cookies. Eh, if someone is able to access those cookies, then it would be possible to some extent to know what is transferred, not exactly everything, but I can believe this can be useful or information for some people.

X: Clear, thank you. Then on another notion, what kind of digital threats do you deal with on a normal day?

Y: Eh, digital threats as in social media, or-

X: Yeah, as an [the professional services firm] professional.

Y: Okay. Eh, I think I have eh, on a daily basis, my main interaction with digital platforms eh, as [the professional services firm] professional is three or four instances. [\[Start drawing 5_7\]](#). I use [social media platform] eh, to keep in touch with people and I get all these messages. Eh, so this is one platform that I use through [the professional services firm] VPN. Second one is [an internal page], which is my daily driver where I have to work constantly 24/7. And the third portal is [an internal page], this is again a new portal that is being developed by [the professional services firm] [country] eh, to use this portal quite a lot and there is a lot of data that is uploaded to [an internal page] on a daily basis. [0:25:34 until 0:25:47 has been omitted]. So, this is the major digital portal interaction that I have on a daily basis. Yeah, of course, there is always a possibility that I can open eh, let's say [e-mail] as well. Eh, I generally don't use [social media platform], I don't like it. So, I never tend to open it on eh, office or open it at all. Eh, other than that, I think I also open [social media platform], I am sorry, I can't type apparently. Eh, I am trying to think, [social media platform] is sometimes open in case I want to yeah, listen to music or someone sends me a link of eh, cat doing something, then yeah. So, these are the regular interaction that I do eh, on the digital platform.

X: And you use VPN for this purpose?

Y: Well, I need VPN only for these two applications, I do not need a VPN for all these purposes. But I do not keep switching on and off. Once it is the start of the day, once I connect my laptop to VPN, after that all of this is within VPN. Although I do not need VPN for this. I can do it without connecting. So, over the weekend, if I am using my laptop eh, for personal use, I never connect to VPN, because then my laptop is simply my private laptop. I do not have to access [the professional services firm] systems. I can just do with the Internet by using my Wi-Fi and I don't need any of the codes to work.

X: Clear, great. And how does this threat or what- Are these also digital threats you would say?

Y: Are you asking if these systems are threats to [the professional services firm] systems?

X: Yes, because eh, I asked what kind of digital threats do you deal with on a normal day- O, you thought of other threads. Eh, okay. I mean threats as in, well not so, okay, it is a bit strong word, but as in attacks.

Y: O, attacks. Okay, I am so sorry, I misunderstood.

X: No worries. I get the confusion.

Y: O, I am so sorry, okay.

X: No problem, no problem.

Y: Eh, okay. So, I think the major threat, I do not have to personally deal with, but something that I always have in the back of my mind, is eh, yeah, something let's call it eavesdropping. [\[Start drawing 5_8\]](#). Eh, I am not sure if you are aware of that term. Eh, eavesdropping is someone trying to eh, yeah, read over my screen or listening to my telephone, when I am talking to a client. Since I have sensitive information open on my laptop, I always tend to use a privacy screen eh, yeah, whenever I am in public. I am also I think, I potentially deal with something called a man-in-the-middle attack. [\[Start drawing 5_9\]](#). Eh, yeah, this is quite eh, this is quite a high risk for a situation like this, where there is a VPN connection. [\[Start drawing 5_10\]](#). I am sure if we run a pentest on a [the professional services firm] system, there can be some vulnerabilities that can be exposed to either this kind of attack or something, yeah, this was what I was

referring to. And someone tries to snoop in and read some information by being, yeah, an invisible party and trying to act as a person they should not be. This is one of the digital threats I think all of us deal on a regular basis, when we're trying to connect to a Wi-Fi that's not secure. Eh, I think the other threat that we have to deal with on a daily basis is legacy systems. [\[Start drawing 5_11\]](#). [0:29:47 until 0:30:19 has been omitted]. Dealing with legacy systems is quite risky, especially to a VPN, some services don't even work. And they are not really built to send out these kinds of attacks. So, when dealing with these kinds of systems, it is always a worry what to do. [0:30:33 until 0:30:47 has been omitted]. Eh, o, yeah, there is an alternate possibility of phishing e-mails. And [the professional services firm] seems to get a lot of it, I think we get a lot of these eh, mindless e-mails saying please I just offer this course. I can imagine they are trying to add a worm to [the professional services firm] network that keeps multiplying through different devices, I am not sure if anyone opens the links what happens. But we get a lot of phishing e-mails to see if they can steal credentials, they can gain access to the network. I can imagine this can be easier if you're connected to a non-secure VPN. So, that is something that we have to actively keep an eye on. Eh, another digital threat is, well, I mean this is something that everybody has to take care of themselves, but eh, there are a lot of data leak incidents. Well, not a lot, but it is quite a serious issue, because we deal with four or five clients at the same time, and you can imagine the nightmare if you send data from one client to the other. You have to raise a data privacy incident and we know the recent AVG regulation, that makes it even more difficult to deal, time-consuming, you have to be extra careful who are you sending the data to. And that kind of stuff. So, these are the main digital threats that I worry about every day. Including VPN and excluding VPN.

X: Yes. And you say that using a VPN when you need to access legacy systems is an extra risk, could you explain why that is a risk?

Y: Eh, yes. So, I think eh, let's say, [0:32:25 until 0:32:46 has been omitted]. Accessing that application through VPN is quite secure, because the application itself has a robust eh, authentication mechanism first. [0:32:55 until 0:33:06 has been omitted]. But again, it is not possible to log into the legacy systems in this environment, for that purpose we have to be on-site. [0:33:13 until 0:33:30 has been omitted].

X: Clear. And you say you get a lot of phishing e-mails, do you mean phishing e-mails at your [the professional services firm] e-mail?

Y: Yes. Eh, so, I think, I am not sure if you can answer this question, ... people as well, but eh, I think I get a lot e-mails eh, from specific eh, training company from [country], but we get all this trainings platforms, please look at these others, they might also be interested in that. Eh, if you look that eh, organization up and eh, eh, on Internet it kind of, it looks a lot like sham and it looks like a phishing e-mail, that you wouldn't click any links on it. Eh, that kind of stuff. I know one of my colleagues was also running after one of the companies to remove all of his personal data eh, stating the AVG, yeah GDPR regulations, saying he, I have the right to be forgotten, please delete all my data and I do not want to receive any information from you et cetera. So, I think I am sure that other colleagues that you interview will also agree to this point that they get a lot of phishing e-mails. There is at least one per day.

X: And this was about social threats-

Y: Yes.

X: Eh, or digital threats. Eh, how does the threat change because of the VPN connection?

Y: Okay. Eh, I am trying to think, I am trying to go into my technical knowledge to see if I can make a comment. Eh, so, I think, I know that eh, that an attack like MITM, a man-in-the-middle attack is possible eh, if you're using VPN. Someone can impersonate you and then try to access information, but I do not know how the threat landscape changes eh, because of using a VPN. Eh, specifically speaking, so, I am, because I am not really, technicalities for cybersecurity, I can just say that okay, it is possible to create an MITM attack eh, if you're using a VPN. But beyond that I am not able to add anything valuable. Eh-

X: No problem. Could you explain how a man-in-the-middle attack would work when you are using a VPN?

Y: Okay, so, the first thing any attacker would want to initiate an MITM attack eh, would be to gain credentials. [\[Start drawing 5_12\]](#). Eh, yeah, yeah, if you want to access the same portal, the only thing that recognizes me is my user ID for example. What is the user ID. If I have a password to the system, he would want to know what the password is. Eh, if it is not encrypted than it is a big problem. And then the second

layer of security in this case is the [access token provider] token. So, if he is able to decipher how these number work, then he should be able to gain access to it. Eh, or, I, okay, and I am getting into technicalities, I am not sure if he can act as a silent listener in this case, but eh, this is how I understand it. He might have to phish out my details eh, from my services, when I enter these details in my browser for example. If there is eh, yeah I am not, I forgot the technical name for it, it is like a phase blocking, where all the information is collected eh, in a **tile or sheet(0:37:17)**, like a tracing eh, that is how I can imagine he can eh, impersonate me and be connected to [the professional services firm] network.

X: Okay, thank you. So, this was around digital threats. Do you also have to deal with social threats in a normal day?

Y: Eh, no, on a normal day no. There are eh, I have eh, I have never had a situation where someone was trying to follow me or someone was trying to eavesdrop. It is eh, it can be a challenging situation if you are working on some sort of project and if they found out the information is clear that someone is working at this is a [the professional services firm] laptop that can hold information, then yes. But, on a regular basis eh, there are not so many social threats that we deal with except these phishing e-mails of course, but eh, yeah, so, yeah, that's the major challenge. I know a lot of people have their laptop stolen eh, when I say a lot, it is more like one or two percent eh, but well that can be attributed to general thievery. Just because people like stealing stuff eh, we're not specifically targeted because it is a [the professional services firm] laptop. That's how I understand the situation that would go down when people are sleeping in trains for example and the laptop is stolen eh, et cetera. But these are the social threats that we deal with on a regular basis.

X: Okay. And does the VPN connection have any influence on this?

Y: Eh, I think yes. It has a big influence. Even if someone is able to steal my laptop, they will not be able to connect to the [the professional services firm] systems without the [access token provider] token, which is on my phone. Or in this case- Or in the case where it is a physical token, this, the thief will have to steal both of them to be able to access [the professional services firm] systems. So, I think VPN is very useful in this case, because it is a secure connection eh, and one part of the token can still be with me, and that is my phone. And again, my phone has this secure two-factor eh, well, sorry, my [mobile phone] has a lock on it, right, so, no one can access the phone either way. So, no one can reach the digital data and security and [access token provider] token. Eh, however, if you have a physical token, if you are like most of the people, who keep their physical token also in the laptop bag, which means if your laptop is stolen, your secure token is also stolen. Then, the person only has to know your password and he will be able to log into all systems at one time. Which is quite risky. That is why I called it a dinosaur system in the first, I think everyone should switch to a phone-based [access token provider] token. Eh, it has an additional layer of security.

X: Okay. And if you think about these digital and social threats, who or what could be an attacker behind the threat?

Y: Eh, who or what could be behind the threat. So, people on the attack side, right? Who would want to do it? Is that what you mean? Eh, hallo? I'm sorry.

X: Sorry, that is what I mean.

Y: Eh, okay, so, to clarify the question once again, you want to know eh, who could be behind these kinds of attacks right, from my perspective.

X: Yes.

Y: Okay. well, eh, eh, okay, that's a good question, eh, well, eh, I would imagine some portion of people being eh, yeah, eh, doing it for the sake of adventure. I'm not particularly certain if someone is specifically trying to target and phish out important e-mails, to get some sensitive information from clients. But I think a very small portion of attackers can specifically be targeting that information, that they already know. So, the one thing that most of the people outside, they are not in [the professional services firm], they do not know what kind of sensitive information exists. So, the only idea that there is some sensitive information at [the professional services firm] for the clients [0:41:37 until 0:41:38 has been omitted], but they do not know what kind of information might exist. So, it can be a very blindfolded attack, let's see what we can get out of the system. However, there will be very small percentage of people who might have all this information and he precisely also what he wants from this kind of attack. In that case we would classify it

as a high-risk attacker. Others are just, yeah, the technical term, scriptkiddie, who just want to see he, can we can we bring down someone like eh, the eh, the DDoS attack on eh, Ziggo, eh, I don't know. In 2015 or '16 they brought down the services for Ziggo, just because they weren't taking care of their customers. Something like that. But nothing very specific, like terrorist or eh, specific governments targeting [the professional services firm] specifically, nothing that bad.

X: And what could be an attacker's intention?

Y: Eh, either cause disruption in the services, or eh, gain access to certain valuable information, to see what is important and what is not. So, I can imagine that with many points in time, especially a [role] e-mail, mailbox or his communication with the clients, a [role] laptop is very valuable, because it contains all confidential information, like [0:42:57 until 0:43:03 has been omitted]. Now all this information will not be available with me, but it can possible be available to [role]. I am just guessing, I don't know. I think this is something they might be interested in, [0:43:13 until 0:43:44 has been omitted]. So, if you want to gain access to this world of data from which is very sensitive, then it can be a minefield. You can sell this data for quite a high value on the black market, so this could be something that the client might be interested in. O, sorry, not the client, the attacker.

X: And what would be an attacker's capability?

Y: Eh, how do you mean capability?

X: What would they need to be able to do eh, to make an attack successful? Or what would an attacker's background be?

Y: Eh, I would consider [the professional services firm] technical system to be quite eh, robust. We have lot of layers of security to prevent these kinds of attacks, we also have a special security eh, yeah you call it a SOC organization eh, which has all these alerts popped into the system. So, whenever you do some kind of fishy activity, you will immediately get a call from [country] team, there is a specialized team in [country], who does the monitoring on all these kinds of incidents. So, if you want to avoid all these, I call it a minefield, if you want to avoid this minefield, you have to a lot of expertise on how to navigate across a corporate environment. So, let's say if I read a book, let's say red hat or red teaming strategy, I will not be able to do it myself. I believe someone who is either a certified hacker or has a lot of experience dealing with complicated systems, who knows his way around all this security monitoring and incident monitoring eh, only then you are actually able to extract this information. Eh, of course you also have to be a social engineer, to be able to get this information, like the access information from employees. Like most, I can, I would, I pray that all other colleagues that you interview are also aware of these kinds of attacks. We do a lot of training eh, to keep yeah, be aware of your surroundings. Who is looking at this screen for example. So, I would expect everyone to be responsible and have this in the back of their mind. So, I think the person has to be quite smart, he has to be, have some technical background, that they can navigate across the environment, it is not that easy. Yeah.

X: And does the kind of attacker change because of the VPN connection?

Y: Okay, that's, well, I mean, I am not sure if it changes eh, because, well, I mean I do not know any company that does not well, there are companies that do not offer VPN, but a sophisticated attacker would be ready to attack a VPN louder than attacking [the professional services firm] network directly, because doing that is quite impossible going into the datacenter for example, trying to crack into the [the professional services firm] office network in the offices, which is quite a difficult eh, strategy. I think the easiest way for an attacker to do is to attack the VPN, because it is remote and it highly depends on how the VPN is connected, how secure the Wi-Fi to which it is connected. So, that is how I believe an attacker might change. Yeah, it is easy to use a smart intelligent attack rather than use a brute force and break into the datacenter or crack open eh, the [the professional services firm] network inside the offices.

X: Thank you. And what could be the impact of an attack? The impact for [the professional services firm]?

Y: O jeez. Okay. Eh, I think it would be quite significant. Eh, if, well, if the attacker is successful to attack our network, it would not result in a public humiliation, unless the incident becomes public. However, if there is a data leak incident, if the attacker is able to steal private information, [the professional services firm] is obligated to report this incident to the data officer, who is within our firm or who is external I don't know, within 72 hours what that impact, what impact it has on our clients, [0:48:04 until 0:48:22 has been

omitted]. So, I think in that cases the consequences of these attacks will be quite higher. But, let's say, someone is able to crack into VPN and steal someone's personal ID or network, he might not be able to do much. So, this incident might not be reported outside, unless the attacker makes it public himself. The impact in that case again, like I said, there is security monitoring. So, if there is anything fishy going on, it might be sensed by this team in [country], and immediately they will try to block the account. Or, yeah, it happened, one of my colleagues eh, he was trying to eh, access a website, that website had a worm or some kind of pop-up, which was very malicious. After the pop-up opened, he got a call within a few second from the [country] team saying what the hell are you doing? We got a security alert and this is not okay, please close the website and restart the system. So, we have this kind of measure in place eh, but to prevent any further impact. But a data leak can have a significant impact eh, on our reputation. It results into eh, yeah, the attackers stealing something from us. It will not go down very well. It will result in financial losses, it will also result in a lot of reputational damage, there will be a lot of eh, extra work that needs to be put in after that, to make sure this kind of situation does not happen again. Eh, I can also tell you about recent measures. [0:49:47 until 0:50:18 has been omitted]. Eh, so, yeah, sorry, I am speaking to much, okay.

X: No, that's not a problem at all.

Y: Okay.

X: Could you think of any other possible impact of an attack?

Y: I am trying to think of an impact of an attack. Eh, I am not certain if the target, if the attacker would actually target employees individually to blackmail or something. Because most of us do not have any sensitive private information on our office laptop, I surely hope so, but I can imagine that if someone gets a hold of your laptop and is able to access your laptop and you lose all the sensitive information that is in the laptop, like your pictures for example, with your loved ones, et cetera. The attacker can use it to blackmail you eh, but certainly something like that. But other than that, I am not aware of any other impact that it can have on [the professional services firm] or on the personnel.

X: Clear, thank you. And you mentioned a bit about it already, but if we look at the VPN connection itself. How secure is the VPN connection?

Y: Eh, it depends how you measure it. So, eh, it depends what you call a very secure connection. Eh, I mean, I don't know the technicalities, I don't know if there is a scale to measure. But, if I am connected to my home Wi-Fi and I am connected to VPN, I would consider it a very secure connection. Eh, but I am sorry, I am not able to answer this question probably, because I don't know what to measure it against.

X: Not necessarily on a scale, but more eh, for, could you think of reasons why the VPN connection is not 100% secure?

Y: Eh, yeah, well, I mean, so, eh, yeah, I am not quite certain why. But I can imagine when you are remotely connecting the system has to trust the person who is connecting is actually [me]. In this case it is me. Eh, when I am in [the professional services firm] office, if an unknown person is sitting on someone's floor, [0:52:40 until 0:52:46 has been omitted], trying to represent [me] for example, then it is a different situation. But I mean, VPN is only as secure as long as your credentials are with you and not with someone else. If the data, if I share all these details with [partner], is also able to say [partner] is [me] and [partner] is connecting to and accessing all the information. So, it is only as secure as responsible people are with it. And the technicality, because you are using network that is not [the professional services firm] eh, that is one vulnerability in place. But I kind of touched upon that before. But I would not have anything to add beyond the points I already mentioned.

X: And you already mentioned a bit about it as well, how do your actions change because of these insecurities you mentioned?

Y: Eh, how would my what change, sorry?

X: How would your actions change?

Y: O, my actions, well, my interaction with [partner] about my work is eh, well private. I sometimes, eh, yeah, so basically, first, we do not share the same laptop. [partner] does not get to access the laptop eh, when we talk about work it is also very formal. It is nothing more details involved, because eh, if, if all the details are shared with your partner or anyone else, it is quite easy for an attacker to fish those details out from your partner for example. But, in the end, in this case for example, [partner] does not know the

password to my system, [partner] cannot access it, [partner] doesn't have access to my phone, so [partner] cannot know the [access token provider] token ID. All this information I mean, that is something that actively I try to do. I isolate the work environment away from the partner, so that the details are only limited to me. Eh, that is one type of action that I do. I actively avoid clicking on any other link, even if those links are sent by my colleagues in the e-mail. Yeah, you can always copy a link and put in a, on these Internet websites, where you can see is it fishy or not. But I just tend to avoid doing that in any situation. So, these are the measures I would take to eh, even give small eh, yeah, small chance for the attack.

X: Okay. In that case I am sorry for sending a link to you in an e-mail.

Y: It's okay. I put that link in a, in the checker before I went to it. [0:55:14 until 0:55:26 has been omitted].

X: Makes sense.

Y: Okay. It's okay.

X: These were so far my questions, do you have anything that we did not talk about, about VPN?

Y: Eh, yeah, so, eh, well, I do not have questions right now, but it's just more like a remark. So, I know that VPN is kind of the only resource we have right now, especially in a situation like Corona crisis, it is one of the only solutions we have right now. Is to connect through VPN. So, even if it is very eh, how you say, weak, well, not really weak, but if it has vulnerabilities, we have to live with it and we have to make sure that we are as employees or as people who are using VPN, we are responsible with it. Because either way, we do not have an alternative solution to properly authenticate, you give a secure connection in a way that no one else can listen or see what is being transferred, et cetera. Eh, I am not sure if there is eh, another kind of technology that is being developed other than VPN, but this is all we have right now, and I think it works well so far. I am not certain if there are any severe vulnerabilities that have been discovered for it, or if there is any kind of research going on. But I am sure if someone would be able to crack VPN code and coming here, then we will have to move to a new technology. But this is the best we have so far.

X: Okay. Do you have any other questions for me?

Y: Well, I am not certain if my questions were useful to you, because I would not consider myself as a very technical competent eh, individual. But I did my best to share all the insights that I can tell from using the VPN. Eh, but eh, eh, yeah, I mean, I am not certain how I can ask more information. But if I have a need for any questions or anything I will definitely eh, ask you about it. At the moment I do not have a question for you.

X: Okay, then I would like to thank you a lot for your participation.

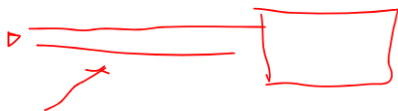


Figure C.5.1: Drawing 5_1

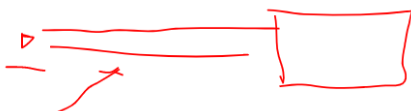


Figure C.5.2: Drawing 5_2

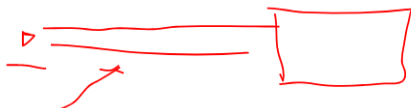


Figure C.5.3: Drawing 5_3

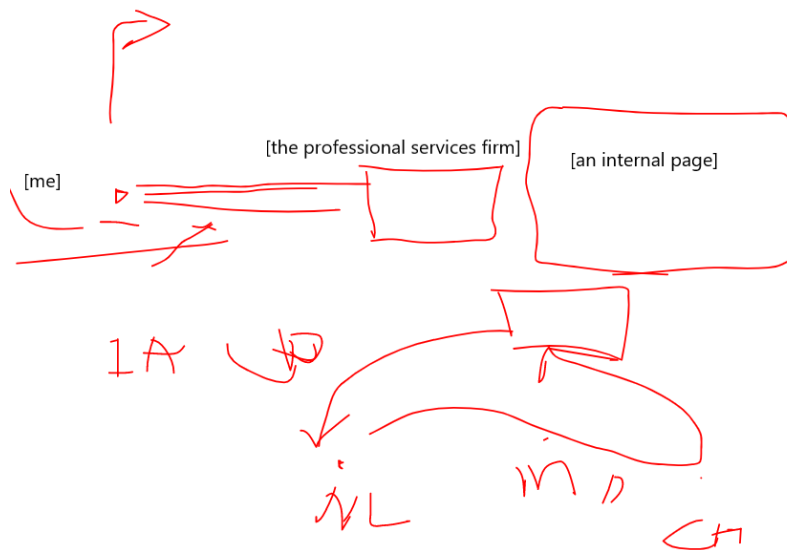


Figure C.5.4: Drawing 5_4

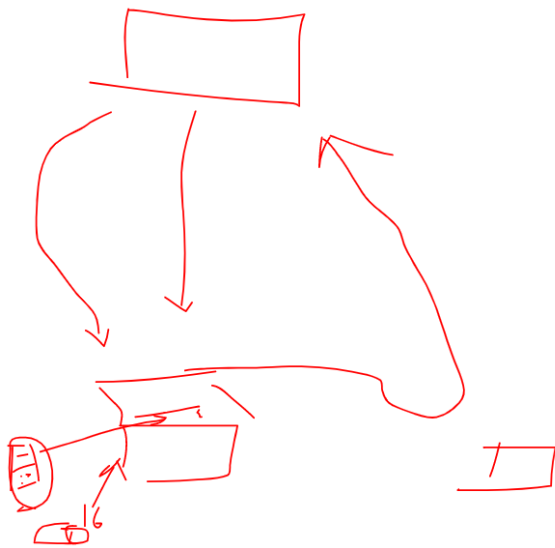


Figure C.5.5: Drawing 5_5

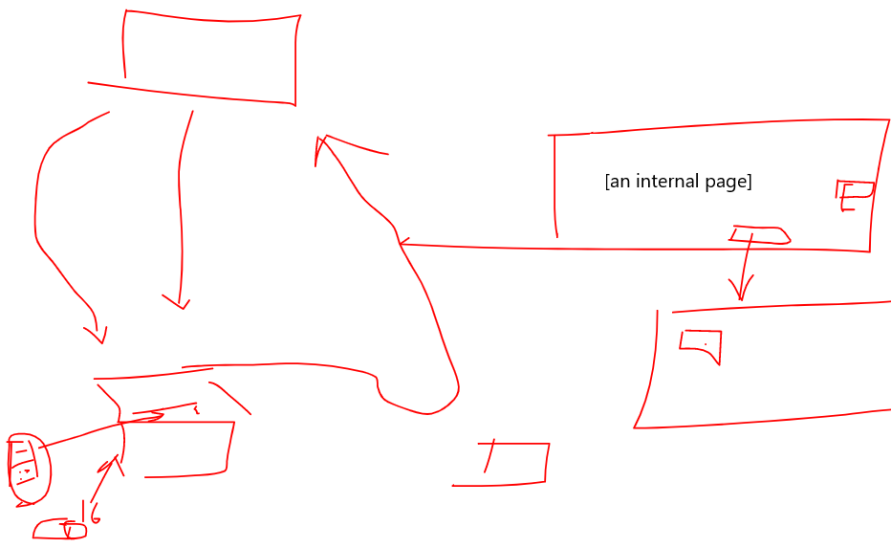


Figure C.5.6: Drawing 5_6

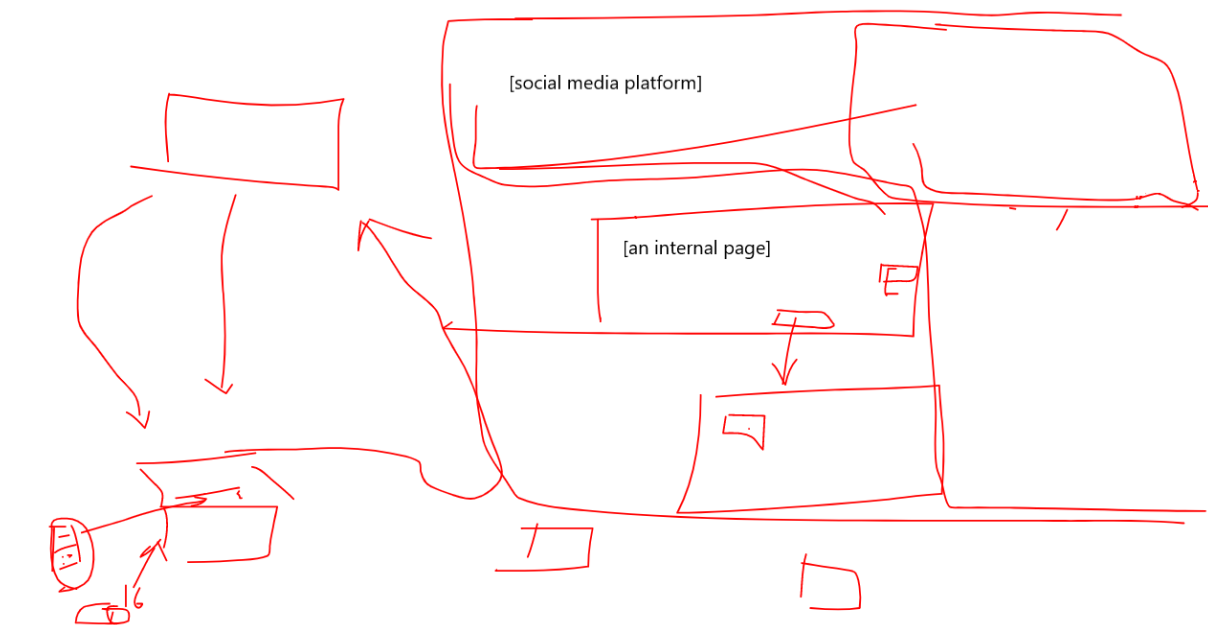


Figure C.5.7: Drawing 5_7

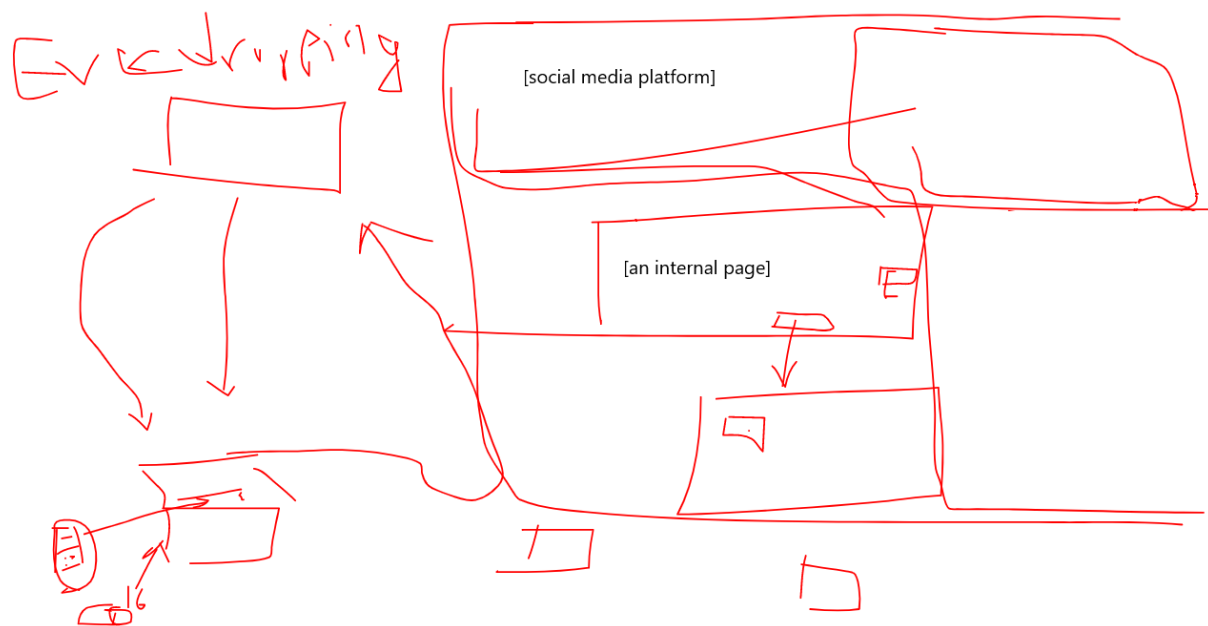


Figure C.5.8: Drawing 5_8

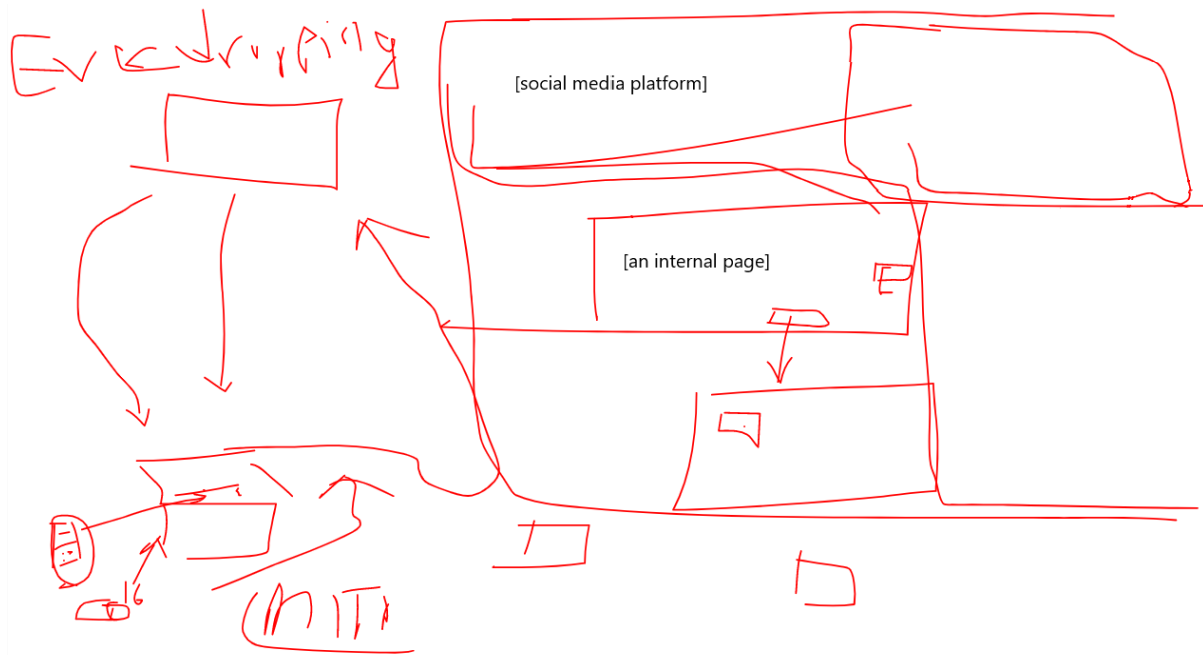


Figure C.5.9: Drawing 5_9

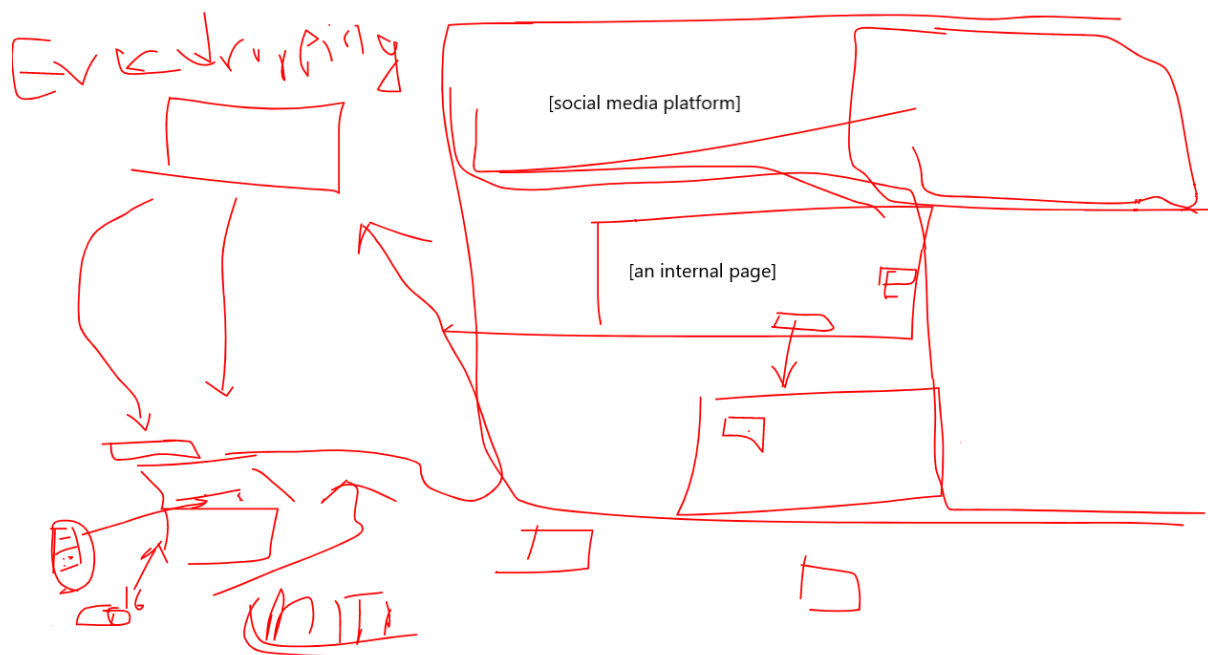


Figure C.5.10: Drawing 5_10

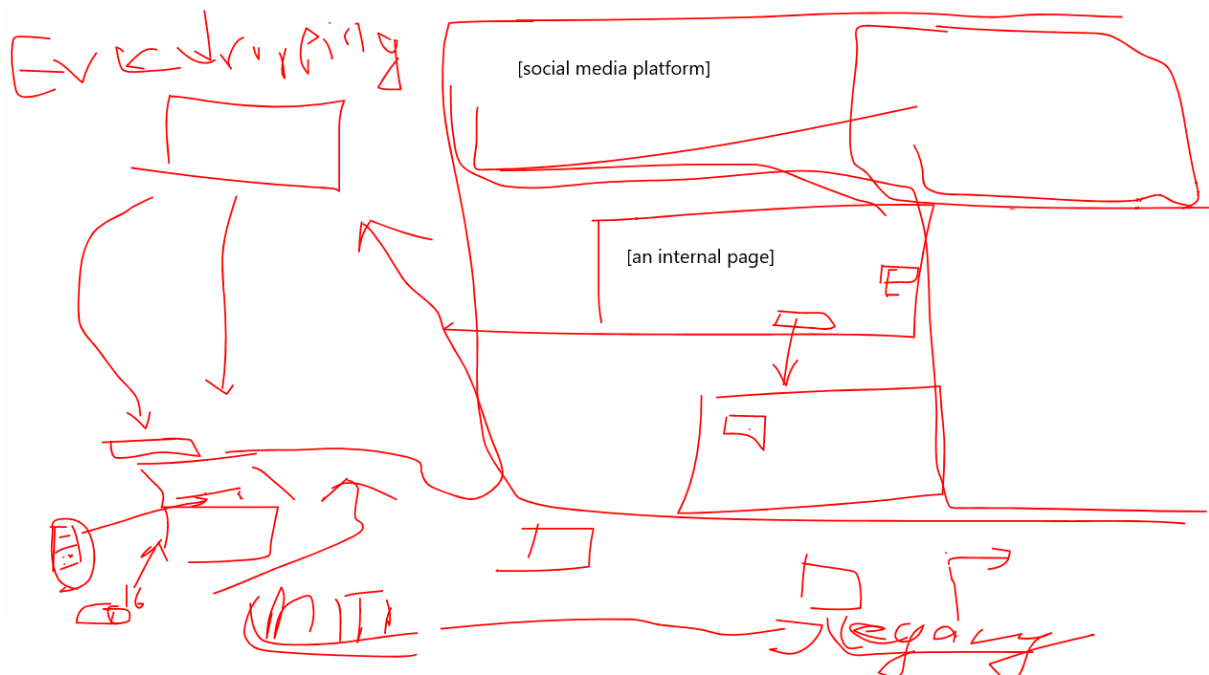


Figure C.5.11: Drawing 5_11

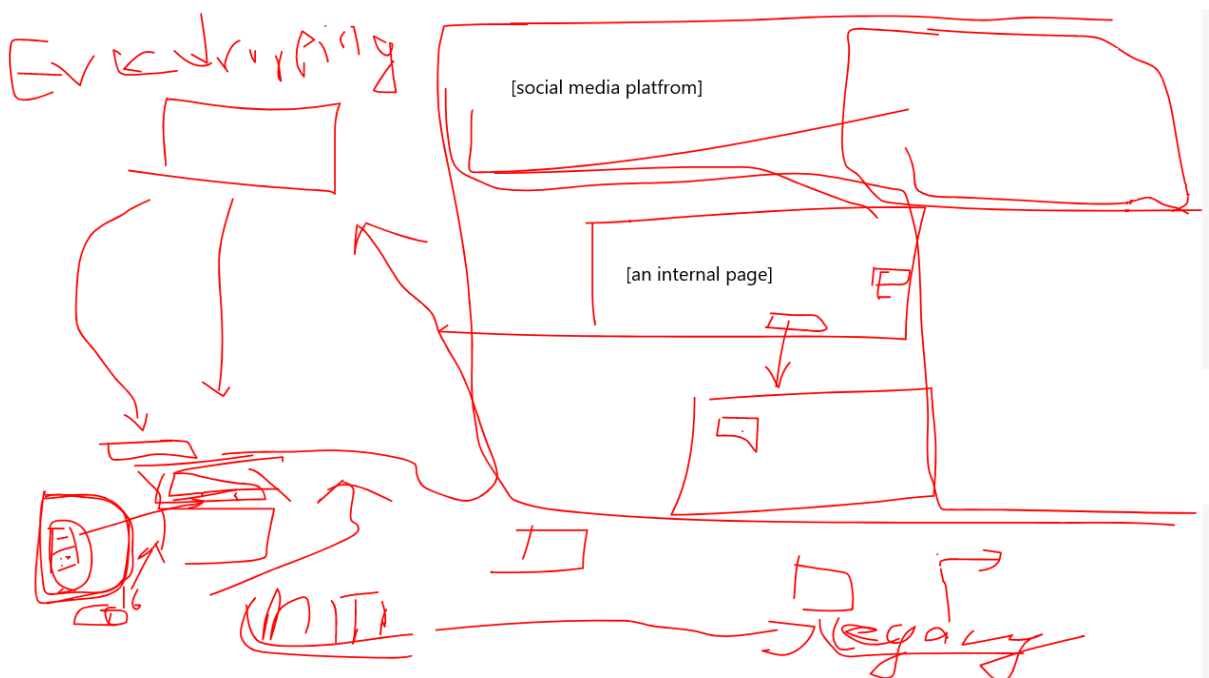


Figure C.5.12: Drawing 5_12

C.6: Transcript Expert 6

Duration: 29 minutes

Language: Dutch

Number of drawings: 2

X: Dan begin ik met een hele open vraag. Kan jij aan mij vertellen wat een VPN is?

Y: De afkorting staat voor Virtual Private Network als ik het goed heb. Eh, een VPN is in principe, ja, is een mechanisme om een soort van veilige verbinding te maken tussen eigen laptop en een externe omgeving. Dat is hoe ik het zie. En daar zit dan een VPN-verbinding tussen om het ja, meer beveiligd eh, te maken. Eh, en dat is dan ook wat op alle [the professional services firm] laptops eh, uiteindelijk ook staan met die eh,

die code, die je ook- Die [access token provider] code, die ik moet invoeren anders kom je niet op het netwerk van [the professional services firm]. Dus dat is hoe ik een VPN zie, dus eigenlijk een soort van, zoals ik zei, een beveiliging om, om te zorgen voor een veilige verbinding tussen je eigen standalone laptop die je gebruikt en tot een extern netwerk. Dat is hoe ik het zie.

X: Kan jij vertellen hoe deze verbinding beveiligd is?

Y: Oeh. Eh, ja, ik neem aan door middel van, ja, hoe, en dan het je het in de zin van technische zin, of-

X: Ja, of op een andere manier. Je zegt dat het een veilige verbinding is, wat bedoel je daarmee?

Y: Nou ja, dat je slechts, doordat je dus een app hebt op je telefoon met daarin dat je een code krijgt, die niet iedereen zomaar kan krijgen, dat je slechts op die manier in kan loggen op het netwerk. Dus in die zin dat het technisch wordt afgedwongen dat je eerst een code, of een software token code, nodig hebt, voordat je überhaupt op het netwerk kan komen.

X: En je maakt verbinding met een externe omgeving, wat bedoel je daarmee?

Y: Eh, daar bedoel ik mee de [the professional services firm] omgeving. Dus inzicht krijgen in de [the professional services firm] portal tot de [the professional services firm] documentatie die wij vastleggen op bijvoorbeeld [an internal page], daar zit gevoelige eh, informatie in en daar kan je alleen maar toegang toe krijgen als je eerst met je VPN verbonden bent.

X: Zijn er andere redenen waarom jij een VPN gebruikt?

Y: Eh, nou ja, ik gaf al aan, beveiliging van documentatie, privacy. Verder, ja, ja, wat een vraag, ja, ik denk dat is het.

X: Welke handelingen voer jij uit als een gebruiker om een verbinding te maken? Want je zegt al net dat je de [access token provider] code invult-

Y: Hmhm. Ja, dat klopt. Dus welke handelingen ik moet verrichten, of-

X: Ja.

Y: Is je vraag. Oké. Ja, allereerst als je bij [the professional services firm] komt werken heb je die app nodig, zonder die app krijg je ook geen toegang. Dus je hebt ook sowieso een [the professional services firm] mobiel nodig. Of in ieder geval je moet [the professional services firm] medewerker zijn. Dus ik heb een, naast dat het een app kan zijn kan het ook een token zijn, en daar eh, dan krijg je daar die code op. Je moet eerst zelf een persoonlijke code instellen, weet ik nog. Eh, aan het begin van mijn dienstverband. Die wijzig overigens geloof ik niet, die hoeft je niet periodiek te wijzigen en dan eh, ja, om echt toegang te krijgen moet je eerst je eigen persoonlijke code dus instellen, zodra je die hebt ingesteld kun je verbinding maken met de, je eigen code dus samen met dan de [access token provider] code, die je ja, standaard krijgt vanuit ofwel die app ofwel de token, de fysieke token.

X: En op welke apparaten gebruik jij een VPN?

Y: Alleen op mijn laptop.

X: En maak jij ook verbinding met het interne netwerk van [the professional services firm] op jouw mobiel?

Y: Eh, nou, ik heb het wel eens gedaan, maar ik heb eigenlijk, bijvoorbeeld ik heb mail en al dat soort dingen heb ik eigenlijk niet meer op mijn werktelefoon staan, dus nee. Ik heb dat dus ook niet echt meer nodig, omdat ik die apps er ook niet op heb, op heb staan.

X: Gebruikte je daarvoor dan destijds een VPN-verbinding voor?

Y: Phoe. Goede vraag. Ik geloof voor sommige apps wel, maar niet voor allemaal. Ik weet even niet meer helemaal uit mijn hoofd voor welke wel, welke niet eh, to be honest. Het is al een hele lange tijd geleden dat ik die op mijn mobiel had, had staan.

X: Oké. En je zei al dat je niet heel veel van VPN van de technische kant weet, maar zou je mij kunnen vertellen hoe een VPN-verbinding werkt? Hiervoor kan je het whiteboard gebruiken als je dat fijn vindt.

Y: Ja, ja, eens even kijken. Nou, laten we eens even kijken. [start drawing 6_1]. Eh, als dit, kan je ook, dit kan niet he, nee, o, ja, kan wel. Als dit je- Moet ik gewoon zo, ja. Ik dacht misschien kan je ook schrijven, maar dat kan niet.

X: Je kan typen.

Y: Toch wel?

X: Door een vierkant ook te tekenen, dan kan je daarin eh-

Y: Misschien eh, nee. O, eens even kijken. Hmhm. O, zo ja. Als dit je laptop is, dan- Ik weet niet of ik het zo goed omschrijf hoor, misschien doe ik het ook wel helemaal fout. Maar je gaf al aan er zijn niet echt foute antwoorden.

X: Maakt niet uit.

Y: Wat zei je?

X: Maakt niet uit of het goed of fout is, het gaat erom hoe jij denkt dat een VPN-verbinding werkt.

Y: O ja, dit moet de cloud voorstellen, maar oké. Cloud eh-

X: O.

Y: Sorry. Andere kleurtjes. Zo, hmhm. Dan is dit eigenlijk je, ja, maar misschien dat ik het verkeerd omschrijf hoor. Eh, het is nu wel iets te klein, kan ik het groter maken. Hij heeft eigenlijk iets meer als een firewall, maar oké. Eh, hmhm. Nee. Ik weet niet een beetje hoe ik het zou uittekenen, dus dat je hier je toegang moet maken met je eh, VPN. [\[start drawing 6_2\]](#). Als je geen signaal terugkrijgt, dan kun je ook niet toegang krijgen. En zodra je pas een signaal krijgt, krijgt je pas toegang tot het netwerk. Hoe ik het zou uittekenen.

X: Wat bedoel je met een signaal terugkrijgen?

Y: Eh, nou, een signaal terugkrijgen bedoel ik mee dat je altijd een code nodig hebt. Zonder dat je een code hebt, kun je ook niet toegang krijgen. Als je je code foutief invoert, dus stel ik heb code, een persoonlijke code, dus ik zeg iets, 00887766, en je vult daar een andere code in, dan krijg je een foutmelding. Dus dan krijg je geen toegang.

X: Daarmee bedoel je dan je pincode? Je persoonlijke code dus zeg maar, die niet verandert.

Y: Ja, klopt.

X: Oké, duidelijk. En kan je meer vertellen over de gele lijn?

Y: Deze? De oranje?

X: Ja.

Y: Oké, eh. Wat kan ik vertellen. Ja, dat zal een soort van, een, ja, ik weet niet helemaal hoe ik het moet omschrijven. Vind ik wel moeilijk. Een soort van een, ja, ik weet niet helemaal of je het kan noemen zo, maar een firewall is in principe ook een soort van een tunnel of het is een bepaalde zone waar je in principe doorheen moet. Eh, ja, voordat je er doorheen komt. Eh, ik weet niet helemaal of het een zone, ja, een soort van versleutelde zone waar je eerst doorheen moet, zonder dat je er daadwerkelijk echt doorheen kan komen. Ik weet niet of dat het toelicht, deze lijn, een versleutelde zone.

X: Wat bedoel je dan met versleuteld?

Y: Ja, dat je er slechts doorheen kan als je de juiste toegang krijgt.

X: En je omschrijft het ook als een tunnel, wat bedoel je daarmee?

Y: Ja, een tunnel omgeving. Er zal iets zitten in je laptop waarmee die bepaalt of je er wel of niet doorheen komt. Dus er zal wel een iets van een tunnel of een soort van kluis, die pas open gaan als je dus de juiste codes invoert.

X: Oké, dankjewel.

Y: Zodoende een tunnel.

X: Eh, dan een andere vraag. Wat is de invloed van een VPN-verbinding op jouw computerbeveiliging?

Y: De invloed van VPN op mijn computerbeveiliging, is dat je vraag?

X: Ja.

Y: Eh, nou ja, dat je dus niet zomaar bij gegevens kan van eh, van, van klanten die eigenlijk in principe op de [the professional services firm] eh, netwerk staan, of [the professional services firm] gegevens staan. Dus vanuit die zin heeft VPN een positieve invloed, omdat je eigenlijk alleen maar erbij kan als je VPN, met VPN verbonden bent.

X: Oké. En zijn er nog meer invloeden van VPN op jouw computerbeveiliging?

Y: Eh, nou het enige wat mij wel opviel is dat ... dat we eerder gebruikte we, of gebruikte ik eigenlijk altijd eh, Firefox, zeg ik dat goed. Nee, Explorer, Explorer gebruikte ik altijd. En nu gebruiken we ook, sinds kort gebruik ik Edge of Chrome en ik geloof in ieder geval voor Edge in het begin had je soms niet een VPN-verbinding nodig tot eh, tot bepaalde [the professional services firm] tools te komen, dus dat vond ik wel interessant hoe dat dan werkt.

X: En was dat nog locatieafhankelijk?

Y: Eh, nee, ik geloof dat maakte in principe toen niet per se uit. Als je op [the professional services firm] netwerk zit, dan ben je er sowieso al in, dus dan heb je ook niet meer de VPN eh, code nodig. Dan zit je op het [the professional services firm] netwerk, dus dan herkent die blijkbaar al dat je geautoriseerd bent. Maar vooral namelijk vanuit andere locaties dan een [the professional services firm] kantoor kon je gewoon al standaard er al inkomen, in ja, [an internal page] heet dat in ieder geval, dat is de omgeving die ik hiermee, waar ik zelf gebruik van maak. Dus dat vind ik wel interessant, eerder had je altijd een code nodig, anders kom je [an internal page] niet eh, in principe niet in.

X: Een verbinding nodig hebt om eh, binnen [an internal page] te komen.

Y: Ja, en in [an internal page] leggen wij eigenlijk alle, ja, dat is ons dossier om onze ja, werkzaamheden in vast te leggen, dus daar liggen best wel veel gevoelige, gevoelige informatie in.

X: Dan een andere vraag. Met wat voor digitale dreiging heb jij op een normale dag te maken?

Y: Eh, voornamelijk phishing e-mails. En zelf heb ik ja, ik denk voornamelijk phishing e-mails, maar die krijg ik niet naar mijn werke-mail hoor. Meer naar mijn privé e-mail.

X: Kan je nog een andere digitale dreigingen bedenken?

Y: Nou eh, niet waar ik zelf mee te maken heb. [the professional services firm] breed zal er wel mee te maken hebben. Zoals eh, ik zeg maar iets, ransomware of eh, DDoS attacks, maar dat heb ik zelf niet een eh, reguliere dag basis. Ja, we hebben natuurlijk wel, ja, digitale dreigingen, ik weet niet of je het dan ook hebt over fysieke dreigingen, fysieke digitale dreigingen, maar dat is misschien anders.

X: Ja, bijvoorbeeld.

Y: Nou, bijvoorbeeld, ik heb, stel dat [0:15:02 until 0:15:04 has been omitted] en ik heb eh, mijn code, ik heb een token, die heb ik nog, maar die moet ik eigenlijk al heel lang inleveren, dus dat moet ik nog even doen. Maar stel dat iemand die pakt en ik laat mijn laptop open staan, dus ik lock mijn laptop niet. Ja, dan kan iemand zo maar even meekijken met mijn eh, gegevens op mijn laptop of eh, überhaupt meekijken op mijn scherm. Dus daarvoor heb je ook die privacy screen setting op je laptop, moet je eigenlijk wel altijd aan hebben [0:15:33 until 0:15:37 has been omitted] zou kunnen meekijken. Dus dat soort ja, misschien iets minder dus echt een digitale dreiging, maar wel een-

X: Meer een sociale dreiging is dat dan.

Y: Ja, misschien dat dat het is ja.

X: Kan je nog andere sociale dreigingen bedenken?

Y: Eh, ja, nou ja, maar dat is meer, stel dat ik probeer in te breken bij een ander bedrijf, stel dat ik in het pand probeer te komen met een eh, pasje van iemand anders en dat ik zo ook toegang krijg tot bepaalde informatie, maar ik denk dat dat iets te veel afwijkt van het onderwerp, maar dat kan ik me nog bedenken. Eh, ik bedenk even niets, misschien wel dat ik er zo op kom.

X: Dit zijn al voorbeelden. Eh, heeft de VPN-verbinding nog invloed op deze dreiging?

Y: Wat zei je, sorry?

X: Verandert de soort dreiging door een VPN-verbinding?

Y: Ligt eraan wat je dreiging is. Eh, VPN-verbinding kan best een goed mechanisme zijn, alleen als de mens het eh, een beetje laat slingeren, dan heb je er alsnog niks aan. Dus stel dat ik mijn code, mijn token overal laat slingeren, ja dan is het heel leuk dat je een VPN kan eh, verbinden, of in ieder geval met je code, maar als iedereen toegang heeft tot die code dan heb je er alsnog weinig aan. Eh, als je het echt hebt over die phishing mails die ik aan het begin zei, dan denk ik niet dat VPN daar invloed op heeft, maar dat is misschien mijn technische, niet onderbouwde, hoe noem je dat, niet onderbouwde technische kennis. Naar mijn eigen inschatting zou VPN daar geen invloed op moeten hebben.

X: En als je het dan hebt over phishing mails of eh-

Y: Hmhm.

X: [0:17:46 until 0:17:49 has been omitted], wie of wat is dan de aanvaller die de dreiging veroorzaakt?

Y: Eh, wij zelf. ...

X: Sorry?

Y: Moet ik nog iets toelichten? Ik weet niet hoor.

X: Sorry, wat zeg je?

Y: Moet ik nog iets toelichten? Of niet?

X: O, ja.

Y: O, ik hoorde de laatste vraag niet denk ik.

X: Oké, eh, als je het hebt over die verschillende soorten dreigingen-

Y: Ja.

X: Wie of wat is dan de aanvaller die de dreiging veroorzaakt?

Y: Ja, oké. Nee, ik dacht dat ik daarop antwoord gaf. Ja, wij zelf, vaak initieert een phishing mail, dat is iemand die, een soort van een outsider, die probeert in te breken in eh, in de omgeving natuurlijk. Maar dat wordt altijd geïnitieerd door een mens, dus een persoon. Dus daarmee zijn wij zelf eigenlijk de initiator van zo een dreiging.

X: Als je het dan hebt over die outsiders, wat voor outsiders zijn dat?

Y: Ligt eraan wat hun intenties zijn, dus het kan een outsider zijn, bijvoorbeeld een eh, ja, ik weet niet of- Ik kom niet helemaal op het woord, maar een soort van een rookie, een rookie, zo een woord. Dus het kan zijn een, gewoon een gast, een jonge gast die denkt nou ik ga haha, ik ga voor de lol even proberen in te breken, maar het kan ook zijn dat het echt gaat om een outsider die meer ja, politieke bepaalde dreigingen te veroorzaken. Eh, dus dan kijk je, dan is het een heel ander motief waarom iemand zo een dreiging zou initiëren. Eh, andere outsiders, ja, het kan hacktivists, maar het kan ook gaan om, dus die politieke redenen gaf ik aan, het kan ook zijn iemand die echt schade aan wil richten, dus iemand die eh, ja, wat is het woord nou daarvoor, [0:20:13 until 0:20:15 has been omitted], vijf van die typen outsiders. Maar ik weet even niet meer de naam van zo een, echt iemand die dus echt schade wil aanrichten, dus niet om politice, politieke redenen of eh, maar echt bewust bepaalde gegevens op straat wil geven. Maar ik komen even niet op de term van zo een outsider.

X: Ik ben niet op zoek naar specifieke termen per sé, maar meer gewoon omschrijvingen. Dus je noemt al verschillende motivaties die er zijn, kan je nog meer motivaties bedenken?

Y: Even kijken, ik zei dus politieke redenen, ik zei om gewoon grapje uit te halen, ik zei om ja, dus echt eh, schade aan te richten vanwege zeg maar iets eh, nou, hoe heet het nou, ik kom er gewoon even niet op, he. Eh, redenen. Nee, ik denk het niet, misschien dat ik er zo nog even op kom. Ik ben nog heel even aan het malen in mijn geheugen.

X: We kunnen naar een volgende vraag doorgaan.

Y: Ja, misschien na een volgende vraag. Misschien kom ik er zo wel op terug.

X: Ja, prima. Als je bedenkt wat voor achtergrond een aanvaller heeft, wat zou dat kunnen zijn?

Y: Eh, denk ik ook, licht er wel aan, die mensen zijn best wel, ze zullen vast wel een technische, technische achtergrond hebben, anders weten ze echt niet hoe ze zo daarbinnen kunnen komen. Dus de achtergrond zal vaak zijn, of het is iemand die- Ik weet niet helemaal wat je bedoelt met achtergrond, in de zin van opleidingsachtergrond of in de zin van waarom zou iemand een dreiging willen veroorzaken.

X: Ja, opleidingsachtergrond, dan wel formeel of informeel.

Y: Oké. Ja, ja, ik denk dus inderdaad eh, qua opleidingsachtergrond zal het echt wel een technische studie zijn, dus ik denk iets van business informatics ofzo, of iets van computer science, waarvoor je eh, ja, echt wel de skills nodig hebt eh, om zo een dreiging te kunnen veroorzaken. Ik denk niet dat je dat zo maar kan als je nou, zoals ik [me] heb gestudeerd. Maar dat is mijn eigen inschatting. Maar het hoeft niet altijd te zijn door middel van een opleiding, maar ook gewoon mensen die gewoon slim zijn eh, met computers aan sich, dus die hebben dat op de een of andere manier aangeleerd of die hebben er gewoon affiniteit mee.

X: Als je nadenkt-

Y: Zal wel een soort van bètastudie zijn.

X: Sorry, wat zei je?

Y: Ik denk vooral mensen met een bèta achtergrond, bèta, bèta.

X: En eh, wat zou de impact van een aanval kunnen zijn voor [the professional services firm]?

Y: Voor [the professional services firm] denk ik relatief, licht eraan waar ze toegang tot krijgen. Eh, maar als ik het weer heb over bijvoorbeeld stel dat een hacker toegang krijgt tot eh, tot [an internal page], dus tot die omgeving, dan kan dat best wel veel eh, schade verrichten, want daar zit gewoon allemaal klantgevoelige informatie in, in ons dossier. [0:23:44 until 0:24:20 has been omitted]. Dus dan heeft het zowel impact ons onze reputatieschade [0:24:24 until 0:24:26 has been omitted]. Dus dat heeft echt wel

een hele grote impact. Maar als ze alleen toegang krijgen tot bijvoorbeeld het, ik zeg maar iets, intranet ofzo en daar staat alleen op dat eh, ik zeg maar iets hoor, dat [role] verspreidt hoe wij omgaan met coronavirus, ja, dan denk ik nou dat is misschien iets minder spannend als dat op straat komt, maar ligt er dus ook aan waar ze toegang tot krijgen.

X: Deze verschillende soorten impact, zou daar nog verschil in zijn?

Y: Ja, ja, dus ik denk wel inderdaad echt toegang tot ons [an internal page] dossier zou een heel grote impact hebben, maar toegang tot een intranetwebsite zou misschien minder impact hebben.

X: Oké. Dan gaan we terug naar de VPN-verbinding zelf-

Y: Ja.

X: Hoe veilig is een VPN-verbinding?

Y: Ja, nou, dat eh, ik zag dat al dat dat een van je vragen was, maar dat vond ik al een lastige vraag, want ik geloof dat je best wel makkelijk kan inbreken in een VPN, maar zoals ik zei, ik ben niet heel technisch onderlegd, dus ik weet het niet helemaal. Dus dat weet ik eigenlijk niet. Wat zei je?

X: Zei je dat je wel of niet kan inbreken in een VPN?

Y: Nee, nee, ik zou het niet weten. Ik weet niet of je daarop kan inbreken, ik denk dat je, dat het wel moet kunnen ofzo, maar ik zou niet weten hoe.

X: Oké. Ik zou ook niet weten hoe hoor, als je dat-

Y: Haha, ik denk dat het vast allemaal kan allemaal, vast, maar-

X: En houd jij nog op een bepaalde manier rekening met mogelijke onveiligheden van VPN? Zijn er bepaalde handelingen die jij uitvoert?

Y: Nee, nee, eerlijk gezegd niet. Ja, goed, ik houd me token houd ik altijd in mijn etui, zeg maar iets, ik laat hem niet- Mijn etui heb ik eigenlijk altijd eh, dicht zitten, want ik haal er alleen maar een pen uit en dan doe ik hem weer dicht, dus daar let ik wel op, maar voor de rest ben ik er niet heel bewust mee bezig, to be honest. Het is meer een handeling geworden, een automatische handeling als je je laptop opstart, want je vult gewoon zo een code in, maar ik heb daar niet echt specifieke beveiligingsmethodes voor ofzo.

X: Jij, eh, iedere keer als jij je laptop opstart, maak je direct verbinding met de VPN?

Y: Ja, ja, als ik thuis werk wel ja.

X: En ga je dan alleen naar het [the professional services firm] netwerk?

Y: Eh, ja, ja. [0:27:22 until 0:27:22 has been omitted].

X: Oké. Zijn er nog dingen van VPN die jij wel weet die niet ter sprake zijn gekomen, waar ik niet naar gevraagd heb?

Y: Eh, even nadenken hoor. Nee, denk het niet.

X: Dan waren dit tot zo ver mijn vragen, heb jij zelf nog vragen?

Y: Ja, ik vraag me af waar dit dan uiteindelijk op uitkomt, laat maar zeggen, want jij, op het einde ging het er natuurlijk wel even over, van denk je dat VPN ja, moet ik heel even nadenken hoe ik het duidelijk weer- Dus helpt, is VPN, kan dat, is dat secure genoeg om die dreigingen laat maar zeggen te eh, nou ja, tegen te houden of te voorkomen, ja, ik vraag me af wat daar dan uitkomt laat maar zeggen, waar jouw, wat jouw resultaat is van jouw onderzoek, maar dat weet jij nu ook nog niet, want je bent nu nog volop bezig met interviews natuurlijk.

X: Ik zal even de opname stopzetten.

Y: Ja.

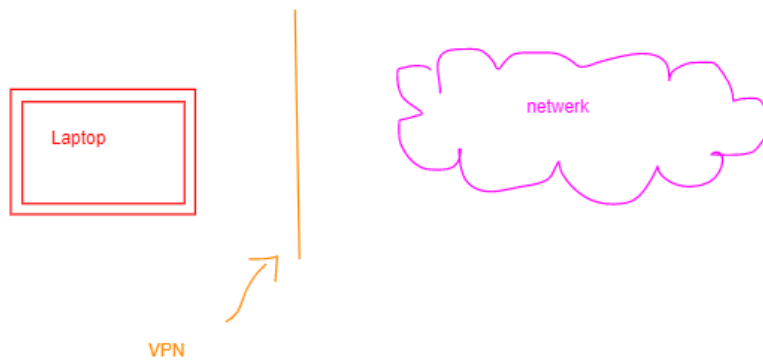


Figure C.6.1: Drawing 6_1

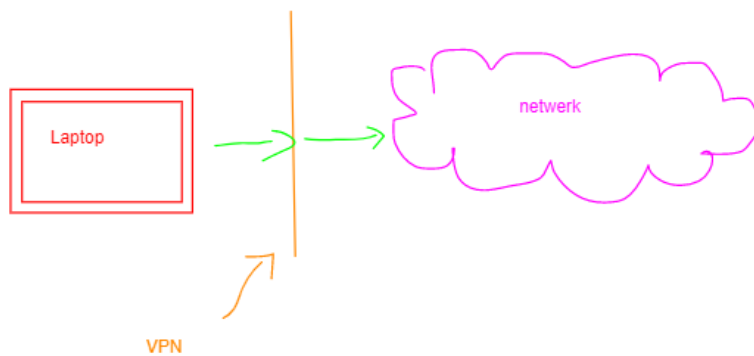


Figure C.6.2: Drawing 6_2

C.7: Transcript Expert 7

Duration: 48 minutes

Language: Dutch

Number of drawings: 6

X: Dan de eerste vraag voor het interview. Kun je mij uitleggen wat een VPN is?

Y: Eh, ja. Hangt ervan af hoe technisch je het wilt. Eigenlijk de meest eenvoudige vertaling daarvan is een eh, ja, eigenlijk een privé lijn wat je hebt richting een bepaalde locatie, richting een server, voordat je verbinding hebt met eh, bijvoorbeeld het Internet, maar dat kan ook een VPN zijn, een lijn zijn naar een bepaalde server voor je verbinding hebt met een andere server. Dus eigenlijk he, om een privé lijntje die eh, op een manier beveiligd is.

X: Wat bedoel je met een privé lijn?

Y: Dat gaat dus al echt om een virtuele verbinding, dus eh, een eh, connectie he, tussen jouw eigen device en een eh, en een server. Dat gaat dus wel over het Internet, maar he, je bent niet direct initieel verbonden met het Internet. In de vorm van je zit niet op het publieke netwerk, je zit in een afgescheiden kanaal.

X: Waar zit je dan niet in het publieke netwerk bedoel je?

Y: Sorry. Je maakt wel gebruik van eh, eh, van natuurlijk dezelfde techniek, maar je zit niet direct in het publieke netwerk. In het gedeelde netwerk. Dus je bent altijd met een beveiligde verbinding direct naar een eh, een doellocatie, naar een server.

X: Hoe is de verbinding beveiligd?

Y: Sorry?

X: Hoe is de verbinding beveiligd?

Y: Eh, met encryptie.

X: Oké. En wat is encryptie?

Y: Eh, encryptie is versleuteling van data. En dat gaat via specifieke, oeh, eh, ja, ik denk dat je het het best kan omschrijven als tunnels. Dus eigenlijk een soort van eh, van poortje. Eh, en dan om die eh, om die te kunnen lezen, wat erin staat, heb je een bepaalde sleutel nodig. En als je die sleutel niet hebt, dan kan je daar dus niet in.

X: Duidelijk. Eh, wat bedoel je met een tunnel?

Y: Een datatunnel zeg maar. Een poortje, kan het ook een deur noemen of eh, een transportkanaal, laten we het zo noemen.

X: Oké, en eerder noemde je dat de verbinding gaat naar een server. Hoe gaat deze verbinding naar een server?

Y: Kan op verschillende manieren, he. Een private line kan je ervoor hebben of je kan een VPN hebben wat gewoon valt over het eh, over het reguliere netwerk gaat. Dus je wordt altijd via een he, of via een Internetverbinding direct of een private line betekent eigenlijk een privéverbinding daarvoor richting een server.

X: En wat is een server?

Y: Een server is een device, ja, eigenlijk je, je, net als je je computer hebt, een client, is dat een device voor het regelen van, in dit geval, een eh, een dataverkeer. Dus de server kan zijn in eh, specifiek in dit geval een router vanuit de VPN, maar achterliggend zit daar een he, een basisplatform.

X: Dankjewel. Waarom gebruik jij een VPN?

Y: Waarvoor ik het gebruik vanuit mijn werk of waar ik het gebruik persoonlijk of algemeen waarvoor iemand een VPN gebruikt?

X: Ja, waarom jij de VPN gebruikt binnen [the professional services firm].

Y: Waarvoor ik hem binnen [the professional services firm] gebruik, oké. Binnen [the professional services firm] eh, gebruik ik hem om diverse eh, authenticaties met diverse eh, applicaties. En denk hiervoor aan eh, even kijken, [an internal page] is volgens mij nu niet meer, maar [an internal page] bijvoorbeeld, zit ook nog achter een VPN. Dus als ik in, bij [an internal page] wil komen, kan dat alleen maar via een specifiek eh, punt, dus moet ik eerst VPN naar zo een eh, locatie gaan, naar zo een server, en daarvandaan kan ik de omgeving, in dit geval eh, [an internal page] benaderen. Maar dat is ook voor-

X: En wat-

Y: Sorry, wat zei je?

X: Je kunt je zin afmaken.

Y: Ja, er zijn dus ook overige applicaties die draaien eh, ten minste die alleen toegankelijk zijn vanuit VPN-locatie binnen [the professional services firm].

X: En wat bedoel je met authenticatie met applicaties?

Y: Authenticatie eh, betekent he, dus het toegang krijgen tot, dus het hele proces omtrent het eh, identificeren en toegang krijgen tot een omgeving of applicatie.

X: Zijn er nog andere redenen waarom jij een VPN gebruikt?

Y: Binnen [the professional services firm] momenteel-

X: Ja.

Y: Hebben we het over, he, de scoping. Eh, ik zit even te kijken op welke applicaties dit nog van toepassing is. We hadden het over voorheen ook op [an internal page] natuurlijk, voor een stukje veiligheid, want het is vanuit authenticatie zit natuurlijk daarachter een stukje beveiliging. Nee, ik weet niet over welke je het nu precies eh, specifiek naar opzoek bent.

X: Welke handelingen voer jij uit om een VPN-verbinding te maken?

Y: Wat ik uitvoer persoonlijk is eh, ik moet zowel eerst in mijn eh, in mijn laptop moet geconfigureerd zijn het adres van de VPN-server, als die geconfigureerd is en dat staat over het algemeen al gedaan vanuit IT staat dat in je device. Dan moet je inloggen met jouw gebruikersnaam met een eh, een authenticatiecode en die authenticatiecode is onderdeel, een code die eh, die je zelf bepaalt, een vaste pin en het tweede deel van die code wordt gegenereerd via een soft token. Dat betekent dus he, een token die op jouw mobiel device wordt gegenereerd.

X: En die soft token, zijn er nog andere mogelijkheden naast een soft token?

Y: Voor zo ver ik weet is er een eh, kan een tijdelijke soft token worden gegenereerd vanuit helpdesk, eh, voorheen hadden we hardtokens, die zijn als het goed is geheel uit gefaseerd, maar dat zal vast nog wel he, [the professional services firm] kennende zullen die ook nog wel in de omloop zijn.

X: En waarom zijn die uit gefaseerd, weet je dat?

Y: Een keychain is natuurlijk minder veilig dan een, een token op je eh, mobiel device waar nog eens een wachtwoord op zit. Eh, maar je houdt ook het hele stukje beheer daarvan- Het is makkelijker om eh, keygenerators te beheren dan de fysieke eh, tokens die mensen bij zich dragen. Het is ook makkelijker om een token te verliezen wat dat betreft, dan een mobiele telefoon. En als die token is verloren, dan heeft iemand gelijk toegang tot die code en op je mobiele telefoon zit dan altijd nog en een wachtwoord plus je device kan ook vanaf afstand worden gecleared, dus leeggehaald. Dus als je aangeeft dat jouw telefoon gestolen is bijvoorbeeld, dan eh, zal daar niet eh, niet zo snel misbruik van gemaakt kunnen worden.

X: En op welke apparaten gebruik jij een VPN?

Y: Ik gebruik het persoonlijk alleen nu op mijn laptop, maar ik kan dat natuurlijk ook gewoon op mijn telefoon gebruiken of elk ander willekeurig device, als ik daarvoor eh, richting [the professional services firm] apps zal benaderen. Momenteel eh, is dat niet ingeregeld.

X: Je kan eh, meerdere apparaten gebruiken om verbinding te maken met [the VPN of the professional services firm]?

Y: Volgens mij kan dat ook vanuit eh, de omgeving, ik weet even niet zo goed hoe die omgeving nu heet, dat is een paar keer van naam veranderd, maar we hebben [example of mobile application] hadden wij op de telefoon. Eh, maak ik nu even geen gebruik meer van. Waar wij uiteindelijk dus ook via een VPN-verbinding eh, bent verbonden.

X: En kan jij aan mij uitleggen hoe een VPN werkt? Het meer technische waar je het over had. Je kunt als je wilt het whiteboard daarvoor gebruiken.

Y: Ja, oké, dat is even basisconcept, he. Even kijken. [start drawing 7_1]. Basisconcept is ik heb een device, ik heb een mediating server en, nou laten we het noemen, heb ik een, o, gaat niet, wat doe ik verkeerd, eh, een device, een server en tekenen, je hebt het Internet, laten we het zo even noemen. Nou, dit is mijn eh, mijn client, tekst had ik hier ook ergens. Mijn client, dit is- Server noemen. En dan voor eh, even kijken hoor, hoe ga ik terug. Dus het idee is, o, wacht, hier nog even Internet bij, dit het eh, het Internet, publiek noemen of algemeen Internet, is wel goed denk ik voor dit doel. [start drawing 7_2]. Het idee is dat je voordat je echt hierzo, voordat je, o, hoe verwijder ik.

X: Je kunt op undo, het pijltje, klikken.

Y: [start drawing 7_3]. Dit is het basisidee, dat ik hier, als ik vanuit mijn client verbinding wil maken hier ergens met een device X, ga ik eerst naar de server, hiervandaan wordt die, ga ik door vanuit die server naar het publieke deel van het Internet of naar het, een, eh, wordt verkeer gemanaged. Het kan ook zijn dat een eh, een doel waar ik heen ga op dezelfde server staat, in dezelfde omgeving als de VPN-omgeving. [start drawing 7_4]. Dus ik heb hierzo mijn client, die staat ergens willekeurig. En deze server staat binnen het netwerk van eh, van [the professional services firm]. [start drawing 7_5]. Nou, om een voorbeeld te noemen van [an internal page], die staat volgens mij hier ergens he, dus dan heb je hier eh, een [the professional services firm] app, laten we het zo even noemen. Die staat dan binnen de omgeving van [the professional services firm], waardoor ik dus niet door hoeft weer terug het Internet op. Initieel is dit dus, deze lijn, dit is die private line waar ik het over had. Wat dus eigenlijk een soort van encrypted tunnel is eh, richting de ontvangende server.

X: En waar begint en eindigt de encryptie?

Y: Dit deel, dus van je client tot aan de server is encryptie. Tot aan je VPN-

X: Daarna niet meer.

Y: Daarna he, in principe op het moment als je daarna eh, hangt ervan af waar je naartoe gaat in je [the professional services firm] netwerk. Je zou in principe ook encryptie verder nog kunnen hanteren eh, maar in principe als je hiervan uitgaat, na je VPN nog even terug, naar je publieke Internet op, dus naar een willekeurige website, dan heb je natuurlijk niet meer een encryptie daarop zitten. Want een encryptie werkt tussen twee partijen die allebei de sleutel hebben. Dus als je hier naar een willekeurige omgeving gaat op

het Internet, die heeft he, die heeft niet een sleutel, die heeft he, die kan nooit, kan geen gebruik maken van die encryptie.

X: Maakt het voor deze tekening nog uit eh, wat je fysieke locatie is?

Y: Nee, die client dat is dus overal. He, fysieke locatie van je client is niet gebonden. Dus ik kan eh, net, ik zit nu ergens op een access point, als ik nu aan de andere kant van de wereld ga zitten is het natuurlijk precies dezelfde situatie.

X: Duidelijk. Dan een andere vraag. Wat is de invloed van een VPN-verbinding op jouw computerbeveiliging?

Y: Eh, ja, is een goede natuurlijk. Want aan ene kant, al het verkeer wat via die verbinding gaat he, wordt natuurlijk getunneld, dus dan zou je zeggen dat voor dat verkeer veiliger is, ten minste beveiligd is laten we het zo nu even noemen. Het werkt ook twee kanten op, dat betekent wel dat verkeer dat je binnen krijgt via de tunnel vanuit de andere kant eh, dat dat potentieel een eh, zwakte punt is, want het gaat door je beveiliging heen van je systeem. Een voorbeeld stel he, die server hier die gaat zo meteen eh, allemaal malicious berichten versturen, die VPN-verbinding die gaat beide kanten op, dus van mij naar die server, maar ook andersom. Dus dat is potentieel een poort die vatbaar is voor beveiligingsincidenten.

X: Ik snap niet helemaal wat je bedoelt. Eh, wie zou dan, waarvandaan zou dat verstuurd worden?

Y: Sorry?

X: Waarvandaan zou ja, malicious eh-

Y: Nee, kijk, wat ik bedoel is, je krijgt hier een open poort die dan ontstaat, he, dus tussen je client en je server. Dat betekent dat voor al het verkeer dat vanuit die server he, dat zal een, dat gaat dus buiten je beveiliging laag om die je hierzo aan je clientside hebt voor overig verkeer. Dus hier bestaat zeg maar een trusted connection tussen.

X: Heeft een VPN-verbinding verder nog invloed op jouw computerbeveiliging?

Y: Eh, nou vast wel, maar ik zal het nu even niet weten eerlijk gezegd. Weet niet welke kant je daarmee bedoelt.

X: Of er nog meer invloed is. Dan een hele brede vraag. Met wat voor digitale dreiging heb jij op een normale dag te maken?

Y: Digitale dreiging vanuit scoping nu ik ben aan het werk op mijn [the professional services firm] laptop. En dan de dreiging voor [the professional services firm], die bedoel je denk ik, of niet.

X: Ja.

Y: Oké. Nou, de grootste dreiging die ik heb dat eh, direct zie ik als alles wat door klanten wordt aangeleverd, of alles wat door collega's wordt aangeleverd via onofficiële kanalen. Altijd een, een, eh, grootste dreiging zit bij mensen op dit gebied. Dus de, je kan nog zo mooi je systemen hebben ingericht he, dat, dat je allemaal beveiligingslagen hebt ingebouwd, maar als vervolgens de eh, ik noem maar even wat, een collega die eh, die krijgt een mail, een mail door en in die mail staat salarisinkomsten of bonussen van [role] en die klikt erop en die stuurt dat vervolgens ook door naar jou, ja, of eh, vanuit de klant krijg je bestanden door die eh, laten we zeggen niet eh, niet heel schoon zijn en die gaan via onze, buiten de formele kanalen waar bestanden gescand worden, worden die met ons gedeeld.

X: Wat bedoel je met ze gaan buiten de formele kanalen?

Y: Sorry?

X: Wat bedoel je daarmee, dat ze buiten de formele kanalen gaan die gescand worden?

Y: Nou je he, natuurlijk hebben wij vanuit [the professional services firm], vanuit het netwerkverkeer wordt he, wordt gescand, maar ook vanuit mail en vanuit een eh, [an internal page], zit ook bepaalde scanning op. Maar als iemand ik noem maar wat via WeTransfer wat binnen haalt of op een andere manier eh, waarbij die maatregelen dus niet meer van toepassing zijn, dan is dat een eh, eh, een gemis in je, in je defensie.

X: Duidelijk. En als je nadenkt over verschillende soorten digitale dreiging, verandert de soort dreiging dan door een VPN-verbinding?

Y: Je bedoelt in een situatie waarin je alleen maar op VPN werkt? Of?

X: Ja, als je via VPN werkt, heeft dat invloed op de digitale dreiging, op een digitale dreiging?

Y: Ja, oké, stel he, we zouden alles alleen maar via VPN werken he, dus ik ben nu met VPN he, stel ik zal altijd via VPN verbonden zijn en al het verkeer gaat over VPN, dan krijg je dus dat in dit gebied hierzo, deze kant, dat het makkelijker te monitoren wordt. Dus je krijgt minder kanalen waarin data eh, richting het

publieke netwerk gaat. Dus je krijgt he, wel dat dit, deze kant hier rechts belangrijker wordt, dus je gaat je kanalen beperken, dus dan wordt het wel he, krijg je een bottleneck daarop zitten. Maar het is wel beter te beheersen. Aan de andere kant, het heeft dermate veel performance dat dat vraagt, dat ik niet zie een situatie waarin [the professional services firm] op kort termijn alles via VPN te laten verlopen. Juist zijn er nu bewegingen gemaakt om zaken zoals [an internal page] niet via VPN te hebben.

X: Wat bedoel je met kanalen beperken?

Y: Eh, met je lijntjes. Dus een lijntje kan zijn als ik hier mijn data altijd via deze server laat verlopen, dan weet ik dat alles eh, he, eh, hierzo ook binnen gaat komen. Als ik eh- [start drawing 7_6]. Dus of ik nou hier naar dit punt ga, hierzo ga, hierheen ga, of daarheen ga, he, dat gaat altijd via deze server in plaats van eh, dat ik vanuit de client direct daarheen kan benaderen. In plaats van dat je al die lijntjes zo he, dus al die dreigingen zou moeten afvangen, heb je dat nu vanuit een centraal punt.

X: Eh, en dan was dit omtrent digitale dreigingen, maar heb jij op een normale dag ook te maken met sociale dreigingen binnen [the professional services firm]?

Y: Bedoel je dan wederom heeft dat nog een relatie tot eh, VPN, of bedoel je algemeen sociale dreigingen in de vorm van social engineering op kantoren en dergelijke?

X: Ja, algemeen.

Y: Natuurlijk heb je op he, op kantoren heb je sociale dreigingen. En ik weet niet in hoeverre je op de hoogte daarvan bent, maar we hebben binnen [the professional services firm] [0:23:58 until 0:24:06 has been omitted]. En je kan ook zien dat mensen eh, toegang tot kantoor verkrijgen middels social engineering door gewoon met iemand mee te lopen. Dat is mogelijk. En dat is ook een van de, van de he, van de grote mensaspect waar ik net op doelde van awareness. Weet wat je aan het doen bent, dus als iemand achter je aanloopt, of je ziet iemand [0:24:26 until 0:24:27 has been omitted], spreek die erop aan. Maar hetzelfde, [0:24:30 until 0:24:31 has been omitted] en je gaat zelf niet fatsoenlijk om met je wachtwoorden of je eh, met je laptop open laten staan he, ongelogd of überhaupt je laptop onbeveiligd, niet aan een eh, niet op slot achterlaten.

X: Heeft een VPN-verbinding invloed op deze sociale dreigingen?

Y: Eh, ja in, ja en nee. Ja, als jij, hangt ervan af hoe je er mee omgaat. Als je, op het moment dat jij zo meteen nog steeds altijd alle ... doet opnieuw moet authenticeren bij die VPN-omgeving, dus iemand heeft toegang tot je laptop, maar vervolgens kan die nergens bij omdat die niet binnen die, die authenticatie laag heen gaan, dan kan dat bijdragen aan je beveiliging.

X: Oké, en je zei ja en nee. In welke zin bedoel je dan nee?

Y: Eh, dat eh, het grote deel, momenteel, het is als ik een VPN-verbinding op start, start ik nu een keer een VPN-verbinding op en ik blijf gewoon de rest van de dag blijft die draaien. Of een x aantal uur blijft die draaien, dan steun je nog steeds vooral op de toegang tot je laptop zelf. Het is dus niet dat ik elke keer opnieuw die verbinding moet initiëren.

X: Oké. Eh, en als je nadenkt over deze digitale en sociale dreigingen, wie of wat is dan de aanvaller die de dreiging veroorzaakt?

Y: Als [the professional services firm] zijnde eh, ja, dat kan he, dat kan divers zijn. Het kan zijn dat ze op zoek zijn naar specifieke financiële data, want we kunnen natuurlijk bij zeer gevoelige klant data. Het kan zijn dat het he, direct een target is op eh, voor [the professional services firm] als organisatie, dan is het doel de organisatie is diskrediet brengen. Het kan verschillende dingen zijn.

X: Kan je voorbeelden bedenken van aanvallers?

Y: Voorbeeld, nou ja, iemand die eh, bijvoorbeeld eh, [0:27:00 until 0:27:05 has been omitted] zal een motivatie kunnen zijn. Gezien dat wij natuurlijk heel veel [0:27:11 until 0:27:16 has been omitted]. Daar kan significant veel geld mee verdiend worden. Ik denk dat dat cruciaal is. Aan de andere kant hebben we ook heel veel persoonsgegevens, direct, indirect. Maar als specifiek [the professional services firm] wordt getarget, zal mijn inschatting zijn dat dat of gaat om een stukje eh, financieel gewin [0:27:37 until 0:27:39 has been omitted] of reputatieschade.

X: Dat is meer motivatie beschrijven eh-

Y: Sorry?

X: Dat is meer motivatie beschrijven, maar wie of wat is dan echt de aanvaller zelf?

Y: Eh, ja, een individu, een persoon. Ik zal verwachten he, dat dat niet intern is vanuit een [the professional services firm] bijvoorbeeld. Want wij hebben daarvan steun je natuurlijk een deel op het stukje integriteit van überhaupt mensen die bij [the professional services firm] werken en eh, stukje eh, [0:28:21 until 0:28:29 has been omitted]. Ik denk dat [the professional services firm] he, eerder een target is van een specifieke hacker wat dat betreft dan, social engineering he, kan ook een manier van hacking zijn. Maar niet zo zeer van hacktivisten.

X: Duidelijk. En eh, wat voor achtergrond heeft een aanvaller?

Y: Eh, ja, die zal zelf ook een [0:28:59 until 0:29:08 has been omitted] of eh, aan de kant van social engineering, als het eh, op een andere manier technisch vlak, dan zal het, zal het, ja, haast een whizzkid zijn. Dus of een hacker gewoon met heel veel he, ervaring of iemand die persoons gedreven erop uit gaat om [0:29:32 0:29:32 has been omitted] data te ontvreemden. Alleen heb je natuurlijk wel specifieke kennis nodig om het eh, om het verder nog toe te passen. Het is niet zoals een willekeurig persoon een [0:29:45 until 0:29:55 has been omitted].

X: Eh, heeft een VPN-verbinding nog invloed op de soort aanvaller?

Y: Eh, ja eh, nu specifiek voor [the professional services firm] in de situatie waar we dan alleen gebruik zouden maken van VPN bedoel je? Of in de huidige situatie?

X: Ja, als je gebruik maakt van de VPN altijd ten opzichte van de huidige situatie.

Y: Oké, dus de situatie waarbij we altijd gebruik maken van VPN. Eh, ja, dan heb je een eh, wellicht een hele andere ingangshoek inderdaad. Eh, specifiek eh, de techniek voor dat hacken daarvan zou ik niet weten. [0:30:44 until 0:30:54 has been omitted].

X: En je zegt wel eh, dat waarschijnlijk de soort aanvaller verandert, op wat voor manier verandert de aanvaller?

Y: Dat he, als je vanuit de techniek probeert dan aan te vallen, kijk eh, je krijgt dan wat grootschaliger ja, je krijgt een specifieke VPN-verbinding die, dus vanuit een centraal punt waar je een ingang moet vinden. En niet aan de kant van heel veel clients die allemaal potentieel een ingang hebben. Al die he, weer het verschil tussen een centrale situatie waar je je verkeer monitort ten opzichte van diverse eh, eh, gedecentraliseerde kanalen die je zou moeten monitoren en beveiligen uiteraard.

X: En wat zou de impact van een aanval kunnen zijn voor [the professional services firm]?

Y: Eh, grootste impact reputatieschade. He, dus impact dat klantgegevens worden ontvreemd, persoonsgegevens worden ontvreemd en je hebt natuurlijk [0:32:05 until 0:32:39 has been omitted], als [the professional services firm] lek jij die gegevens uit, dan krijg jij een behoorlijke dreun in je reputatie. [0:32:46 until 0:33:00 has been omitted]. Een situatie waarin dus klantdata of eigen data wordt ontvreemd, nou dan heeft het een gigantische impact.

X: Zou je nog meer voorbeelden van impact kunnen bedenken?

Y: Ja, het kan natuurlijk ook interne verstoring zijn van de processen binnen [the professional services firm]. Maar ik denk dat de grootste is vanuit [the professional services firm] zelf, is een stukje reputatieschade.

X: Duidelijk, oké. Dan over de VPN-verbinding zelf, hoe veilig is een VPN-verbinding?

Y: Eh, dat hangt uiteindelijk vanaf hoe die verbinding beveiligd is. In de vorm van he, de ene VPN-verbinding is niet even goed beveiligd als een andere VPN-verbinding. En hier moet ik heel eerlijk in zeggen, ik weet dat hier verschillende concepten van zijn, maar ik ken die niet in detail.

X: Oké, en kan jij kwetsbaarheden in de VPN-verbinding bedenken?

Y: Ja, een van de grootste is natuurlijk je, je encryptie.

X: Oké-

Y: Of de he, dus he, als je encryptie, we draaien nu eigenlijk volledig op steunt (0:34:34), als die eh, als je daar niet meer, als je niet meer kan steunen op een stuk vertrouwelijkheid van die data, ja, dan is eigenlijk het hele concept weg natuurlijk.

X: En als je nadenkt over deze onveiligheden, maar ook wat je eerder noemde, veranderen jouw handelingen hierdoor?

Y: Welke handelingen bedoel je nu? Of hoe je acteert richting het eh, richting externe bronnen of?

X: Jouw omgang met VPN.

Y: Mijn omgang met VPN, nee, ik gebruik VPN-verbinding binnen [the professional services firm] he, nu, in de huidige situatie alleen maar om naar eh, bepaalde applicaties toe te gaan. Verder zet ik hem uit. Dat ook vanwege een stukje eh, capaciteitsproblemen die we hebben binnen [the professional services firm]. Terwijl wij hebben he, ik kan wel continu via VPN werken, maar dat heeft ook impact op de eh, capaciteit van de VPN-server, aangezien we wereldwijd nu allemaal aan het thuiswerken zijn. Het is niet zo dat ik bewust meer via VPN zal gaan werken. Maar ik ben wel van mening dat als [the professional services firm] zijnde breed, moet je wel goed nadenken over welke verantwoordelijkheden je bij je eindgebruikers he, dus hierzo bij je clients allemaal neerlegt, want niet iedereen is even, heeft dezelfde awareness van risico's van buitenaf en kan daarin dus ook zelf de juiste eh, inschatting maken of ze wel of niet bijvoorbeeld zo een WeTransfer moeten gaan gebruiken.

X: En gebruik jij nog wel eens een VPN-verbinding op een andere locatie dan thuis?

Y: [0:36:33 until 0:36:36 has been omitted]. Eigenlijk alles wat niet op kantoor is. En op kantoor heb je eigenlijk ook een VPN-verbinding he, op de kantoren hebben ze een interne verbinding. Dus je maakt verbinding met het kantoor netwerk en daarvanuit zitten hun, zit je met een centraal VPN-netwerk zit je verbonden. ... Dus het is niet als je op een kantoorlocatie zit eh, dat er dan totaal geen gebruik is van VPN, alleen maak je er zelf dan geen eh, merk je er zelf op dat moment niets van.

X: Zou je nog andere situaties kunnen bedenken waarin je een VPN-verbinding gebruikt op een andere locatie?

Y: Eh, je bedoelt op het moment als je op een onveilige locatie zit extern. Dat zal-

X: Ja, bijvoorbeeld.

Y: Dat zal kunnen, maar als je op een onveilig netwerk zal zitten dan zou ik eerder mijn mobile device gebruiken voor eh, mijn mobiel kanaal. Niet zo zeer dan op een onbeveiligd netwerk.

X: Op je mobiel kanaal?

Y: Ja he, een hotspot op je mobiel, dus dat je via het mobiele netwerk gaat.

X: En dan gebruik je daarbij geen VPN-verbinding?

Y: Nou, hangt er vanaf he, wederom he, als ik op mijn mobiel gebruik als een hotspot en ik ga naar services waarvoor ik geen VPN-verbinding nodig heb, dus ik hoef niet van specifiek [the professional services firm] services gebruik te maken, waar, die afhankelijk zijn van VPN, dan zou ik daar niet een VPN-verbinding voor gebruiken, nee.

X: Waarom gebruik je een mobiele hotspot in plaats van een openbaar netwerk?

Y: Omdat ik van mijn mobile hotspot weet ik zeker dat het dan direct via de eh, Internetprovider verloopt en vanuit een openbaar, onbeveiligd hotspot heb je altijd het man in the middle risico. Stel dat al je data he, potentie voor je data om onderschept te worden, in ieder geval gemonitord te worden.

X: Heeft een VPN-verbinding hier impact op?

Y: VPN-verbinding zal dat risico zeker beperkter. Dus als jij op een onbeveiligd eh, eh, ten minste op een slecht beveiligde access point zit en je hebt een VPN-verbinding, dan pak je een directe tunnel he, met de server. Waardoor je dus weer, vanwege de encryptie, een beveiliging laag toevoegt.

X: Oké, duidelijk. Eh, dit waren tot zo ver mijn vragen. Heb jij dingen over VPN die nu niet naar voren kwamen?

Y: Eh, ja er zijn natuurlijk he- Nee, het gaat nu specifiek he, dat snap ik, je onderzoek gaat over VPN en in welke mate dat kan bijdragen aan je beveiliging. Dat is hoe je onderzoek is ingericht. Eh, dan heb ik hier niet specifiek nu nog toevoegingen over. Wel mijn vraag in hoeverre eh, vanuit oplossingen voor [the professional services firm], dus even buiten het onderzoek om, of het antwoord alleen maar vanuit VPN moeten zoeken.

X: Dan eh, over de [the VPN of the professional services firm] niet per se in eh, betrekking tot beveiliging, maar algemeen, is er dan nog iets dat niet ter sprake is gekomen?

Y: Nou ja, [the VPN of the professional services firm] an sich, kijk ik vertelde je dat wij een standaard key hebben die wij moeten invoeren, een persoonlijke key. Eh, nou die key die heb ik volgens mij eh, ten minste ik heb hem een keer toen ooit ingesteld, ik zou niet eens weten of ik die kan aanpassen. Dus he, als het gaat om de maat van beveiliging hoe die nu is, voor [the VPN of the professional services firm] zie ik wel wat aandachtspunten. Een daarvan is een VPN-connectie kan gestart worden volgens mij vanuit iedereen die

een eh, die over een username en uiteindelijk wachtwoord plus key beschikt. Maar dat betekent ook dat je meerdere sessies per persoon kunt hebben. Zit uiteindelijk dan wel gekoppeld aan je AD-gebruiker, dus het is wel mijn laptop die ik heb, waar ik ben ingelogd, die geeft, zorgt ook sowieso voor de authenticatie met de verschillende servers. In theorie zal dat dus betekenen dat als ik mijn eh, mijn mobiel niet heb en ik moet inloggen, dat ik op iemands anders inlognaam zou inloggen bij eh, op VPN, zijn code invul, of hij zijn code invult, zijn authenticatiecode invult en ik vervolgens wel verbonden ben met, met de VPN-server. Dus hoog over he, ja, als je op zoek bent naar nog verbeterpunten in de huidige VPN is dat misschien nog een aandachtspunt dat je VPN-connectie ook gekoppeld zit direct aan je AD-user. En eh, dat een standaarddeel van je wachtwoord he, wat er inzit, een deel van je code dat vaststaat, dat het wellicht wel handig is om dat ook met regelmaat te wijzigen. Dat niet statisch te laten voor onbeperkt.

X: Duidelijk. En eh, je noemde meerdere aanbevelingen, kan je nog meer aanbevelingen bedenken?

Y: Eh, ja sowieso he, je hebt he, dit is eigenlijk een soort van eh, je hebt ook VPN, ik weet deze techniek nog niet helemaal he, maar ik weet je hebt tegenwoordig ook een VPN by design, dus volgens mij een VPN-verbinding die eh, automatisch wordt geïnitieerd op het oment als dat je je laptop opstart. He, dus dat maakt dan gebruik uiteindelijk, dat steunt dan op de authenticatie die je hebt om op je eh, user in te loggen en vervolgens haalt die zelf automatisch al een VPN-verbinding op met de server waar verder geen handelingen meer nodig zijn.

X: Oké, zie jij dat als een voordeel of een nadeel?

Y: Eh, ik zal he, die techniek zal gezien kunnen worden als een voordeel. Dat zal he, gebruikt kunnen worden, maar dan zal ik wel zelf nog een eh, een notificatiesysteem bij hebben. Oftewel dat je een eh, bericht krijgt op je telefoon waarbij je nog op een knopje moet drukken van accept bijvoorbeeld. Maar nogmaals, ik ben niet helemaal thuis nog in die techniek.

X: Nee, dat is geen probleem. Oké, eh, ja, dus tot zo ver mijn vragen.

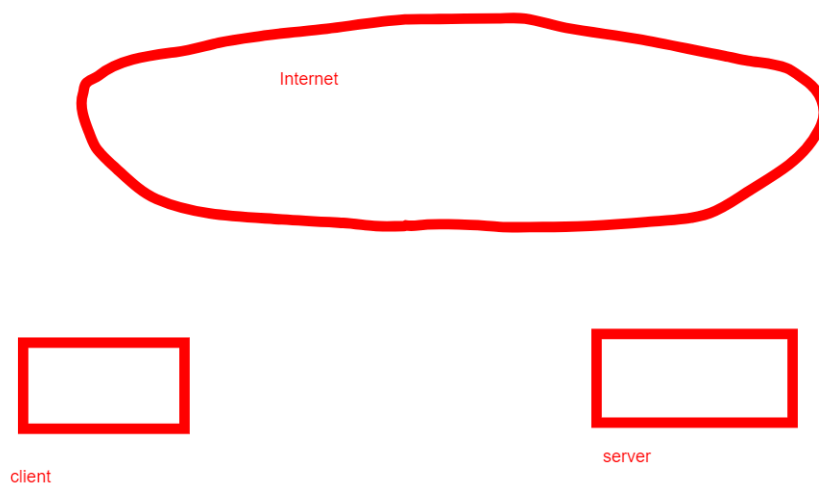


Figure C.7.1: Drawing 7_1

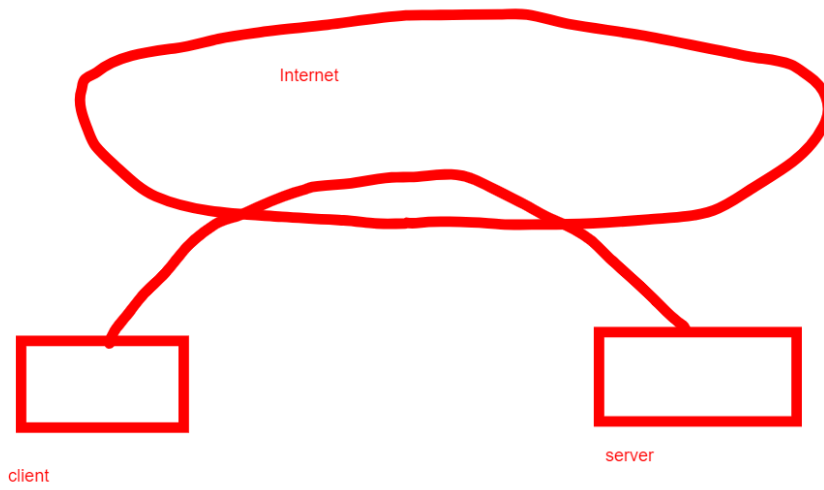


Figure C.7.2: Drawing 7_2

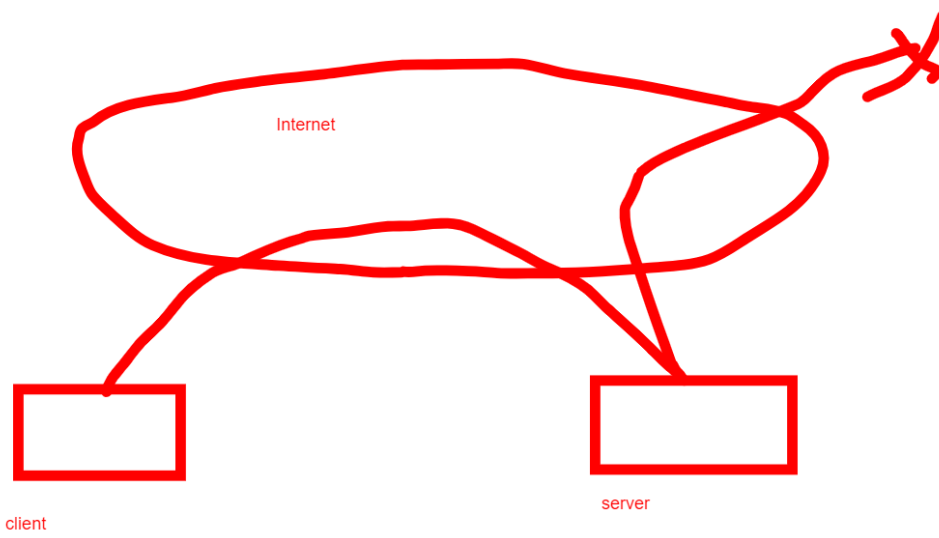


Figure C.7.3: Drawing 7_3

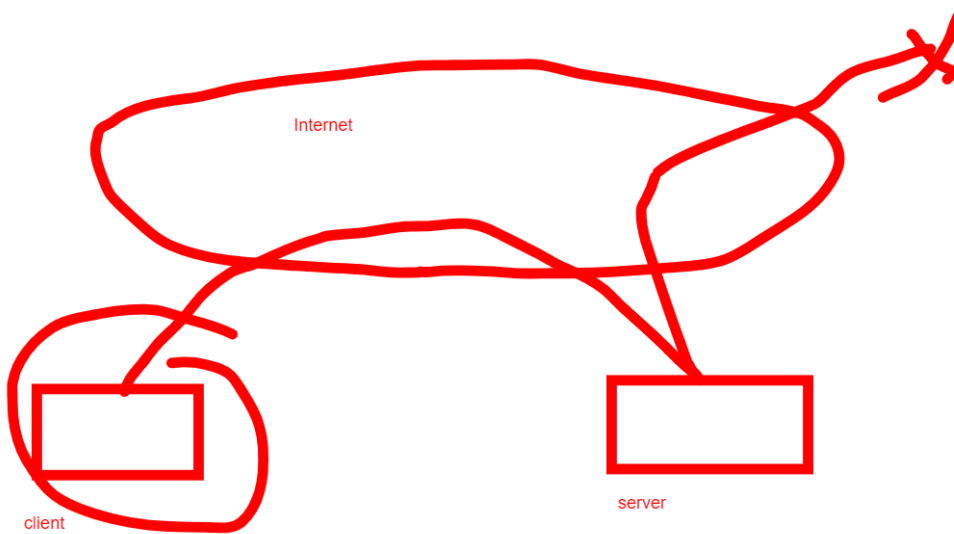


Figure C.7.4: Drawing 7_4

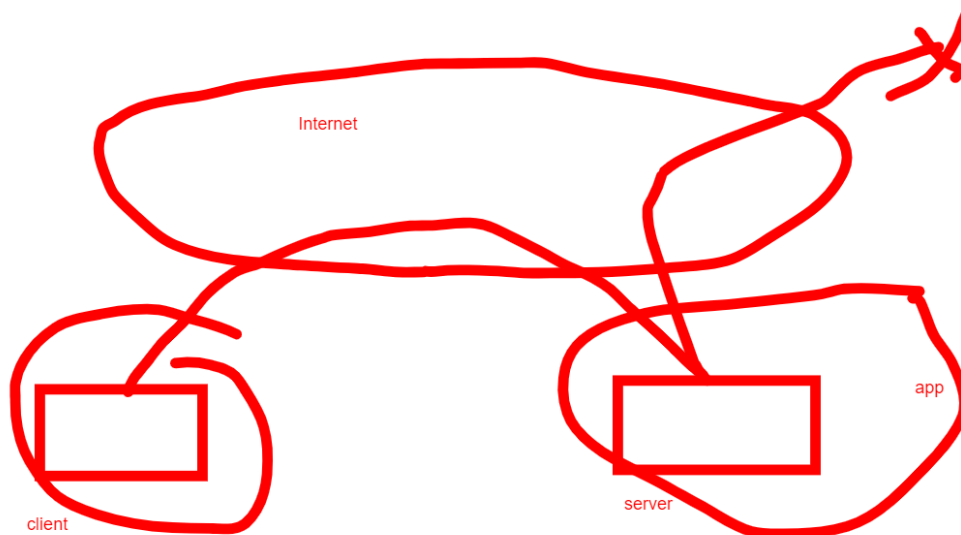


Figure C.7.5: Drawing 7_5

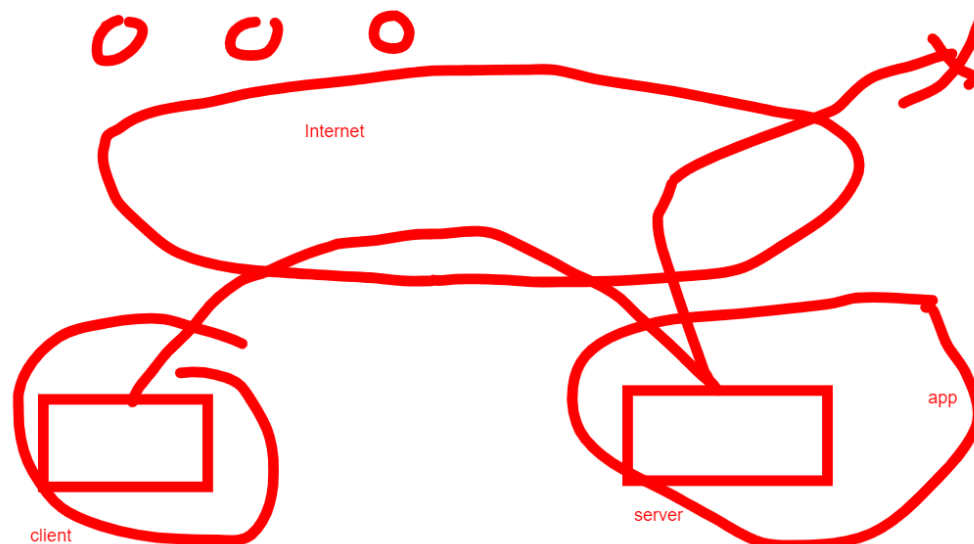


Figure C.7.6: Drawing 7_6

C.8: Transcript Expert 8

Duration: 38 minutes

Language: English

Number of drawings: 2

X: Could you explain to me what a VPN is?

Y: It is a virtual private network. Eh, it is basically eh, secure environment, where connection happens. Eh, you can protect your information, you can eh, bypass your region of your laptop of your IP address. It allows you to navigate protect in the eh, in the Internet. And it is usually companies require you to use when you have, when you work outside their secure environment.

X: Okay. You said a secure environment, what do you mean with this?

Y: Eh, secure environment is an environment in which you can be I would say protected from external eyes. For instance, man-in-the-middle attacks or people that are eh, like seeing your information. Sorry, it is a bit difficult in English. Eh, people like seeking information or spying on the transfer of packets, where they are

transferring from one terminal, one terminal to the others. Like for instance the [the professional services firm] intranet network, then you are supposed to turn on every time that you work at home.

X: Okay. And you say you can use it to protect your info, how can that be done?

Y: Sorry, what?

X: You said it, eh, it can be used to protect your info, how can that be done?

Y: Because eh, the VPN works, there is codes via tunneling, the process, so there is, it protects the information, the transmit of the package from your let's say, your starting point to the ending point. For instance, could be communication between servers or from a website it protects the or it confuse your region IP. For instance, I can visit a website now from The Netherlands, but with some VPN connection I can make eh, I can appear as for instance I am in Italy or eh, something. So, this is through the tunnel, the tunneling process.

X: What do you mean with tunneling?

Y: Eh, it's like eh, the way how is the VPN, the way the VPN works, so, it's like protected, like the package that you are sending from one terminal to another is protecting from eh, external attacks. Like they are- You don't have, you don't see the information so, when packages travels towards the Internet, you usually can see like IP or eh, some information. Eh, but if you are, if you are doing via VPN and you are external observer, you don't see this kind of information passing through from one point to the other.

X: And how is it that you can see that?

Y: If I can see what? The-

X: The IP address or the location.

Y: With the VPN or without?

X: With the VPN.

Y: Eh, no, sorry, I- Can you reformulate it? Like-

X: Yes, we can come back to it later otherwise. You said you can bypass your regions IP address-

Y: Yeah.

X: How can this be done?

Y: Eh, via protocol, like, you have specific protocols eh, and that can hide the IP address. Now, I wouldn't know specifically which one, but I know there are some VPN services that allows this.

X: Okay, thank you. And you said it helps you to connect from one terminal to another, what do you mean with that?

Y: That it is the way how they communicate. So, for instance from, it's like a private channel from one input to the other input when you transmit the information. It's creates this, this private eh, private tunneling that is invisible to other people. Like to other, for instance, an attacker is watching, it doesn't see the information, can't grasp the information in the middle.

X: And why do you use a VPN?

Y: To protect confidential information, for instance, yeah, when you work in a company and you need to communicate with outside or for instance, as now working, smart working from home, you need to have your secure environment when you deal with eh, confidential information. So, to protect.

X: How is it then protected?

Y: How is, sorry?

X: How is it then protected?

Y: Eh, because you have no, because you have just eh, a VPN, then it is protected.

X: Could you explain how it is protected?

Y: Eh, because you eh, eh, you protect your information by hiding the content to outside eyes.

X: Okay. And how are you hiding the content?

Y: Through the VPN system. Am I repeating myself, because the question are like the same or it is supposed to be like this?

X: Yes, a bit. But that is no problem. Eh, we can go on to the next questions. What actions do you- Or, are there any other purposes for which you use VPN?

Y: Eh, more, it is, it depends on what you need. If you mean like protect your information, that is basically the main purpose, or if you want to eh, yes, hide, like, navigate in, not incognito mode, like hiding eh, some

kind of eh, of eh, information as we were mentioning before the IP address. Basically, I would say it is generally for protection and safety of what you are transmitting.

X: And what actions do you take to create a VPN connection?

Y: Eh, set up server, asking somebody, I am sorry, I am not technical on that. Eh, but you have to, yeah, you have to require a service provider, you need eh, specific eh, I wouldn't say app, but device or it could be like a website, when you have connection for instance, [0:09:22 until 0:09:30 has been omitted].

X: Okay, and as a user, what actions do you take to create a VPN connection?

Y: Sorry, the voice skipped.

X: O, sorry. As a user, what actions do you take to create a VPN connection?

Y: Eh, as I user I need to start like username, password, eh, maybe also have a code for instance. Eh, there is like token that you need that change every single time that allow you more eh, protection in case your eh, like eh, double eh, multi-factor eh, multi-factor eh, authorization. And is eh, yeah, for instance, we have like the key or the token for [the professional services firm]. Eh, yeah, it serves, it is additional steps to protect eh, in case you have, you lost your laptop or they steal the token.

X: What kind of token do you use?

Y: I use, it's a small device with a self-generated number every single time. So, it is four or five eh, [0:10:54 until 0:11:00] is number, like random number plus a fixed password.

X: Okay. And do you know whether there are multiple tokens in [the professional services firm]?

Y: Eh, yeah, there is, I think there is also something combined with an app. Eh, but I am still not using that.

X: And on what devices do you use the VPN?

Y: Eh, device, it is [access token provider], I think token.

X: Yes, and on what devices do you use the VPN?

Y: On my laptop.

X: Do you use it on any other devices?

Y: Eh, no.

X: And you said it a bit already, but can you explain to me how a VPN works? You can, if you would like, use the whiteboard for this.

Y: Eh, can I draw also?

X: Yes, you can.

Y: [start drawing 8_1]. Okay. So, so, if this is my laptop and I need to transmit to server, and this is the connection is what I have. This is the package in here, this is the tunneling, they are protected from whoever is looking from the outside and this is like Internet. Okay, not very- I hope it is clear.

X: Yes, it is clear. Could you explain to me what a server is?

Y: O, god. The server is terminal that sends out or in information once requested.

X: Okay. And in this drawing, how would it look like if you access an internal application?

Y: Sorry, if?

X: If you access an internal application.

Y: If I access- I am sorry, because the, the audio is not very clear. If I access internal application?

X: Yes. How would this look like in the drawing if you access an internal application?

Y: Okay. Eh, it will be inside from eh, inside the same, I would. No, it would be the same, because I need anyway to connect to a server to have that information that I need.

X: Clear, thank you. And in your drawing, you describe the Internet as above the VPN, do you do that on purpose or what is the relationship between the Internet and the VPN?

Y: [start drawing 8_2]. It is like this. Internet, like it is- No, I just randomly am putting there, sorry. Internet is everywhere I would say, so, it is not the-

X: Okay, clear. Thank you. And you said the package are protected by the tunnel. How are the packages protected by the tunnel?

Y: Because of the eh, of the private channel. Like, when information transits inside the tunnel, they are private, so this is, they become invisible to people from the outside.

X: How do they become invisible?

Y: Because of the, they are eh, use eh, they are coded, I don't know if it is the right word in English, eh, they are, they have, for instance, when you have HTTPS, before a website, like on the eh, on the link, it is like eh, yeah, it is coded. Cypher, they use cyphers. I don't know if it is the correct way to express it.

X: Clear, thank you. And for your computer, does it matter on which physical location you are?

Y: For my laptop?

X: Yes. Would the drawing change if you go to a different location?

Y: Eh, no.

X: Okay. Eh, I am going to ask a question in a different direction. What is the influence of a VPN connection on your computer security?

Y: Well, technically it is supposed to make it better. Eh, because protecting information, you should also be able to recognize malicious threats eh, or at least protect or raise a flag. So, eh, I would say it would increase.

X: How would it recognize threats?

Y: Eh, hopefully having a very good eh, antivirus. No eh, like avoiding website that you don't know, opening e-mails from people you don't know or look suspicious, avoid the eh, phishing, phishing website, phishing e-mails, just trying to be careful. Don't link, or like don't click on whatever link people send to you even if you have VPN connection.

X: What is the role of the VPN connection in this?

Y: To add, I would say, add an extra layer of protection of any communication you can have with eh, like with eh, confidential information. For instance, if I think about communicating with my clients by sending an e-mail to them without eh, being connected to either VPN [0:18:28 until 0:18:29 has been omitted] from the company, it increases the risk of someone being able to exploit the e-mail or to see what there is actually written inside. Eh, instead adding the VPN, adds an extra step in hiding confidential information.

X: Okay, and how- You also said it can help you recognize a threat, how does that work?

Y: Sorry, I also have to recognize?

X: It helps you to recognize a threat-

Y: No, I was expressing wrong, sorry.

X: Okay, no problem. Was just trying to clarify that.

Y: Yeah.

X: Okay. And eh, what else eh, what are the other influences of a VPN connection on your computer security?

Y: What, I am very sorry, it is just the audio, what?

X: What are the other influences of a VPN connection on your computer security?

Y: Eh, I wouldn't know. I would just stick with protection. Increased layer of protection.

X: You mentioned antivirus shortly as well. Does that have a role?

Y: Eh, no, I mentioned antivirus when you asked how you can recognize a threat.

X: Okay.

Y: That was not linked to the VPN.

X: Okay. Then that's clear as well now. Eh, then a broader question. What kind of digital threats do you deal with on a normal day?

Y: Eh, could be eh, most of all it is trying to eh, avoid people to eh, exploit your information. So, phishing e-mails eh, trying to make sure I am not, from my point of view, I am not texting confidential information in e-mails or sharing- Eh, I would say that from my position it would be more trying to not leave my eh, my laptop open or without a password or eh, yeah, I think generally in my small let's say, I would say more attack from the outside as like people reading something they are not supposed to. Eh, so yeah, just phishing, I would say phishing.

X: Okay. And does the threat, or if you think about these threats, do they change because of the VPN connection?

Y: It is not that they change because of the VPN connection, because they can still attempt to do it. Like for instance the man in the middle attack, he might does not know that there is a VPN connection, so, usually they, how they operate is, let's, basically let's try to say in the middle of this transfer and let's see what are we able to catch from that. Eh, they might after, I would say that in the initial stage, they don't change. Of

course, if you realize that somebody has a VPN connection, and you want absolutely exploit that person or that company, you should maybe think about something also physical for instance, using something from social engineering. Being able to actually exploit, I don't know, using the USB, so, not mere digitally.

X: Okay, and if you think about these non-digital threats, does the VPN connection have any influence on those?

Y: Eh, no. On non-digital threats, no. Because if I steal your laptop, and you have documents in their without no encryption whatsoever, doesn't, yeah, I don't need the VPN connection for stealing that.

X: Clear. And eh, if we think about these threats, who or what could be an attacker behind those threats?

Y: Who is the VPN attacker?

X: Yeah, the VPN attacker or the one performing a social engineering attack.

Y: I would say it is somebody- Depends, people do it for various reasons. Usually it is for money, very few people do it for seeking truth or whatever. Eh, it is more for blackmail and exploit the victims for money.

X: Okay. And could you think of other motivations?

Y: Eh, no, because at the end it is all about money. Even if I steal money and power, you have confidential information about somebody that you could use at any time if you don't do whatever they want. Eh, no, because most of the, also most of the attack are, very few are just to disrupt some environment or company. It is more because you want something in return.

X: Clear. And who would want something in return. Who would be the attacker?

Y: Depends. People activists, people that want money for their own costs, people that just, like, scriptkiddie that wants just more money at the end of the month. There could be lots of reasons. Depends also for the company, like who is the victim, usually if the victim is like a state or, a government body or agency, usually it is more to expose them. Eh, like you, maybe they are activists, they do it for having something in return, like for their costs to use the money. Could be to undermine someone else's government eh, if you are just somebody that wants to blackmail a random CEO, you'd do it for money. Yeah, depends, depends on what you are looking for and what your end goal is.

X: Okay. And what would be an attacker's capability?

Y: Capability?

X: Yeah. So, what would they need to be able to do to successfully perform an attack?

Y: With a VPN you mean?

X: Yes.

Y: Depends on how good you know your target. And how much resources you have, how much good you are and if you have, sometimes it helps to have someone from the insight. Eh, definitely it is not something you do from one day to the other. You need a bit planning about that. But I wouldn't say it is not impossible. Because if you think recent privacy scandals about stolen data and confidential information, I probably would say also those companies had VPN and that didn't help much.

X: Would there be some kind of basis background you'd need as an attacker?

Y: Eh, background in, well, if you ask any hacker, if they have like background as a study or something, they will tell you no. They just start to hack, learn on the ground. Are you meaning background of the attacker personal or background on the victim of the attacker?

X: The background of the attacker.

Y: Okay. Eh, well, not they, depends, it is not that everybody eh, sometimes the attacker are like really kids that spend their, their years in front of a computer learning, watching videos. They don't have degree that match eh, hacking. For instance, it is not that every of them has a degree in computer science or something. So, no, you just have to have practical knowledge of the, of how a computer work, how a system work, of VPN. But it is not eh, something that you need to deeply study, I would say.

X: Okay, thank you. How does the kind of attacker change because of the VPN connection?

Y: How does, sorry?

X: How does the kind of attacker change because of the VPN connection?

Y: The attacker or the attack?

X: Both.

Y: Eh, well, the attack change, because, yeah, if you can't eh, take eh, the information while looking from the outside, you need to think differently eh, because it could be something that you didn't, you didn't eh, foresee at the beginning of your attack. So, as I said before, maybe you should consider to enter or to take, like, to steal the information of the company in other way. Eh, for what concern the attacker, I don't think the attacker profile change if there is no VPN.

X: Okay. And what could be the impact of an attack?

Y: The, sorry?

X: What could be the impact of an attack?

Y: Well, the impact of an attack could be eh, disruptive, could be stealing, could affect physically eh, laptop, like laptop servers, virtual environment, for instance you could strike it down, turn it off eh, block it, like you don't have access anymore. Or it could not, you could also not even realize, and it could just be spying on your information, on what you're doing with your laptop or stealing everything, and you didn't even realize they were in. Eh, modifying information inside your eh, your servers, your eh, yeah, your laptop. It could be a lot of different attacks that you could do. And lot of different outcomes.

X: Okay and eh, if we think about the VPN connection in itself, how secure is a VPN connection?

Y: In, sorry?

X: If we think about the VPN in itself-

Y: Hmhm.

X: How secure is a VPN connection?

Y: Eh, technically a lot. Because this is how, this is what the scope it is supposed to work. This the why has been created a VPN connection and the why you install it is to protect, but also, the strongest for instance, the strongest type of encryption could be exploited at some point with effort and patience. So, there is always a possibility, a small chance that something might not work. Nothing is secure at 100%, especially in cyber.

X: You mention encryption, what is the relationship between encryption and the VPN?

Y: The information transfer are encrypted.

X: Okay.

Y: You use encryption.

X: How does that help you?

Y: It helps, because if you don't have, if you send from one point to another, information encrypt need to have like the key to actually read the encryption, if you don't, if you see from here, you just see a lot of symbol, let's say inside. So, if you don't have the key to decrypt them, they have no sense for you. Have no meanings.

X: And if you think about the vulnerabilities you possibly mentioned of the VPN connection. Do your actions change because of those vulnerabilities?

Y: If change, sorry, if change?

X: Do your actions change because of these vulnerabilities?

Y: Eh, not really, because there are some vulnerabilities that I might not be able to control, for instance where the VPN server is based, who is stealing with, like who is the service providers, there are some things, usually it is a third party. So, I don't have control over that. Eh, and it could not, could be something for instance eh, also where the server is located. If it just a country where protection is not really eh, in place, also, like, from the point of view of eh, confidential information. Eh, I don't know how much eh, powerful, powerful or how much big the servers are. So, there might be eh, if the powers goes off. There are a lot of things that can happen that are outside the control of actually the user of the VPN.

X: Yes. And you say it matters who the VPN supplier is, why does that matter?

Y: Why does it?

X: Why does it matter who the VPN supplier is?

Y: Because the, not everybody as we know has eh, the same level of security, or have to respect by states or by law the same level of protection. So, for instance I expect that in, usually in Europe or in the US, there might be a big, like, higher level of requirements a company can ask when provide this kind of services. For instance, in other eh, in other it might be eh, more- If I have to choose between set a VPN service in

[country] or in [country], I would probably wouldn't go for [country], because I know that they are, there might be more implication politically. And if something happened, it might be more, it might be harder for me, from being based in Europe, to actually understand what happened eh, and where my, my information went. So, yeah, this is why it matters.

X: And can you think of any other yeah, risks or threats with VPN?

Y: Eh, they can trust some VPN that for instance eh, I know they do it anonymously, but they still collect information from eh, they use for statistic and everything, but we, yeah, I think everybody knows that is not a good eh, a good thing in any case to have information, even if randomly and anonymously. Because you also don't know if what, actually the law on their side, for instance because of the location, you don't know how much eh, anonymized the information are, to which extent they can actually collect this kind of information coming from you. I would say that all the risk could be related to privacy and eh, yeah, privacy and confidentiality.

X: Are there any other risks?

Y: Risk could be that someone breaks in in the server, like physically. Could be someone breaks in where the servers are and, I don't know, like switch cables, but I think that would be too much eh, eh, movie, I would say. Because you are, you are supposed to have like secure physical environment when you keep this kind of eh, of server. It can happen, but also, statistically, it is less possible then a digital attack in this case.

X: Okay. Thank you. Those were actually my questions so far. Is there anything you want to say about VPN that did not, that was not spoken about now?

Y: Eh, no.

X: Okay.

Y: Everything.

X: Okay. In that case eh, I would like to thank you a lot for your participation, this helps me a lot.

Y: Okay, I hope so.

X: And do you have any questions for me?

Y: Eh, no. No.

X: Okay.

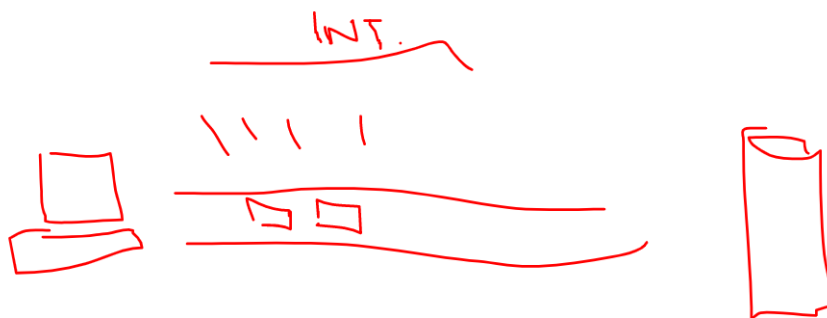


Figure C.8.1: Drawing 8_1



Figure C.8.2: Drawing 8_2

C.9: Transcript Expert 9

Duration: 46 minutes

Language: English

Number of drawings: 5

X: Could you explain to me what a VPN is?

Y: Eh, yes. VPN eh, from what I know I think it is a sort of private network and it is used within [the professional services firm] as well, so we use [the VPN of the professional services firm] to log into a private network that is operated, managed by [the professional services firm]. And from what I know it is, well, it separates the private network with the external network, so the big bad Internet and it makes the Internet connection more secure and it allows for eh, well, services that are only allowed if you are logged onto the private network. That is my understanding.

X: Okay. And what kind of services do you mean?

Y: Eh, services such as, we have some [an internal page] for example, that is only accessible if you are connected to eh, [the VPN of the professional services firm], so that's [0:02:28 until 0:02:46 has been omitted]. Yeah, I think that's it.

X: Okay. And you describe it as a private network, what do you mean with private?

Y: Eh, as in not connected to the external eh, Internet, I suppose. It is like a shell around your organization and inside the shell all the data traffic is of course not linked to the outside world and the data traffic inside it is managed as well by your own organization or the third party who is managing this internal network. Yeah, that's my understanding of it.

X: Okay, and eh, with manage, in what sense do you mean that?

Y: Eh, some sort of restrictions, like probably I cannot visit all websites, or they can also manage, well, what websites I visit and eh, what data I send out or download probably. I have not met anything like this eh, but yeah, I think those are the possibilities.

X: Okay, and you said that it makes your connection secure, what do you mean with secure?

Y: Eh, well, from what I know, if you normally log onto the Internet, you of course you have eh, you log in from your outbound network, so you have your own IP-address and eh, when you visit a website, it is like two servers talking with each other. And eh, yeah, they can see my IP-address and eh, if I am more technical maybe you can also view their IP-address. And if you use a VPN, I think that is like an extra wall in between, so my connection goes via the VPN to this external source. So, they cannot directly view what is my eh, IP-address, among other data. I am not so sure what other data they can't get to, but pretty sure about the IP-address part.

X: Okay, and you mentioned a server, what is a server?

Y: O, good question, haha. Eh, basically eh, a device that regulates data traffic going in, going out. Eh, yeah, it is able to store data, it can manage the eh, also the Internet traffic going in and out, I don't know. I don't have a good definition for what is a server.

X: Okay, and in what sense does it manage the traffic?

Y: Sorry, can you repeat?

X: In what sort eh, in what kind of sense does it manage the traffic?

Y: Eh, you mean the, a server or the VPN?

X: The server.

Y: Does the server manage traffic, I don't think the server does it by itself, right. I think it is either VPN or the person that manages the VPN or some sort of firewall that can manage traffic. I don't think that is something that happens in a server, right.

X: Okay. Eh, that makes it a bit more clear what you meant earlier. Eh, why do you use a VPN?

Y: I think I touched upon that briefly already. Eh, well first off to eh, for an organization like [the professional services firm] it is good to identify your eh, employees, that they are part of this private network, they can identify themselves. And by doing that eh, you can then provide the extra services, such as [0:06:44 until 0:06:47 has been omitted], so examples I gave before. Eh, and other than that, also the secure connection of course. It helps that you cannot visit for example weird websites or download malicious software. Or at

least, that's a bit more regulated than not using a VPN. Eh, and of course the story about the IP-address that it's masked, that also offers some security benefits, from what I know. Eh, yeah, I think those are the prime examples.

X: Okay, what would be the benefit from masking your IP?

Y: Eh, good question haha, I am not too technical in this area. I do know that eh, if you know someone's IP, you can eh, have targeted attacks on that IP. You can eh, how do you say that, I don't know if for example DDoS attacks are related to this. I give you our- If you know an online address and you want to target this with a hundred computers, then you're able to do so. Eh, yeah, it is the identity of your network, your internal network. I don't see why you'd want this to be exposed to the outside world. Especially if I am logging in from home right now and I am working, would it make sense for eh, the connections I have in the workplace to have my personal IP-address, so to say.

X: Okay. And do you use a VPN for any other purposes?

Y: Eh, yes. Eh, some things I can think of are for example some services that we use as eh, just at home. Eh, for example [country] has a very strict policy for [social media platform] for example, it blocks videos. Eh, and if you can use a VPN to eh, mimic you are in a different location, or at least shield that you're in [country], then maybe you can view other videos. Eh, I think that is one of the applications for a VPN. Eh, yeah, yeah, I think that is it. Other than the security reasons of course that I already mentioned. Those are, yeah, strong reasons to use a VPN as well.

X: Yes, and do you also use the [the professional services firm] VPN to change your geographical location?

Y: No, no.

X: Okay. Eh, then another question. What actions do you take to create a VPN connection?

Y: So, for me, to create one?

X: Yes, as a user.

Y: Eh, well, then I would Google some services, I suppose.

X: Oh, I mean the [the professional services firm] VPN.

Y: [the professional services firm] VPN. Eh, I don't think I fully understand your question. To create a [the professional services firm] VPN?

X: Yes-

Y: Because it is already there, right?

X: If you want to connect to the [the professional services firm] VPN-

Y: Yes.

X: What steps do you take to make that connection?

Y: Eh, well, we have this [access token provider] token. It used to be a physical token eh, but now it is an application that we have on our work phones. Eh, and in the bottom right of our laptop we have this connection screen and you can click on [the VPN of the professional services firm]. Then you need to fill in eh, your own passcode, including the token inside this application eh, and then you're logged into the VPN.

X: Okay, and you said it used to be a physical token, is that still an option?

Y: No, no, the physical token I think we stopped using that two years ago. Or longer even.

X: Okay. On what devices do you use the [the professional services firm] VPN?

Y: Eh, only my laptop I suppose.

X: Okay. Do you have an, a phone from [the professional services firm] as well?

Y: Yes.

X: And do you use a VPN on that?

Y: Eh, well, on my phone I don't need to log onto a separate network, but I do know there are other eh, authentication mechanisms, to still identify that I work at [the professional services firm]. Eh, yeah, I am not sure if you can call those VPNs.

X: Okay. Could you explain to me how a VPN works? If you'd like, you can use the whiteboard for this. I will remove my drawings.

Y: [start drawing 9_1]. Eh. Well, have my laptop here, and you have Internet here. Doesn't show up. This doesn't work the best for me, but just gonna leave it. Eh. Draw a straight line. Suppose normal circumstances, you'd have this direct connection from your network to the external, yeah, to the Internet,

to whatever sources you eh, you might want to visit. [\[start drawing 9_2\]](#). And a VPN is, it is like a private network that you connect to using eh, yeah, different kinds of methods, I our it is using the eh, [access token provider] token. And via this VPN you connect to the Internet. [\[start drawing 9_3\]](#). And then you don't have this anymore. That's a very simple graph, but yeah, because I am not too technical, I am probably missing a lot, but eh, I think this is how it works.

X: Okay. And could you tell a bit more about the bubble with VPN?

Y: Eh, what would you like to know about it? Like-

X: Well, for example, you said it makes the connection secure-

Y: Right.

X: Is that somehow visible in this drawing?

Y: Eh, well, what is visible already is of course that my personal connection is not linked to the, the external network, that already makes it more secure. Eh, yeah, it also can filter or block out some traffic that is unwanted. [\[start drawing 9_4\]](#). So, I don't know, I can draw a filter in here, maybe, just over there. I guess. Eh, that makes it more secure. Yeah, I am not too creative in this, I expect you notice.

X: No problem.

Y: How can I demonstrate this in this picture. That's a good one.

X: Yes, or any other things that come up related to the VPN.

Y: Eh, no, it masks your identity eh, it filters some data traffic that is unwanted, I guess it is two-way, so there is always an arrow back of course from the Internet to the VPN. [\[start drawing 9_5\]](#). So, can also draw this, I suppose. Then in here there is also a filter. Eh, yeah, maybe, what else, yeah, something about the location maybe, I don't think the location makes it more secure, it is just a different location eh-

X: What do you mean with I don't think the location makes it more secure?

Y: Yeah, so, like my personal network can be here in [place], but the VPN can be a server hosted somewhere else in eh, I don't know, in [place]. It just connecting via different location, such as [place] for example, doesn't necessarily make the connection more secure. That is what I mean.

X: Okay, and what is a server in this drawing?

Y: Eh, the server, well, the server that my internal server speaks with in order to eh, identify myself and then reroute my data traffic to the external source, to the external party.

X: Okay. And you have drawn two filters, is there a difference between those two?

Y: Sorry? Difference between?

X: A difference between those two filters.

Y: Eh, no, I suppose not. I think, what I have in my mind is just eh, a whitelisting and blacklisting feature eh, so if I am connected to the VPN, they can eh, they can regulate what sources I visit. For example, if the [the professional services firm] network does not want me to use [cloud software] to share files, then they can filter out eh, [cloud software], or even block it. Eh, yeah, it depends what measures they have. It can also have alarming eh, signals that someone who uploads something to [cloud software] that an IT team gets notified or something and then they can take appropriate action, I am not too sure what they do. Eh, yeah, so I guess two level, so one is signaling, they can manage data traffic and secondly, they can actually block websites, which I guess is what I mean here with filtering. So maybe they can block me from visiting [cloud software] website. Eh, and the way around, yeah, the traffic coming in eh, from the Internet, maybe when I am downloading something. If they don't want me downloading a huge trojan from a shady website, then they can block the website, or they can even block the download. Eh, yeah, does that answer your question?

X: Yes, it does.

Y: Hmhm.

X: And if we would change the, your location, so your personal network would change eh, to a location in a coffee bar, would that alter this drawing?

Y: Well, just the location, no. If you consider all the same safety measures eh, no, I don't think so, the only thing that changes is your IP-address, right.

X: Yes, okay. And then another question. What is the influence of a VPN connection on your computer security?

Y: Eh, difficult question. Yeah, I already mentioned the part about the IP-address, that it eh, yeah, instead of my IP-address talking with the outside world, it is the VPN. Eh, yeah, other than that. No, I am not so sure what I can add, what I already told, told you.

X: Okay-

Y: Maybe my understanding is just too limited.

X: No problem, this is very good already. Eh, what kind of digital threats do you deal with on a normal day?

Y: Digital threats eh, as an [the professional services firm] employee or just a regular Internet user?

X: As an [the professional services firm] employee.

Y: Well, I guess we work with a lot of confidential data, you wouldn't want that leaked. Eh, we're talking about security threats, right?

X: Yes.

Y: Yeah, we, yeah, we wouldn't want confidential data to be leaked or sent to the wrong party. It can be a lot of sensitive data, that [0:21:20 until 0:21:31 has been omitted]. Yeah, so of course data security and confidentiality is a very big thing for us. Eh, yeah and that's a challenge we face on a day by day basis. Like how do you [0:21:42 until 0:22:04 has been omitted]. Yeah, and storing the data that we have of course, like we often work with [0:22:16 until 0:22:34 has been omitted]. Yeah, that's something that you want to safeguard, of course, offline on your laptop and you don't want that leaked out if someone were to, for example, gain access to your laptop. And we also work with [0:22:50 until 0:23:21 has been omitted]. So, that's also same thing that you want to safeguard. Yeah, and from myself just to upload all the documents that I have, that I use to [cloud software], yeah, since that is eh, more secure than just having it on my laptop. You cannot just access eh, so the name of that tool is called [an internal page], you cannot just access [an internal page] eh, without the proper access rights. Eh, does that answer your question or are you looking for something else?

X: Yes, that answers the question. You mentioned threats that are eh, like, from a perspective from what you can do wrong or what other employees can do wrong, but are there also threats that come from the outside?

Y: Eh, yeah, I guess, if you download the wrong file, it has a keylogger or something, that someone can steal your passwords. Of course, you have trojan horses, worms eh, yeah, what have you, just, I guess in general viruses that you would not want in your computer that can hinder the data, remove data or even steal data. Eh, that is something that we would not want and that comes from the outside. And yeah, what else, maybe not a security threat, but more from an availability standpoint, you have also DDoS attacks of course. If some party were to perform a DDoS attack on [the professional services firm] eh, to take down the servers, then we cannot work anymore and that's yeah, that's also a threat that we would not want. Eh, what else. Eh, I think those are the main, the main things.

X: Yes, very clear. And how does the threat change because of the VPN connection?

Y: Eh, like I said, so, they can, of course you can acquire viruses through different means, like it can be eh, through a USB stick for example, it can be because you download a random file from the Internet. Eh, I think a VPN can eh, manage that. If you'd log onto a network, they can eh, like I mentioned before, you have this filtering or at least these signaling controls he, where, where the managers of the VPN they can identify it and they can block it. Eh, to prevent these things from happening. For example, if I bring in a random USB stick, they can identify that and even stop me from using a USB stick. Eh, or they can prevent me from visiting a malicious website, or downloading malicious software. Eh, I think a VPN can play a big role in that.

X: Eh, and do you also mean that a VPN eh, would be able to stop you using a USB stick?

Y: Well, of course, I can plug it in myself, eh, but for example, what files can be run, like if it has an alter executable on the USB stick, I think a VPN can play a role in that, in preventing, or at least detecting what I am doing, with the data on the USB stick.

X: Okay. And you also said that it can eh, block certain things coming to you from the Internet-

Y: Hmhm.

X: What kind of things could be blocked?

Y: Eh, just websites, I suppose. If they know that eh, www.virus.com is eh, is a malicious website, they can block it. Then I cannot visit that website. Is that what you mean, or?

X: Yes. And is a VPN able to block any other things as well?

Y: Eh, well, websites, download, yeah, I guess it regulates data, if you put it broadly.

X: Yes, okay. Eh, and then also, this was about digital threats-

Y: Hmhm.

X: What kind of social threats do you deal with on a normal day?

Y: Social threats. Can you define social threats?

X: Yes, I mean all threats that are non-digital.

Y: Very broad description. Eh, difficult question. Let me think about that. You are still talking in the area security, right?

X: Yes.

Y: Eh, your question is does a VPN help with that, or does it block those threats?

X: Well first of all eh, it is more in a general sense-

Y: Hmhm.

X: So, what social threats do you encounter on a normal day, if you don't take the VPN into account?

Y: Well, eh, maybe to take your coffee shop as an example or coffee place, eh. If [0:29:14 until 0:29:16 has been omitted] and then I want to, yeah, maybe work from a [example of restaurant], you often have eh, an open network, like everyone can sign on to it, but that also means that eh, well, it is an unsecure connection to that network. Eh, not sure where I am going with this, but eh, let's say I am working there and eh, I don't want someone looking on my screen or something and then someone else is sitting behind me and can look on my screen. Then I guess that is a social threat and having a VPN does not help with that. Eh, yeah, what else can I really think of.

X: You shortly mentioned an open network-

Y: Yes.

X: Eh, does that eh, matter for the VPN connection? Or would that pose a certain threat?

Y: Eh, I think not for the VPN maybe, but it could be a threat for my own laptop, I suppose.

X: And how could it form a threat?

Y: Eh, from, from what I read, I am not too sure how accurate this is. Eh, if you'd just connect to an open network, especially if it is unencrypted and you then use your laptop and you log onto websites, eh, fill in your credentials, then this open network, or the person who operates it, or the group. Eh, they can actually view what, what data I am sending. So, also what my username or password was if I, if I fill that in. Eh, and then this other threat is of course someone is impersonating that network and then someone eh, hosts a private, sorry, an open server on his phone or laptop and impersonates that he is [example of restaurant] and I log onto that network and I give my data or I sign onto websites that I normally use, then, and then my data could potentially be stolen. I think that's eh, that's a possibility. It never happened to me. Eh, yeah, does that help?

X: Yes, it does-

Y: Or are you still looking for something else?

X: And how does the social threat change because of the VPN connection?

Y: Eh, I don't think it does change. I'm thinking what other social threats are there. Like social threats if eh, the social threats impact people. And people are always I think the weakest link in security. So, if someone eh, approaches me and can look onto my screen, if I have confidential data on my screen and someone looks at it, the VPN does nothing for that. Eh, there are some physical measures that you need to take, like eh, eh, I don't know how you call it, but like a screen so someone else cannot peek onto your screen. Eh, yeah, well, what else. If someone impersonates that he is my boss for some reason, eh, he is my boss and needs my password, and I give it to him for some reason, I guess that is also a social threat. Then, yeah, having a VPN also does not help for that of course. Eh, yeah-

X: Yes, and the other threats you mentioned, of using an open network, does the VPN have a role in this?

Y: Eh, yeah, I guess, eh, yeah, because then the VPN still replaces my own network, I suppose. Eh, and that, so, the VPN can still regulate what data I send or eh, or that gets send, so in that sense I suppose if I log onto a [example of restaurant] network and then my VPN, then my connection would be more secure, yes.

X: Okay. And If you think about these digital and social threats, who or what could be an attacker behind the threat?

Y: An attacker. Eh, you need to split it up. So, digital threats, so, I mentioned viruses, that doesn't necessarily have to be a person, eh, ... but you yourself are the threat basically, because you would need to be the one to get it in. Eh, yeah, if an external person were to try and brute force my login code and password from an external source, I guess that's also a possibility, eh. Can you repeat your question again, eh-

X: Yes.

Y: For the social part.

X: The question is who or what could be an attacker behind the threat.

Y: Hm. Who or what, eh? Yeah, like a hacker or a person can eh, try and brute force into my server, I guess a person is a hacker, it can be anyone with malicious intent. What, it can be a server, a server hosting a website with malicious data, that if I were to visit it and download it, that is a threat to me. So, I guess a server-

X: Okay, and if we look more into the persons eh, could you give an example of a person who would be an attacker or could be an attacker?

Y: Eh, so again, me as a [the professional services firm] employee, right?

X: Yes-

Y: Who would want to attack me. It is a difficult question, I don't see a reason why they would want to attack me. Because then they would first need to know [0:36:33 until 0:36:35 has been omitted], what confidential data I have, before they would want to even specifically target me, eh. So, it is very hard for me to give an example. Who would want that?

X: Okay, and if we look at a more abstract level to [the professional services firm] as an organization as the target.

Y: Right, yeah.

X: Then who or what could be an attacker behind a threat?

Y: Eh, I guess two main things that people would want to steal I guess are the personal data of all the [the professional services firm] employees, the names, addresses, yeah, just all personal data, cause that's valuable to them. You can sell it off to what have you. And of course, we have client data, those are the crown jewels I suppose of [the professional services firm]. So, if anyone were to want that, eh. Yeah, personal data is anyone who is after quick money, I suppose. Eh, yeah, I still call them hackers, cause I just don't have a better term. It can be anyone. Eh, yeah, and for client information, yeah, same for that, but maybe, because we are thinking more about [0:38:03 until 0:38:09 has been omitted]. But then again, it- The same term applies, it is still hackers. Eh, yeah, I don't think I can really specifically name a person or a group of people who would want to perform this.

X: Okay. And what would be an attacker's capability?

Y: An attacker's capability. Eh, what do you mean by that?

X: Eh, what would be an attacker's background need to be to be able to perform an attack?

Y: Depends how sophisticated that attack would be. Eh, Yeah, there are very, there are a lot of ways to attack, so to say. Eh, if it is just setting up a malicious website, then I suppose you need basic knowledge of how to set-up a website. Eh, if you want to program your own eh, virus, your own trojan, then I guess you also need some coding experience. Eh, I don't think there is a study to become a hacker. Eh, yeah maybe, you have ethical hackers of course, but yeah, suppose then, yeah, just some programming background would help of course. Eh, yeah, but there is plenty of information online of course. Like if you want to become a hacker eh, you can do it. You just need eh, to know where to find it on the Internet to get the right eh, coding knowledge and then you need the experience. Just need to try it.

X: Okay, and how does the kind of attacker change because of the VPN connection?

Y: Eh, yeah, eh, I guess a potential attacker can also be someone already working internally at [the professional services firm]. So then, yeah, if you don't have access to the VPN, then you cannot be eh, an internal employee. And if you do use an employee eh, if you do use a VPN, then the attacker could be an internal employee, who already has access to the network. I guess that is a change. Other than that, I cannot think of anything else.

X: Okay. And if we think from the perspective of [the professional services firm], what could be the impact of an attack?

Y: Phoe, huge, I suppose. Eh, first as personal data and eh, the biggest thing is of course the confidential data, if we lose our client data eh, yeah, that is a major breach in trust. Eh, our clients trust us with their confidential data, and trust us that we safeguard their data. If we lose that it is just a lot of reputation and eh, brand damage to [the professional services firm]. [0:41:35 until 0:41:40 has been omitted. Our entire practice is based on trust, without trust there is no [the professional services firm]. So, in that aspect, yeah, it would be catastrophic to [the professional services firm] I think if that happens.

X: Can you think of any other impact?

Y: Eh, other type of impact or eh, what do you mean?

X: Yes, other type of impact.

Y: Eh, yeah, it can have financial impact, I suppose. Like it would cost a lot of money to eh, find out where the leak happened and to close this leak and to track all the data that you lost and follow up with the client as well, because of course you need to report this to the local authorities, to the AP for example. And eh, most definitely to the client, you need to report it to them, that you lost their data, eh. [0:42:38 until 0:42:39 has been omitted]. The client needs and has the right to know that their data has been compromised as well. So, you need to communicate that. [0:42:45 until 0:42:52 has been omitted]. Eh, yeah, so a lot of time, and effort, money is involved as well, I guess, that is also a major threat. Eh, is that what you're looking for, or?

X: Yes, it is.

Y: Okay.

X: And now another question. Eh, if we look at the VPN connection itself-

Y: Yeah.

X: How secure is a VPN connection?

Y: How secure, I don't think I can answer that, it depends. It depends on the operator of the VPN, how secure the person or the group makes it, right?

X: And what would you mean with how secure it makes it? What could change?

Y: Eh, the filters that they apply. If I log onto VPN, what filters do they apply on data traffic or what, what data traffic do they block, that is something that the, the operators of the VPN can configure. Eh, if they don't configure it, then it is maybe not very secure. If they do configure it and go very far, like even block my [e-mail] use, that I don't send some confidential data to my private e-mail or something, it can be very secure, but also very annoying for the users. So, yeah, my answer is, it depends.

X: Yes, okay, very clear. These were so far my questions. Is there anything important to know about VPN that I did not ask about?

Y: No, I think you did a good job. You eh, well, at least my knowledge of VPN is very limited, so, I think you asked- You pulled all the knowledge out of me about VPN, so in that case, yeah, good job.



Figure C.9.1: Drawing 9_1

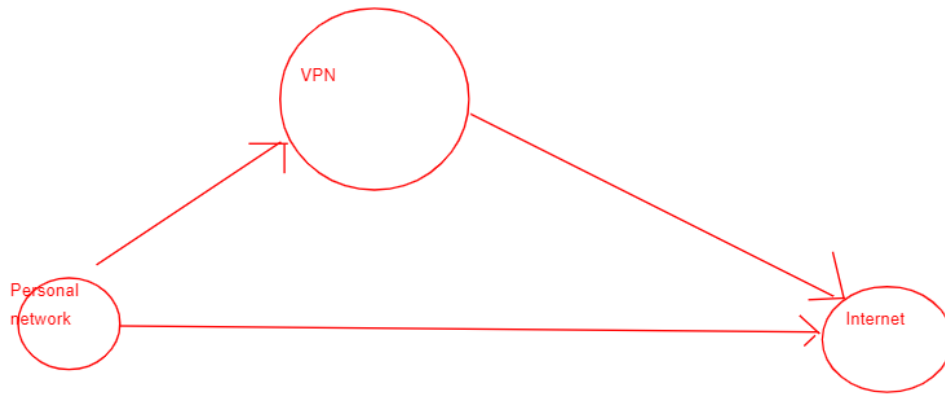


Figure C.9.1: Drawing 9_2

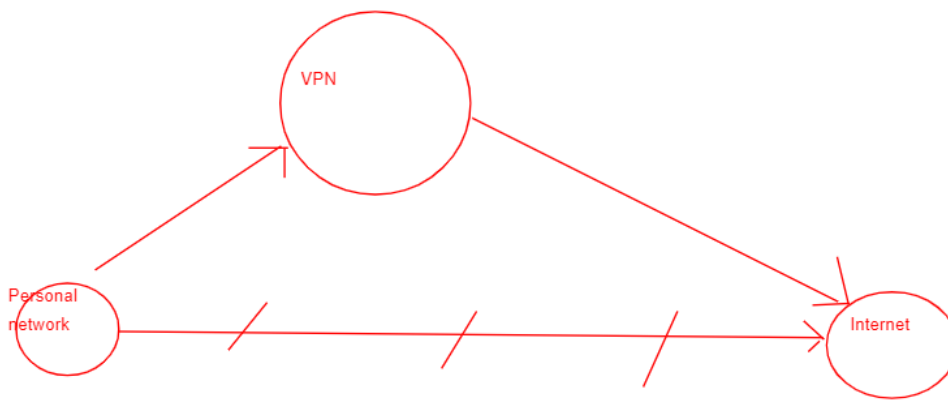


Figure C.9.1: Drawing 9_3

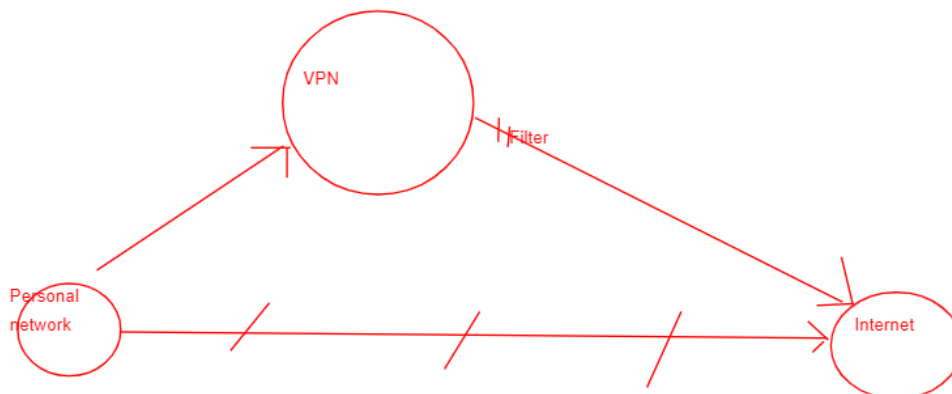


Figure C.9.1: Drawing 9_4

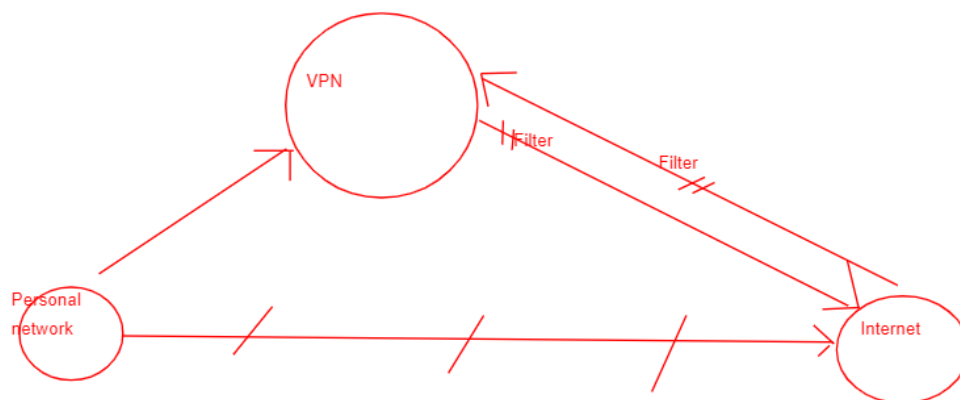


Figure C.9.1: Drawing 9_5

C.10: Transcript Expert 10

Duration: 40 minutes

Language: Dutch

Number of drawings: 3

X: Dan begin ik met de eerste vraag van het interview. Kun je aan mij uitleggen wat een VPN is?

Y: Haha. Nou ja, kijk, ik denk dat een VPN heel lastig woordelijk eh, uit te leggen is, maar het komt erop neer dat het een soort van tunnel is naar een andere computer. Eh, waarbij jij vanaf jouw eigen device een eh, nou ja, als het ware een tunnel opzet die versleuteld is, die verkeer naar de andere eh, eh, server of eh, toestel versleuteld. En vanaf dan acteer je eigenlijk als het ware vanaf dat andere eh, toestel of server, hoe je het wilt noemen. Eh, en nou ja, dat heeft allerlei voordelen, maar in feite is de VPN dus de, de verbinding naar, zo zou ik hem omschrijven.

X: Oké. En kan je iets meer uitleggen wat je bedoelt met een tunnel?

Y: Eh, ja, eh, ik zou zeggen dat is een verbinding, zoals eigenlijk eh, iedere verbinding er een is. Maar deze versleuteld eh, het verkeer vanaf jouw eigen device tot en met eh, de server. En daardoor kun je als het ware als buitenstaander niet eh, het verkeer nou ja, lezen, of eh, nou, onderscheppen kan wel, maar je kunt er in ieder geval niets mee zonder het sleutelmateriaal. Eh, en omdat het dus om een afgeschermd eh, eh, verbinding gaat op die manier, spreken veel mensen van een tunnel.

X: Oké. En op wat voor manier is het versleuteld?

Y: Eh, uit mijn hoofd via public-private-key.

X: Oké. En je zegt dat de tunnel loopt tot de server, wat is een server?

Y: Haha. O god. Eh, een computer, haha.

X: Oké. En wat gebeurt er daarna met de verbinding? Na de server?

Y: Eh, hoe bedoel je?

X: Is de server het eindpunt van de verbinding?

Y: Volgens mij wel.

X: Oké. Kan je iets meer vertellen over deze server?

Y: Eh, anders dan dat die VPN moet ondersteunen, nee.

X: Oké. Prima. Dan de volgende vraag, waarvoor gebruik jij een VPN?

Y: Eh, binnen [the professional services firm] gebruik ik een VPN om eh, een verbinding op te zetten naar het [the professional services firm] netwerk. Eh, zodat eh, ja, mensen zeggen altijd zodat je verkeer veilig is, he. Eh, zodat ik veilig kan eh, eh, mijn e-mail kan checken. Ik denk dat dat ook wel klopt, want in feite maak ik verbinding met de server van [the professional services firm], waarop al mijn applicaties draaien en eh, daar staat eigenlijk alle data op van [the professional services firm], dus als het eh, als het erop aankomt dat ik eh, nou stukken van [the professional services firm] wil inzien, en die zijn ook maar enigszins

vertrouwelijk eh, dan gebruik ik een VPN, want dan heb ik inzage of dan heb ik de mogelijkheid om die stukken te bekijken. Eh, dat is eigenlijk waarom ik de VPN gebruik.

X: Ja, zijn er nog andere redenen waarom jij de VPN gebruikt?

Y: Eh, nou ja, waarom ik het gebruik niet. Ik denk dat [the professional services firm] een VPN afdwingt eh, omdat ze daarmee ook gemakkelijker kunnen inregelen dat ik bijvoorbeeld niet naar bepaalde websites ga waar ik helemaal niets te zoeken heb.

X: En hoe hebben ze dat ingeregeld?

Y: Dat hebben ze ingeregeld op die server waar ik verbinding mee maak, want als ik die VPN-verbinding niet opzet vanaf mijn laptop, dan kan ik wel bijvoorbeeld naar alle websites die ik wil. Nou, dat is niet helemaal waar, maar laten we even voor het gemak zeggen dat het kan. Eh, maar als ik die VPN opzet, dan maak ik dus als het ware verbinding eerst met die andere server van [the professional services firm] en acteer ik vervolgens als het ware als die server en dan heb ik ineens wat extra restricties.

X: Oké-

Y: Maar ook de voordelen van de eh, vertrouwelijkheid en de integriteit.

X: Ja. En als een gebruiker, welke handelingen voer jij uit om een VPN-verbinding te maken?

Y: Het meest basale antwoord is denk ik eh, ik maak een Internetverbinding, vervolgens eh, start ik een programmatje op dat eh, dat de VPN-verbinding voor mij opzet en daarvoor maar ik gebruik van een gebruikersnaam, wachtwoord en eh, tokencombinatie. Nou, als dat goed lukt, dan wordt de verbinding voor mij automatisch opgezet.

X: Oké. En kan je meer vertellen over deze token?

Y: Ja, die token dat is eh, een token die via een RSA-algoritme wordt gegenereerd en eh, ik heb dat op mijn telefoon heb ik een app hiervoor geïnstalleerd, daar heb je uit mijn hoofd, iedere zestig seconden wordt die eh, token vernieuwd en eh, nou ja er zit wel wat latency op, op het moment van token op mijn app versus wanneer kan ik hem nog invoeren. Dus nou ja, wat ik daarmee bedoel is ik moet die token invoeren op mijn laptop, nou kan het in theorie zijn dat die token op mijn app net even vervallen is, nou dan kan ik hem nog wel eh, invoeren en wordt die als geldig gezien. Ik denk dat dat een seconde of tien is ofzo, dat durf ik niet met zekerheid te zeggen.

X: Ja. En je zegt dat het een app is, is er ook een andere mogelijke manier?

Y: Eh, ik meen dat de eh, hardware token nog steeds wordt ondersteund. Eh, eigenlijk is het principe dan hetzelfde. Je hebt een eh, ja, wat is het, een soort kastje, of een soort sleutelhanger eigenlijk. Eh, waarop eenzelfde soort token iedere zestig seconden denk ik wordt weergegeven. En dan wordt die vervangen door een andere token via ik denk hetzelfde RSA-algoritme eh, ik weet echt niet welke dat het precies is. Maar het is in ieder geval RSA en ja, verder werkt het mechanisme hetzelfde. Je moet wel aangeven of in die applicatie of ergens anders, dat weet ik niet eens meer, welke token je gebruikt. Eh, dus je moet wel ergens je token koppelen aan eh, nou, jouw laptop en jouw gebruikersaccount, anders zou je een willekeurige token kunnen gebruiken natuurlijk.

X: Ja. En op welke apparaten gebruik jij de [the professional services firm] VPN?

Y: Ik gebruik hem alleen op mijn laptop.

X: Zijn er andere mogelijkheden?

Y: Nee, dat is niet waar trouwens. Ik gebruik ook een VPN-connectie op mijn eh, op mijn telefoon. Maar dat werkt net even wat anders. Eh, volgens mij kun je ook eh, en dat is via dezelfde VPN-connectie, via eh, iPad, tablet, kun je ook VPN-verbinding opzetten. Die VPN-verbinding via telefoon die werkt op een andere manier trouwens, dat werkt via Citrix. Eh, ik weet niet uit mijn hoofd of dat technisch een VPN-verbinding is eerlijk gezegd.

X: Oké. En hoe werkt een VPN? Als je wilt kun je hiervoor ook het whiteboard gebruiken. Ik zal mijn tekeningen weghalen.

Y: Hmhm.

X: En zou je mij dan kunnen uitleggen hoe een VPN werkt?

Y: Eh, nou laten we eh, ik ga gewoon een poging doen. [\[start drawing 10_1\]](#). Laten we zeggen, o, je kon ook typen, he. Even kijken. Werkt dat zo, nee. Even wat dingen aan de kant zetten. Bij mij werkt het typen van de tekst niet.

X: Als je op de T drukt, dan is het ook als het ware alsof je een vierkant moet trekken en dan kan je daarin typen.

Y: O, nu doet die het wel. Nou, oké. Eh, nu doet die het weer niet en nu weer wel. Oké. De VPN server. Eh, dus eh, je zit als het ware eerst een eh, nou, je hebt eerst verbinding nodig met het Internet. Kunnen we het Internet ook nog intekenen toevallig. Ja, dat kunnen we. Wolkje, ofzo. Eh, dus wat je doet is eh, je zet een verbinding op eerst met het Internet, dat is eigenlijk tot hier. En vervolgens eh, benader je de VPN server met eh, jouw inloggegevens. Dus in mijn geval is dat een gebruikersnaam een eh, wachtwoord en een token. Eh, even kijken hoor. Ik doe dit niet dagelijks. Eh, even kijken. Goed. Je meldt je aan eh, vervolgens eh, heb je hier een soort van eh, nou ja, een bibliotheek waarin mijn gegevens dus ook staan, en heb je datzelfde RSA-mechanisme dat kan controleren van goh, is het [me] wel in dit geval. [start drawing 10_2]. En als dat oké is, dan eh, gaat die gewoon weer terug, dan zegt die joh, je bent aangemeld. [start drawing 10_3]. En vanaf dan eh, heb je een succesvolle VPN-verbinding en gaat eigenlijk alles zo, via de server, en kun je vanuit daar doen wat je wilt.

X: Oké-

Y: Nou zit er een stap tussen. Eh, ik weet niet precies, ik heb hem er niet ingetekend, want ik weet niet precies waar die zit, maar je moet ook nog ergens een handshake maken van goh, welk certificaat gaan we nou eigenlijk gebruiken, welke versleuteling, welke versleuteling. He, want een verbinding is eh, deze initiële verbinding is natuurlijk als wel versleuteld eh, want anders zou ik mijn eh, inloggegevens direct over het Internet versturen en dat lijkt me ook niet handig. Volgens mij zit er vooraf, zit er nog ergens een soort van eh, pingetje van mijn device naar de VPN server die dan zegt van hoi, ik wil verbinding gaan maken. Dan komt er volgens mij eerst nog een signaaltje terug van nou, dat is goed. Ik ondersteun deze versleutelingstechnieken. Laten we zeggen TLS 1.2 of whatever, en deze eh, cijferpers, noem maar op. Nou, vervolgens zegt mijn device volgens mij is goed eh, ik ondersteun ook deze eh, versleuteltechnieken. Ik eh, ik stel voor dat we deze techniek gebruiken en omdat dat er dus eentje is dat de VPN server ook is, stuurt die direct de publieke sleutel mee. Eh, vervolgens wordt er een berichtje teruggestuurd vanuit de VPN server eh, hoewel, nee, ik denk andersom. Ik denk dat de VPN server de publieke key teruggestuurt eh, en vervolgens wordt er een eh, wordt mijn bericht, en dat is dus die eerste pijl, eh, met die publieke sleutel versleuteld, kan de VPN server het ontsleutelen, controleren en bericht teruggesturen met goh, het klopt. En ook dat bericht is dan waarschijnlijk versleuteld. Eh, en vanaf dan heb ik dus een eh, dezelfde beveiligde eh, eh, verbinding en heb ik mezelf geautoriseerd tegen die VPN server.

X: Oké. En welke verbinding is dan eh, versleuteld?

Y: Welke verbinding is versleuteld. Eh, uiteindelijk alle zou ik zeggen, behalve dan de verbindingen die ik niet heb ingetekend. Dus he, waar het echt gaat om hoi, ik wil VPN-verbinding opzetten eh, dat is goed ik heb deze certificaten, dat zijn niet versleutelde verbindingen.

X: Dus alle lijnen, deze en deze-

Y: O, ja, en deze die eh, deze hangt ervan af. Maar dat, ik denk dat die niet onder de VPN-verbinding valt. Eh dit is eh, als het ware van goh, ik maak verbinding naar een andere website en als die andere website eh, geen versleuteling behoeft. Laten we zeggen dat het een HTTP eh, eh, protocol voor nodig, benodigd heeft, dan hoeft die verbinding niet versleuteld te zijn. Maar dan is het verkeer van VPN server naar die website en terug niet versleuteld, maar het verkeer van VPN server naar mijn device weer wel.

X: Duidelijk, prima, dankjewel. Dan een andere vraag. Wat is de invloed van een VPN-verbinding op jouw computerbeveiliging?

Y: Invloed van een VPN-verbinding op mijn computerbeveiliging. Eh, ik zou zeggen dat het mijn eh, beveiliging vergroot. Eh, omdat eh, nou ja, eh, ja, hoe zeg je dat, eh. Kijk, als ik vanaf een VPN-verbinding, maak ik verbinding met die VPN server. En vanaf dan lijkt het alsof ik eh, niet meer mijn device gebruik, maar lijkt het alsof ik de VPN server alleen maar gebruik. Dus is, dus denkt eh, nou ja, het andere eind van dit laatste pijltje denkt van goh, eh, een VPN server maakt verbinding met mij, terwijl eigenlijk doe ik dat. Eh, dus in die zin is alles wat aan eh, aanvallers en aanvalsvectoren op dit lijntje zit, eh, ja, die zijn eigenlijk gevaarlijk voor die VPN server. Maar voor mijn device direct niet. Nou, ik denk dat als je die VPN server uiteindelijk weet te hacken, dan is mijn device ook niet meer helemaal veilig. Maar ik denk in eerste instantie he, dus het direct eh, eh, voordeel is dat mijn device zelf wat meer beveiligd is.

X: En daarmee bedoel je dan dat jouw device meer beveiligd is, omdat je uiteindelijk het doel niet jou ziet maar de VPN server.

Y: Correct.

X: Oké. En hoe ziet het uiteindelijke device dan de VPN server in plaats van jou?

Y: Eh, o, sorry, ik krijg even een rare melding in beeld. Eh, hoe ziet het uiteindelijke device, ja, die ziet hier dan achter he. Die, ja, die kan gewoon kijken welke IP-adressen hebben verbinding met mij. Eh, en eh, die zal niet mijn eigen eh, device zien, maar die zal de VPN servers eh, IP-adres zien. Dus, ja, die, die gaat mijn device nooit zien. Tenzij eh, hij op slinkse wijze die VPN server weet te hacken en ziet dat er een VPN-connectie vanuit mijn device is onder andere eh, en dan zou die wel mijn device kunnen zien. Maar ik denk dat dat een scenario is dat eh, dat buiten beschouwing dient te worden gelaten. Eh, want dan is die VPN server gewoon niet meer veilig.

X: Ja-

Y: En dan is het hek van de dam zeg maar.

X: Ja, oké. En je zei eerder dat een VPN er ook voor zorgt dat je niet naar bepaalde websites kan gaan-

Y: Ja, maar dat is dan ingeregeld op de VPN server, als daar eh, bepaalde websites geblacklist zijn, dan wordt dat op die manier geregeld. Maar het is niet zo dat omdat ik deze drie lijntjes heb dat ik dan daardoor niet bepaalde websites kan benaderen. Dat heeft puur en alleen configuratie te maken van die VPN server.

X: Prima. En stel je voor dat je op een andere fysieke locatie bent-

Y: Hmhm.

X: Heeft het dat invloed op de, deze tekening? Op jouw VPN-verbinding?

Y: Eh, volgens mij niet. Eh, ik- Wat ik zeg, je maakt verbinding met het Internet. Dat kun je eigenlijk vanaf overal doen. Eh, en dan kun je een, een verbinding aanmaken met een VPN server die ook overal op de wereld eh, staat. Eh, dus zodoende zou ik nu vanuit mijn huis in Nederland een VPN server in eh, nou noem eens een land, in [country] kunnen eh, zoeken. Eh, en, en, ja, dan kan ik vanuit daar verbinding maken met nou ja, wat vanuit [country] toegankelijk is. Eh, andersom kan ook. Ik denk ook dat ik vanuit [country] een VPN server, nou laat ik geen [country] zeggen, maar in eh, in [country] kan benaderen. Eh, en, en vice versa. En ja, vervolgens he, dat van die websites net dat moet je niet te letterlijk nemen he, want je kunt als websitehouder kun je natuurlijk ook zeggen van joh, ik wil geen verkeer toestaan vanuit IP-adressen vanuit [country]. Eh, dus tuurlijk kun je vanaf de VPN server kun je bepaalde websites blacklisten, maar je kunt als website kun je ook bepaalde IP-adressen blacklisten. Dus dat moet je altijd wel even meenemen. En andersom is ook het verhaal eh, misschien kan ik vanaf mijn persoonlijke device niet bij een bepaalde website eh, maar kan ik juist omdat ik met een VPN-verbinding connecteer eh, eh, kan ik wel weer bij bepaalde websites. Zowel intranet als eh, sorry- Zowel Internet als intranet.

X: Ja, oké. En als je dan bijvoorbeeld in een openbare ruimte zit zoals een café, maakt het dan nog uit?

Y: Hoe bedoel je? Wat maakt dan nog uit?

X: Of, ja, verandert er dan iets aan deze tekening bijvoorbeeld? Of heeft dat invloed op je VPN-verbinding?

Y: Nou ja, kijk, ik denk dat het voor de tekening op zich niets uitmaakt. Eh, maar, kijk, op zo een Internetcafé, daar heb je gewoon heel veel mensen die op hetzelfde netwerk zitten. Eh, dus, ja, ik zou er eigenlijk nog wat dingen tussen moeten tekenen wil het echt helemaal kloppen, maar daar is het whiteboard of te klein voor, of mijn teken skills zijn echt niet goed genoeg. Maar er zitten nog wat stappen tussen. Kijk, mijn device is op dit moment geconnecteerd met mijn eigen eh, eh, wifi-omgeving, met mijn eigen router. En in zo een Internetcafé, dan heb jij eigenlijk hetzelfde. Dan verbind je met zo een router op een Internetcafé. Eh, en is het maar de vraag of al dat verkeer binnen dat eh, ja, binnen het netwerk van het Internet beveiligd is of niet. Kijk, hier thuis geloof ik het wel, want ik ben de enige die het wachtwoord weet en noem maar op. Maar op zo een Internetcafé is het vaak wat anders, zitten veel mensen op hetzelfde netwerk, is het misschien wel of misschien niet een beveiligd netwerk. Eh, maar bovenal kan die eigenaar van die router of degene die die router heeft gehackt, whatever, die kan al het verkeer eh, heel zwart-wit gezegd, die kan het inzien. Eh, dus in dat geval is het wel handig als je zegt van nou, weet je eh, allemaal prima, dat mag die inzien, maar ik wil wel even een VPN-verbinding opzetten, want dan weet ik in ieder geval zeker dat eh, het verkeer vanaf die VPN server naar mijn device, dat is versleuteld. Want die versleuteling dat vindt plaats van device naar server en niet op router naar router zeg maar, of van firewall naar firewall, of eh, eigenlijk

de verbinding zelf eh, ja, die is versleuteld, maar niet omdat het een versleutelde verbinding is, maar omdat de versleuteling plaatsvindt op het device en VPN server.

X: Ja. Oké, duidelijk. Eh, even kijken. Dan een hele brede vraag. Met wat voor digitale dreigingen heb jij als [the professional services firm] medewerker op een normale dag te maken?

Y: Eh, voor zo ver ik zie heel weinig. Eh, dus laat ik mij daar dan ook op beperken, anders moet ik echt gaan gissen. Eh, ik denk dat de digitale dreigingen die voor ons het grootst zijn eh, de phishing mails zijn. Eh, ik werk zelf niet vanuit eh, publieke eh, netwerken. Het enige wat ik doe is een persoonlijke hotspot opzetten eh, [0:22:52: until 0:22:54 has been omitted] en dan zelf alsnog een VPN eh, connectie direct opzetten. Eh, dus daar zie ik eigenlijk weinig risico's verder, omdat ze al gemitigeerd worden door de maatregelen. Eh, een ander risico dat ik zie is ja, verlies van eigendommen zeg maar, dus dat ik mijn laptop ergens laat liggen, of mijn telefoon of eh, wat dan ook. Eh, denk dat dat wel de meest reële dreigingen zijn op dit moment eh, waar wij direct last van zouden kunnen hebben. En, en ik geloof best dat eh, dat er nog verschillende partijen zijn die het [the professional services firm] netwerk bijvoorbeeld proberen te hacken of aan te vallen. Al dan niet via phishing. Maar daar zie ik zelf niets van. Op de phishing mails na dan.

X: Ja. En heeft een VPN-verbinding invloed op deze dreigingen?

Y: Nou, op het laten liggen van eh, spullen niet. Eh, ik bedoel dat doe ik zelf en nou ja, dan raken we data kwijt. Eh, maar ja, met of zonder VPN is dat sowieso het geval. Eh, ik denk dat eh, ja, omdat ik dus eigenlijk nooit met publieke netwerken verbinding maak eh, anders dan mijn eigen wifi eh, denk ik dat dat risico door VPN eh, ja, met of zonder VPN er ook nauwelijks is. Eh, als ik [0:24:28 until 0:24:34 has been omitted], ja, dan heb je wel datzelfde risico ook wat je ook in het Internetcafé hebt, dus dat iemand gewoon mee zit te lezen op je, op je lijntje. Eh, ik weet niet of VPN daar nou eh, het grote verschil maakt. Eh, maar dat is meer, dat heeft meer te maken met de aard van de werkzaamheden die ik doe zeg maar. Eh, omdat dat over het algemeen toch al over een beveiligde connectie gaat. Dus ja, dan is het verkeer van mijn laptop naar eh, eh, [0:25:08 until 0:25:10 has been omitted] dat is eh, via een beveiligde eh, of een versleutelde eh, eh, verbinding. Het is anders als ik intern naar het [the professional services firm] netwerk wil vanaf een [0:25:21 until 0:25:21 has been omitted]. Maar daarvoor heb ik sowieso al een VPN-verbinding nodig, anders kan het niet.

X: Ja. En wat bedoel je ermee dat je over het algemeen al via een veilige verbinding werkt?

Y: Nou, eh, dat eh, de verbindingen die je legt die zijn vaak niet via een HTTP eh, verbinding maar een HTTPS-verbinding. Dus dan heb je al een versleutelde verbinding. We leggen geen FTP connectie, maar een SFTP of een FTPS verbinding. Eh, ja, zelfde heb je met telnet en SSH, telnet doen we niet, SSH wel, maar dat zijn allemaal al(0:26:03) direct al direct versleutelde verbindingen. Dus in die zin denk ik dat het eh, het risico beperkt is. Eh, en dat de VPN-verbinding eh, het risico wel enigszins zou kunnen mitigeren of nog meer mitigeren, maar eh, ja aan het eind van de rit, ja, zou het alleen denk ik echt een groot verschil maken eh, met zaken die van het [the professional services firm] intranet afkomen eh, naar eh, mijn device zeg maar. Maar wat ik zeg, daar heb je sowieso een VPN-verbinding voor nodig, omdat ik ja, het intranet zegt het al, het is een intern netwerk van [the professional services firm]. Daar kom ik vanaf het Internet niet bij.

X: Ja. Oké. En dan zeg je dat je een persoonlijke hotspot gebruikt-

Y: Ja.

X: Als je- In plaats van een publiek netwerk-

Y: Klopt.

X: Gebruik je op een persoonlijke hotspot ook nog steeds een VPN-verbinding?

Y: Ja.

X: Oké-

Y: Al is het dan- Als is het maar omdat ik dan met het intranet van [the professional services firm] verbinding kan maken.

X: Ja. En wat is het verschil tussen je persoonlijke hotspot en het publiek netwerk?

Y: Hele goede vraag. Durf ik niet te zeggen eh, en, en misschien dat ik daarom ook wel eh, een VPN altijd alsnog opzet. Better-

X: Oké. Sorry?

Y: Better safe than sorry zullen we maar zeggen.

X: Ja. Oké. En dan als we nadenken over de verschillende dreigingen die je net opnoemde. Wie of wat is de aanvaller die de dreiging veroorzaakt?

Y: Werkelijk geen idee. Ja, goed, ik zelf als ik mijn spullen laat liggen, maar wie er dan wat mee doet durf ik niet te zeggen. En eh, ja, wie [the professional services firm] aanvallen, ja, ik heb daar wel mijn ideeën bij, maar nee, dat kan ik beter niet zeggen, want dat zou echt gissen zijn. Dat zijn resultaten waar je voor je onderzoek niets mee kunt.

X: Oké. En ik ga toch vragen, wat voor ideeën heb jij erbij?

Y: Nou goh, laten we dan eens concurrenten noemen eh, klanten wellicht eh, misschien een eh, een verdwaalde student die is afgewezen op een stage of op een eh, op een baan eh, ik denk niet dat de grote eh, statelijke actoren nou, die misschien ook wel trouwens, ons willen hacken. Ik denk dat statelijke actoren voor hele gevoelige dossiers misschien ook nog wel wat willen doen. Eh, maar ja, de, de, eh, hoe zeg ik dat, je komt niet zomaar bij eh, de dossiers eh, waarbij staatsgeheimen stukken worden opgeslagen. Daarvoor heb je weer extra beveiligingsmaatregelen die helemaal losstaan van een VPN-verbinding.

X: Oké. En wat is de motivatie van een aanvaller?

Y: Ja eh, ik zou het, het gebruikelijke zeggen. Concurrentie eh, denk ik, omdat ze willen kijken wat [the professional services firm] doet. Hoe wij bepaalde stukken aanpakken, wat we hebben gezien, wat onze strategie is, ja, de verdwaalde student of de scriptkiddie uit wraak eh, omdat het leuk is, verveelt zich, kan van alles zijn, wilt gewoon wat vandalisme eh, doen, beetje gekkigheid. Eh, statelijke actoren omdat ze staatsgeheimen van andere eh, landen willen eh, ontdekken eh, of gewoon kijken waar zwakheden zijn binnen andere staten eh, criminele organisaties wellicht omdat er geld te halen valt eh, ja, het kan van alles zijn. Maar ik durf echt niet in te schatten hoe groot per actor de dreiging is.

X: Oké. En wat voor achtergrond heeft een aanvaller?

Y: Als in eh, studie of hoe bedoel je?

X: Ja, is er een soort basisniveau van kennis dat een aanvaller heeft?

Y: Eh, ja, weetje, het zal best wel iemand met een beetje technische affiniteit moeten zijn eh, wat ik al zeg, ik ben geen hacker eh, dus ik heb zelf niet de kunde om het te doen. Het is sowieso niet handig als ik het doe in mijn functie, maar toch. Eh, ik denk voor het meeste is wel wat technische achtergrond nodig en eh, ja, afhankelijk van eh, nou, hoe je omschreven wordt he, ben je de scriptkiddie of ben je de statelijke actor dan, dan is die bagage dat je meedraagt wat meer. Ik weet wel dat iedere type aanval eh, wordt steeds gemakkelijker om uit te voeren zeg maar. He, dus he, nou ja, waar het dertig jaar geleden onmogelijk was voor iemand op een zolderkamertje een DDoS aanval te doen eh, zou het er nu binnen vijf minuten kunnen initiëren. Zonder dat ik er de technische kennis ervoor heb. He, dus in die zin is de achtergrond die je nodig hebt, de technische achtergrond die je nodig hebt wordt wel steeds kleiner.

X: En waardoor is dat nu steeds kleiner?

Y: Eh, omdat die technieken eh, nou ja, door de komst van het Internet eigenlijk publiekelijk bekend raken eh, dan heb je nog het eh, het darknet of het darkweb eh, waar, waar ja, aanvallen te koop zijn. Dus ja, het is gewoon makkelijker om aan een aanval te komen zeg maar.

X: Oké. En verandert de soort aanvaller door een VPN-verbinding?

Y: Eh, verandert de soort aanvaller door een VPN-verbinding. Dus als ik een VPN-verbinding heb, dan heb ik andere aanvallers wanneer ik dat niet heb, is dat wat je vraagt?

X: Ja. Of eh, ja.

Y: Ja, weet ik niet. Eh, ik denk dat je de scriptkiddie misschien wat meer uitvlakt. He, dus de, de, de huis en tuin hacker zeg maar. Eh, aan de andere kant eh, zo een persoon kan ook gewoon op [social media platform] kijken wie bij [the professional services firm] werkt eh, op basis van onze syntax voor e-mailadressen, die echt bijzonder simpel is, kun je echt naar verschillende mensen een mailtje sturen en kun je op die manier alsnog eh, eh, malware verspreiden binnen het netwerk. En daar doet de VPN-verbinding verder niets aan. Dus ja, weet je, ik denk het niet eerlijk gezegd. Ik denk niet dat het veel verschil maakt.

X: Oké. Maar maakt de VPN-verbinding in zichzelf, heeft dat wel invloed op de soort aanvaller?

Y: Eh, ja, ik zit even te denken of ik je vraag dan goed begrijp. Ik denk van niet, tenzij je dus in een Internetcafé ofzo zit. Eh, of misschien zelfs [0:33:38 until 0:33:39 has been omitted]. Eh, kijk, je, je verkleint

wel je, je exposure zeg maar. He, als je in een Internetcafé zit, dan is iedereen in dat Internetcafé is een mogelijke aanvaller, want iedereen zou in theorie met wat technische kennis mee kunnen kijken in jouw eh, verkeer als jij eh, geen versleutelde verbinding eh, gebruikt. Eh, en zet jij een VPN-verbinding op, ja, dan heb jij die exposure niet. Eh, he, maar dat ja, dat is dan ook het enige wat je er mee wint.

X: Minder exposure. Oké.

Y: Ja.

X: En wat zou de impact van een aanval kunnen zijn?

Y: Als ik een VPN-verbinding gebruik of niet?

X: Ja, of niet inderdaad.

Y: Ja-

X: Impact voor [the professional services firm] dan.

Y: Eh, de impact voor [the professional services firm], nou, dat zou kunnen zijn dat eh, dat er malware eh, binnen het netwerk wordt geïnstalleerd en dat kan dan weer leiden tot eh, tot downtime, dat kan leiden tot eh, eh, lekken van dossiers of persoonlijke data, dat kan leiden tot financiële eh, schade, dat kan leiden tot reputatieschade. Wat, wat langer doordreunt dan die eenmalige afkoopsom zeg maar. Eh, ja, ik denk dat eh, ja, de impact die kan echt verschillend zijn. En die kan afhankelijk van wat de aanval is kan die bijzonder groot zijn en kan eh, kan ook best wel eens wat meevallen.

X: Ja. Oké. En als we nu naar de VPN-verbinding zelf kijken, hoe veilig is een VPN-verbinding?

Y: Ja, die is net zo veilig als het eh, het algoritme dat gebruikt wordt om de verbinding te beveiligen.

X: Oké. En zijn er andere manieren waarop een VPN mogelijk niet veilig is? Of onveiliger?

Y: Eh, nou, wat ik al zei. Als je VPN server gecompromitteerd is dan heeft het weinig zin om zo een VPN-verbinding op te zetten, omdat je dan in de illusie leeft dat het een veilige verbinding is. Want uiteindelijk heb je alsnog een, ja, iemand die gewoon meekijkt in je verkeer. Eh, ik zit te denken van ja, als je eigen device ook gecompromitteerd is of niet ook, maar als je eigen device gecompromitteerd is, dan heeft het ook al weinig zin meer om, om een VPN-verbinding op te zetten, omdat je vanuit je eigen device dan het onversleutelde verkeer of al het binnenkomende verkeer onversleuteld alsnog kunt laten doorsluizen naar eh, iemand anders.

X: Oké. En kan je nog meer van dit soort voorbeelden bedenken?

Y: Wanneer is een VPN-verbinding nog meer niet meer veilig. Eh, nee, ik denk dat dit het eh, wel is. We kijken altijd alles redelijk simpel, he. Eh, een verbinding opzetten doe je tussen een initiator, in dit geval mijn device, als dat niet meer veilig is dan is het niet meer veilig. Je zet hem op met een doel, dat is de VPN server, als die niet veilig is, dan is ook niks meer veilig en als de verbinding niet veilig is, wat er tussenin zit, dan is het ook niet meer veilig. Dus eigenlijk heb je drie zaken waarop het mis kan gaan. Eh, en volgens mij is dat het.

X: Oké. Duidelijk. Even kijken. Eh, dan waren dit tot zo ver mijn vragen. Zijn er nu nog dingen eh, van VPN, die niet naar voren zijn gekomen?

Y: Eh, nou, nee, ik denk dat- VPN is een toepassing, een maatregel eh, maar ik denk dat het samenspel van maatregelen altijd ertoe leidt dat iets wel of niet veilig is. He, kijk, alleen een VPN-verbinding eh, nou, dat kan veilig zijn, maar wat ik al zeg, er hoeft maar een van die drie puzzelstukjes zeg maar, niet goed te zijn en, en je hebt er al niet zo veel meer aan. Eh, dus het gaat er altijd om welke maatregelen zijn er nou nog meer om eventuele restrisico's ook te mitigeren. En ik denk dat dat eh, met name van belang is. En ja, dat, dat is misschien het laatste wat ik erover kwijt wil zijn.

X: Ja, en dan zeg je restrisico's, bedoel je dan de risico's die overblijven na een VPN-verbinding al?

Y: Eh, ja, of, of risico's dat eh, op het moment dat eh, he, het is een maatregel en als die maatregel niet meer goed is, ja, dan wil je niet dat je direct eh, bloot wordt gesteld aan het volledige risico dat die maatregel eh, beoogt af te dekken eh, dus daarom is dat goed om nou ja, in de ... zeggen joh, per risico minstens twee maatregelen, ik denk dat het in cybersecurity niet per se opgaat en dat je nog meer maatregelen hebt. Maar in ieder geval iets wat preventief werkt nou, dat is een VPN-verbinding, maar ook in ieder geval wat detectief of reactief werkt, dat op het moment dat er iets niet goed gaat, dat het in ieder geval gesignaleerd kan worden en dat daar direct op geacteerd kan worden. Eh, en daarnaast, maar goed, dat is dan op het moment dat eh, dat als er sowieso een VPN-verbinding is, want wat ik al aangaf, een VPN-

verbinding op zich is niet zalmakend voor alle risico's eh, zou je ook nog andere maatregelen moeten nemen.

X: Oké. Duidelijk. Zijn er verder nog dingen over VPN-verbindingen die niet naar voren zijn gekomen?

Y: Volgens mij niet.



Figure C.10.1: Drawing 10_1

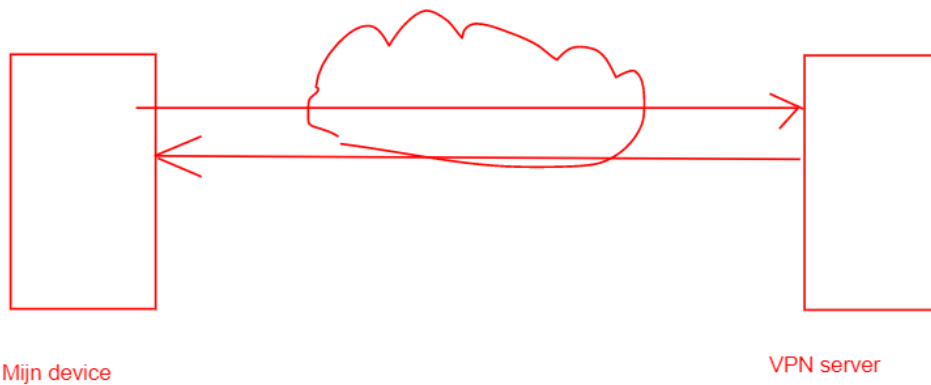


Figure C.10.2: Drawing 10_2

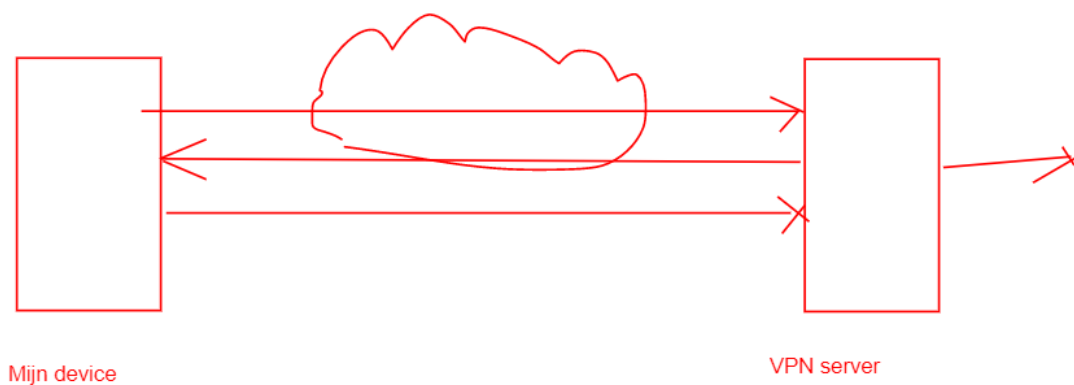


Figure C.10.3: Drawing 10_3

C.11: Transcript Expert 11

Duration: 51 minutes

Language: Dutch

Number of drawings: 8

X: Dan de eerste vraag van het interview. Kan je mij vertellen wat een VPN is?

Y: VPN, of Virtual Private Network, is een eh, eh, een verbinding waarmee je met een eh, eh, een enduser of een enddevice, net hoe je het wilt noemen natuurlijk eh, over he, ze zeggen over een beveiligde verbinding toegang maakt tot het netwerk. Dat kan een bedrijfsnetwerk zijn of bijvoorbeeld het netwerk van een webapplicatie. Eh, in ieder geval dat.

X: Oké. En je zegt dat de verbinding beveiligd is-

Y: Ja.

X: Op wat voor manier is deze verbinding beveiligd?

Y: Ik neem dat het altijd gaat over een eh, eh, gebruik maken van versleuteling van eh, van de communicatie en dat die communicatie versleuteld is op een eh, asynchrone manier, dus door middel van een eh, eh, private key of public key infrastructure. Dat is mijn aanname, maar dat- Dat is een aanname, ja. Ik neem aan dat het over een PKI gaat.

X: Oké-

Y: Versleuteld. Ja.

X: En waarvoor gebruik jij de VPN?

Y: Eh, de VPN dat he, je refereerde aan het begin van het interview naar het gebruik van VPN binnen [the professional services firm], dus in dit geval zou de VPN zou dan zijn om van mijn thuiscomputer of vanuit mijn thuisnetwerkverbinding te maken met het [the professional services firm] netwerk, zodat ik bijvoorbeeld bepaalde zaken kan benaderen die alleen maar werken als je op het lokale netwerk zou zitten of via de VPN-verbinding maakt met het lokale netwerk.

X: Zijn er nog andere redenen waarom jij VPN gebruikt?

Y: Binnen [the professional services firm] of?

X: Ja.

Y: Persoonlijk. O, binnen [the professional services firm] zou dat zeg maar verbinding met het eigen netwerk eh, ja, dus verbinding maken met toepassingen die daarvoor geschikt zijn. Eh, op die manier. Eh, dat zijn de enige redenen, het [the professional services firm] netwerk zelf geeft me niet het gevoel nou dat ik nou zeg maar anoniem op het Internet browse. Integendeel, het is natuurlijk het bedrijfsnetwerk, dus nee. Puur voor verbinding maken met het netwerk, zodat ik toegang heb tot de shares en de applicaties die alleen werken met die verbinding.

X: Ja, duidelijk. En je noemt wel anoniem browsen-

Y: Hmhm.

X: Hoe werkt dat?

Y: Ja, het hele idee natuurlijk he, van een VPN is dat je verbindt met een ander netwerk. Nou, vanuit dat andere netwerk kan je verschillende dingen doen. Net alsof je op een fysiek netwerk aangesloten bent. En een van die dingen die je kan doen is natuurlijk weer verbindingen opzetten naar anderen netwerken. Stel dat je bijvoorbeeld browsed naar een website. Nou ja, als je nou persoonlijk gebruik maakt of eh, ja, vanuit je werk kan natuurlijk ook eh, van een VPN, dus ook bijvoorbeeld een webserver die communicatie maakt met een he, een apparaat dat dan vanuit die VPN een verbinding maakt, dat is natuurlijk wel een voorwaarde. He, dat de verbinding ook opgesteld wordt vanuit het netwerk van de VPN. En die ziet dan enkel als eh, als zender eh, dat netwerk van de VPN en niet het netwerk waar je misschien zelf in zit. Nou ja, op die manier eh, heb je een soort van eh, geanonimiseerde verbinding als in eh, men praat tegen die VPN aan en weet eigenlijk niet eh, wat jouw thuisnetwerk is. Nou als je het natuurlijk een paar keer achter elkaar doet he, dan krijg je een onion of een tor netwerk en ja dan, dan weet men eigenlijk niet wie nou het endpoint is. He, dus op die manier kan bijvoorbeeld een webserver, weet wel met welk netwerk die praat, maar dat is niet het netwerk waar jij zit. Dus op die manier weet die minder waar je vandaan komt en nou ja, dan kan je natuurlijk bijvoorbeeld bedenken aan dat de grote landen IP-reeksen toch wel vaak in brokken zijn uitgedeeld, dus daarmee kan je best wel wat informatie over wij hebben ... daar gaat het voornamelijk om eh, waar jij bent, ja, ontnemen van iemand. En bijvoorbeeld correlaties van andere logs die je achterhaald.

X: Ja, en-

Y: Daarvoor kan ik het [the professional services firm] netwerk niet gebruiken hoor, want aangezien al het netwerk natuurlijk gemonitord wordt, is het voor mij in dat geval alleen maar juist vervelender, maar het is een mogelijkheid.

X: En hoe bedoel je dat dat vervelender is?

Y: Nou ja, stel nou dat ik he, op het Internet dingen wil doen waarvan ik eh, zou verwachten van het is beter dat men niet weet wie ik ben, dan zal het in dat geval ook waarschijnlijk niet beter zijn dat mijn eh, bedrijf he, waar ik werk, weet dat ik die dingen doe. Dus in dat geval zou ik de [the professional services firm] VPN nooit gebruiken.

X: En hoe zouden zij dan weten wat jij doet?

Y: Nou ja, de netwerkstromen die eh, he, ik weet natuurlijk niet precies hoe het bij [the professional services firm] ingericht is, maar er vindt ook gewoon verkeeranalyse plaats, en dat is zeer zeker wel eh, natuurlijk gelinkt aan he, wie achter hun verbinding zit. Want [the professional services firm] beheert natuurlijk uiteindelijk eh, het apparaat waar ik op werk. Dus als ik voor een reden anoniem moet blijven, dan kan ik dat beter natuurlijk niet doen via het netwerk van het bedrijf waar ik werk.

X: Ja, oké. En welke handelingen voer jij uit als een gebruiker om een VPN-verbinding te maken?

Y: Eh, nou, vanuit [the professional services firm] is het zo ingericht dat natuurlijk de VPN-adapter geheel geconfigureerd is, dus de software eh, die eh, weet met wie die moet communiceren, tegen wie het, he, het endpoint toe moet gaan, is allemaal geconfigureerd. Het enige dat aan mij wordt gevraagd is mijn wachtwoord in te voeren, dus eh, binnen het netwerksegment van de omgeving klik ik op connect to this he, tot dit netwerk, dan krijg ik een pop-up veld en dan wordt mij gevraagd om eh, met twee-factor authenticatie in te loggen eh, en een gedeelte daarvan is een eigen persoonlijke identificatienummer en het tweede is een eh, een tweede factor, in dit geval een apparaat he, dat ik heb, mijn telefoon, en die geeft mijn code via door middel van de [access token provider] app die erop staat. En dan samen dat eh, dan worden mijn credentials gecheckt en als dat klopt, dan wordt de verbinding opengezet.

X: Oké. En je zei dat het endpoint geconfigureerd is, wat bedoel je hiermee?

Y: Eh, ja, wat ik ermee bedoel is he, stel nou dat ik moet natuurlijk he, de VPN, als je het zo zou kunnen noemen, weet natuurlijk niet waar het de verbinding mee op moet zetten, dus de gegevens die nodig zijn eh, en ik denk dan he, dat het dus in de configuratie opgesteld is met oké he, verbind naar, ik noem maar wat, naar deze server, en voor ons staat volgens mij alles in [country] he, en daarop he, weet die server, als er verzoeken komen en ik neem aan, maar dat weet ik niet zeker, van he, dit apparaat, in mijn geval zal het waarschijnlijk een MAC-adres zijn of misschien nog wel op basis van andere gegevens, zoals mijn AD-account, mijn AD eh, gegevens, weet die van oké, he, bij een verzoek van deze verbinding hoort ook eh, deze credentials. He, want ook zij moeten natuurlijk controleren dat de hash die, of in ieder geval de wachtwoordgegevens die binnen komen, correct zijn. Dus ik denk dat dat met het configureren is. Dus zeg maar dat de verbinding die opgesteld wordt, ja, moet men weten waar naartoe, je kan geen lege envelop sturen. Of eh, je kan geen envelop sturen zonder eh, adresgegevens erop.

X: Ja. En hoe wordt bepaald waar het uiteindelijk naar toe wordt gestuurd?

Y: Hoe bedoel je?

X: Eh, je zegt adresgegevens-

Y: Ja, ja, dus in he, eh, he, ik wil een verbinding opzetten, ik doe dus een verzoek ergens over het Internet he, dat ik wil gaan verbinden met het netwerk en daarvoor moet ik ergens over het Internet ... die verbinding maken, maar die verbinding moet ook weten dat ik die verbinding mag maken en welke gegevens zij nodig hebben. Dus in die configuratie eh, zal waarschijnlijk staan he, naar welk adres dat verzoek toe staat, dat is wat ik bedoel met de adresgegevens op de envelop.

X: Ja. En dan zei je voor wat je nodig hebt om je verbinding te maken-

Y: Ja.

X: Dat je je persoonlijke code hebt en daarnaast een code op je mobiel-

Y: Ja.

X: Zijn hier nog andere mogelijkheden voor, voor deze andere code?

Y: Eh, even kijken, voor zo ver ik weet bij ons niet. Eh, he, je zit of op het netwerk natuurlijk he, dan ben je fysiek aangesloten of he, fysiek als in eh, je zit op het eh, het bedrijfsnetwerk of je logt inderdaad in door

middel van de VPN en dan voor zo ver ik weet moet dat altijd gaan via de twee-factor authenticatie. We hadden daar vroeger een eh, [access token provider] token voor, maar als het goed is worden die nergens meer gebruikt.

X: Oké. En op welke apparaten gebruik jij je VPN?

Y: Eh, ik gebruik mijn eh, de VPN waar wij het nu over hebben, zeg maar [access token provider] token(0:10:09) en geldt puur voor mijn laptop.

X: Oké. Gebruik je het nog op andere apparaten?

Y: Nou, we hebben, het schijnt dat we sinds kort een mogelijkheid hebben om met onze telefoon ook op een gedeelte van het bedrijfsnetwerk te komen en dan bepaalde webpagina's, maar a het is mij nog niet gelukt het werkend te krijgen en b dat zal via een andere manier ingesteld zijn dan dit. Dus ik denk alleen op eh, dit ik houd het op alleen de laptop.

X: Oké. En kun je aan mij uitleggen hoe een VPN-verbinding werkt? En hiervoor kan je het whiteboard gebruiken-

Y: Hmhm.

X: Ik zal mijn tekeningen weghalen.

Y: Ja, even kijken hoor. [\[start drawing 11_1\]](#). Even kijken, we hebben in ieder geval een paar toren he, en dat is in ieder geval- En onderaan, dan zeg ik even dat dit ... zit. Dus dan zeg maar, he, de user, noem het even de user, hoe, ja, dan tekenen we het gewoon erin, ook goed. O, wacht, zo moet dat, kijk, zo, he, he, user. Ook fijn dat er zo een lange periode tussen zit met transcriberen zo meteen, waarvoor dank. Eh, user, dus we hebben een user he, die zet een verbinding op naar een bepaald adres, he, dat zou dan de, nou ja, ik noem het nu even de VPN-ontvanger zijn. Eh, ik weet niet of dat de juiste terminologie is, maar in ieder geval die zet een verbinding op naar dat adres en die stuurt mee eh, bepaalde gegevens he, eh, en een gedeelte daarvan, dat zijn dan die wachtwoord, het wachtwoord plus dan dat token en dat zal waarschijnlijk in een hash eindigen. He, dus we zeggen hier dat er een hash meegaat, o, wacht, hij staat nu op, zo, even kijken, even kijken hoe die tool precies werkt hoor, zo. He, die stuurt dan die hash mee, kan ik beter niet zo doen, o, he, he, nou, geen enkel probleem. Hup, we weten nu wat we moeten doen. User, zal vast niet de eerste zijn die hem helemaal kapot maakt.

X: Nee, het gebeurt een enkele keer inderdaad.

Y: Ja, precies. Dan we noemen het even he, de VPN-ontvanger, maar ik heb geen idee wat de daadwerkelijke terminologie is. Zo, gaan we eerst een verbinding opzetten. Dus ik heb he, met mij is geconfigureerd he, naar wie ik iets moet sturen. Anders, ja, ik kan natuurlijk niet ... iets sturen. Zo, zetten we een lijntje op zo, wat daaruit komt he, dus we sturen de gegevens mee die nodig zijn eh, he, om te verifiëren dat ik ik ben en dat ik überhaupt mag inloggen, dus in dit geval zal dat usergegevens zijn. Plus dan he, het password. En he, laten we ervan uitgaan dat is een hash. Kan ik dit nog groter maken, nee, jij misschien wel later in je tekening, in ieder geval je weet dat het er staat. Nou, he, die gegevens die komen daaraan en dat wordt gecontroleerd he, dus zij eh, hebben een manier om te controleren van he, de hash klopt met de hash die zij kunnen genereren. Eh, nou ja, en als dat allemaal goed is dan wordt mij toegang verleend. Nou he, dan zorgt de VPN-ontvanger, of de VPN-ontvanger staat misschien al in een netwerk, van het netwerk waar ik naartoe wil verbinden. Laten we daar op dit moment even vanuit gaan dat dat gewoon een gedeelte van het segment is. Die zegt dat klopt, die verbinding mag worden opgesteld. He, die stuurt dus weer de gegevens terug die nodig is om onze eigen communicatie eh, eh, te versleutelen. [\[start drawing 11_2\]](#). Ja, als dat allemaal werkt, dan ja, heb ik feitelijk, o, wacht, verkeerde, toegang tot het netwerk. He, laten we zeggen, laten we dit even [the professional services firm] noemen, tekst, [the professional services firm] netwerk, en nou, om toegang tot dat netwerk te bereiken eh, voor of over bepaalde protocollen of voor bepaalde services of diensten. He, het hoeft natuurlijk niet per se zo te zijn dat voor alle verbindingen die ik straks naar buiten open stel dat die altijd via het [the professional services firm] netwerk gaan. Dus om een voorbeeld te noemen, mijn [e-mail] gegevens he, hoeven niet per se over het, over de VPN te gaan he, dus als ik browse op Internet of een verbinding op stel, dan bepaalt mijn computer ten eerste oké, mag het naar de VPN toe of niet of gaat het over de VPN of niet en alle gegevens die erover gaan die gaan erover en alle gegevens die er niet over gaan, die gaan gewoon via het netwerk waar ik dan daaronder verbonden ben, in dit geval gewoon mijn thuisnetwerk. Nou ja, en dat blijft gewoon gaan tot een sessie termineert.

X: Oké. Eh, dus in dit geval in deze tekening staat de VPN-ontvanger in het [the professional services firm] netwerk.

Y: Ja, maar, ja, maar ik zal je niet durven te zeggen, het zou ook kunnen zijn dat die eh, in ons geval ergens anders staat en zeg maar alleen maar als een soort van PKI eh, fungeert om te zeggen oké he, hij mag die verbinding opstellen en zet de verbinding op, dat weet ik echt niet. Ik weet niet of we dat op die manier intern hebben of niet. En dit is allemaal natuurlijk wel gesegmenteerd he, dat is wel natuurlijk sowieso zo.

X: Wat bedoel je daarmee, dat het gesegmenteerd is?

Y: Nou ja, he, eh, dus het is sowieso een eigen eh, virtueel netwerk binnen dan wat van [the professional services firm] is. He, de VPN-ontvanger zal natuurlijk nooit op die manier vrije verbindingen naar het gehele netwerk open kunnen stellen, maar er alleen voor kunnen zorgen dat ik verbinding kan maken met het netwerk of gedeeltes van het netwerk. Zoals dat met een normale verbinding ook zal gelden.

X: Oké. En je noemde kort even protocollen in het verhaal-

Y: Hmhm.

X: Wat is de rol van een protocol?

Y: Ja. De protocollen he, eh, of in dit geval ook services, en dan denk ik van hoe het geconfigureerd is he, dus de manieren waarop de verbindingen en de diensten voor die verbinding gebruikt kunnen worden. Eh, over een in dit geval, over een eh, over een netwerk of over een verbinding. En het kan heel goed zijn dat je bijvoorbeeld een VPN hebt die jou eh, toegang geeft tot het netwerk of tot een segment van het netwerk, maar alleen maar voor het uitvoeren van bepaalde diensten of voor verkeer over bepaalde eh, protocollen. He, en het meest gemakkelijke geval zal men bijvoorbeeld die als onveilig beschouwd worden niet accepteren, dat een, of eigenlijk biedt die niet aan. Maar voornamelijk voor diensten kan het heel goed zijn dat bepaalde diensten eh, misschien helemaal niet over het VPN gaan, dus ook niet over het netwerk gaan. He, dat, dat, kan ik weten, ik heb echt geen idee hoe dat bij ons van toepassing is. En ik weet bijvoorbeeld dat voorheen het voor eh, ons mailverkeer het noodzakelijk was om verbinding te maken met het [the professional services firm] netwerk, en dat tegenwoordig niet meer zo is. Dus ik neem daarmee ook aan dat eh, zeg maar het mailverkeer, [e-mail] is dat volgens mij, dat weet ik niet zeker, dat dat niet meer over een VPN loopt en ook niet meer over een VPN dus hoeft te lopen. Zoals als je de VPN-verbinding hebt en je stuurt een mail en hij is er op die manier uitgesloopt, dan zal die mail ook niet over de VPN lopen in dat geval.

X: Ja. En als die mail niet over VPN loopt, hoe gaat het dan naar je toe?

Y: Dan loopt het gewoon over mijn eigen netwerk. Dus als we hier ergens het Internet zouden kunnen tekenen. [\[start drawing 11_3\]](#). He, dus ik zit he, de user zit ook in dit geval in zijn eigen netwerk, zo. Hij, mijn teken skills zijn niet de allerbeste, zoals je waarschijnlijk al ziet. Maar he, usernetwerk, nou ja, en mijn mail, waar die voorheen dus waarschijnlijk eerst naar het [the professional services firm] netwerk ging en daar dan een mailserver stond en dan he, verder naar destination toe ging, gaat het nu naar de mailserver en die kan of in het [the professional services firm] netwerk liggen of eh, wat mijn vermoeden is bij [example of softwareprovider], aangezien we [an internal page] hebben. [\[start drawing 11_4\]](#). Zo he, en dan voor de eenvoudigheid gewoon o, wacht, eerst even noteren. He, dus als ik die verbinding op moet stellen, dan zal die ongeacht of VPN aanstaat of niet, naar die mailserver toegaan, die ja, eigenlijk niets met eh, de VPN te maken heeft. En dan ja, naar de bestemming whatsoever.

X: Oké. En als deze VPN-ontvanger niet in het [the professional services firm] netwerk zit, hoe ziet dat er dan uit?

Y: Stel dat die niet in [the professional services firm] he, er zijn een paar dingen, maar he, dus voor mij, op die manier kom ik niet echt veel mee in aanraking mee. Eh, he, maar netwerk technisch gezien zou ik denken dat het mogelijk zou zijn dat je bijvoorbeeld echt een VPN hebt die geheel extern is, he. Die zal dan twee dingen kunnen doen. Ik kan het niet wegnemen he, dit of wel, met het handje misschien, kijken, nee. Oké. Was te proberen. [\[start drawing 11_5\]](#). Eh, dan zou je bijvoorbeeld wat zou kunnen zijn, maar ik weet niet of dat bestaat of dat het werkt, dat je een dienst hebt die gewoon puur hier eh, verifieerd of nou deze user deze user is en deze user nou die verbinding wel mag stellen. En he, indien dat zo is eh, die verbinding doorzet. He, zeg maar een soort van handshake verricht. En sommige partijen die het bijvoorbeeld ook doen voor authenticatie met eh, overheden eh, wat ook heel misschien zou kunnen zijn, maar dat weet ik

ook niet zeker, of misschien is dat wel gebruikelijk, maar eh, dat je ook zo een partij hebt die controleert dat, die verifieert dat he, die voorziet misschien van de credentials. En met die credentials kan ik dan direct zeg maar contact opnemen met het netwerk en dan gewoon het normale netwerkverkeer eh, employen. Maar dat is voor mij gewoon een beetje gokken hoor, ik heb geen idee waar de VPN host, als je hem zo zou kunnen noemen, specifiek staat. Of het in het netwerk moet staan of niet.

X: Ja. En je had het eerder over versleuteling-

Y: Ja.

X: Welke van deze verbindingen zijn versleuteld?

Y: Nou ja he, wat natuurlijk in dit geval he, eh, van alles wat, kijk, verbinding met de VPN dus nadat de VPN sessie is opgesteld he, zijn inherent versleuteld. Dat is het hele idee natuurlijk van het private, van het gedeelte en virtueel staat natuurlijk voor het feit dat je niet daadwerkelijk verbonden bent met het netwerk via een kabel. Eh, he, dus de eerste uitwisseling kan gaan op een op, op, een type versleuteling, maar zal waarschijnlijk enkel gebruikt worden voor het overeenkomen eh, eh, van hoe er versleuteld gaat worden. He, dat je een pre-key gaat definiëren. Eh, daarna zal al het verkeer, nou ja, het hangt ervan af eh, he, als de VPN inderdaad in het netwerk staat dan zal al dat verkeer versleuteld blijven, in het geval eh, dat de VPN verbinding alleen maar wordt gebruikt als een hub, dan blijft dat ook gewoon heen en weer versleuteld hier, en in het geval dat er alleen maar voor wordt gezorgd dat mijn credentials kloppen en dat er zeg maar via een externe partij of een externe host de verbindingen opgezet worden, dan zal daarna al dit verkeer versleuteld lopen. En met [example of software provider] neem ik ook aan dat het versleuteld loopt, maar ja, dat is buiten de, buiten de scope van het onderzoek. Eh, het hele idee natuurlijk van VPN zelf is om versleuteld verkeer mogelijk te maken. Ten minste, verkeer mogelijk te maken tussen netwerken en nou ja, dat moet gewoon versleuteld zijn. Zou wel heel slecht zijn als dat niet versleuteld is, zou vast mogelijk zijn natuurlijk, maar, binnen [the professional services firm] denk ik niet, maar zeg maar in de rest van de wereld. Eh, ja, het idee is natuurlijk dat je op een beveiligde manier versleuteld bent, omdat je niet weet wie het is.

X: En voor deze tekening maakt het nog uit op welke locatie jij bent?

Y: Eh, nou ja, laten we eens naar het beginscenario toegaan. Dus he, dus maakt eigenlijk voor deze tekening maakt het voor de user niet uit of die nou in het usernetwerk zit of in een, weet ik veel, best friend netwerk als je het zo zou kunnen noemen, of een ander netwerk. Het kan wel zijn, maar he, he, dan gaan we weer even terug naar de scope voor het [the professional services firm] netwerk, maakt het volgens mij niet uit uit welk netwerk het verzoek komt. Dus het maakt niet uit in welk netwerk het userapparaat zich bevindt. He, maar het kan wel voor, ik kan me heel goed voorstellen dat je ook met whitelisting natuurlijk kan werken en kan zeggen ik wil alleen maar mensen, apparaten met deze gegevens correct, die correct aansluiten, die ook uit het netwerk komen. Maar dat is voor [the professional services firm] niet geldig, in ieder geval niet geldig op een manier dat ik alleen maar vanuit mijn huisnetwerk, thuisnetwerk een verbinding op kan zetten. Dat is niet zo.

X: Oké. En stel je voor dat je op een andere locatie bent, in dit geval bijvoorbeeld een café-

Y: Hmhm.

X: Verandert er dan iets aan deze tekening?

Y: Nee.

X: Oké.

Y: Nee.

X: Duidelijk. En dan een andere vraag. Wat is de invloed van een VPN-verbinding op jouw computerbeveiliging?

Y: Definieer computerbeveiliging.

X: In een hele brede manier. Heeft VPN invloed op jouw computerbeveiliging?

Y: Eh, nou ja, eh, stel dat ik eh, hangt eraf, laten we even de makkelijke aanname nemen dat de aanname is dat al het verkeer als ik een VPN-verbinding heb, al het verkeer via de VPN gaat. Dus eh, verbindingen naar mij toe of verbindingen van mij af die ik opzet, komen altijd van het VPN-netwerk af. In dat geval, he, omdat het VPN-netwerk natuurlijk beschikt over meer beveiligingsmaatregelen dan ik thuis he, denk dan aan geavanceerde firewall, denk aan eh, analyse, de IDS en IPS, voegt dat toe aan de beveiliging van mijn

netwerkverkeer. Eh, maar dat maakt het zeg maar niet onmogelijk ofzo om virussen op te lopen. Misschien moeilijker omdat er packetinspection kan plaatsvinden op de verbindingen die dan via de VPN via het [the professional services firm] netwerk naar buiten gaan, wat misschien niet beveiligd is. Eh, dus ja, het voegt zeker he, in het breedste zin van het woord, voegt het eh, iets toe, positiefs, aan de beveiligingsaspecten van mijn werklaptop.

X: Oké. En je noemde even kort een firewall, waar in deze tekening zouden we een firewall kunnen vinden?

Y: Nou ja, he, het zal eerst bij het usernetwerk zijn in dit geval. [\[start drawing 11_6\]](#). Dus dat kunnen we ook wel tekenen hierzo bij het usernetwerk he, want de meest elementaire firewall namelijk zit gewoon bij mij in de router met vastgestelde zaken van de IPS. Dan zal de he, de VPN-ontvanger zit natuurlijk in het [the professional services firm] netwerk en alle verbindingen uit het [the professional services firm] netwerk gaan ook over een firewall heen, zou hier zitten. En alle verbindingen die naar buiten gaan, gaan waarschijnlijk ook over dezelfde firewall. Of in ieder geval over hetzelfde firewallsegment heen. En eh, nou ja, dat geldt natuurlijk indien hier een derde partij is, als hier een derde partij is he, alles wat in het netwerk zit in dit geval zal achter een firewall zitten.

X: Oké-

Y: Of een vorm van firewall, he, ja.

X: Zijn er nog meer manieren waarop een VPN invloed heeft op jouw computerbeveiliging?

Y: Even kijken, mijn communicatie is versleuteld he, dus zeg maar man in the middle, dus waar je enerzijds op doelt, iemand die tussen zit zou niet met mij kunnen meelezen. Eh, enerzijds is verkeer dat enerzijds loopt he, naar anderen toe. [\[start drawing 11_7\]](#). Dus stel dat hier weer een andere webserver is he, dat, teken even heel lelijk dat het via [the professional services firm] netwerk gaat. Ja, he, en dit is niet versleuteld bijvoorbeeld he, en dat zet ik hier de maatregelen die wij gesteld heb, stel aan blacklisting eh, eh, verkeeranalyse, ook allemaal gelden voor eh, die verbinding. [\[start drawing 11_8\]](#). Terwijl als ik hem misschien zelf direct doe, dat niet zou gelden. Dus dat voegt op die manier toe, ja.

X: Oké. En je zegt verkeeranalyse, maar ook dat het netwerk versleuteld is, hoe hangt dat samen?

Y: Sorry, ik verstond het eerste gedeelte van je vraag niet. Kan je dat herhalen?

X: Ja, je noemde verkeermonitoring-

Y: Ja.

X: En ook versleuteling, hoe hangt dat samen?

Y: Ja. Eh, he, het zijn natuurlijk- Kijk, stel dat ik hier een verbinding met het netwerk opzet en dat verkeer is versleuteld he, dan moet het op een gegeven moment ergens ontsleuteld worden, want anders weet men niet he, wat er moet gebeuren. Stel dat ik hier tegen een webserver aan loop te praten en die krijgt alleen maar voor hem zeg maar gibberish binnen, ja, dan weet die natuurlijk niet welke zaken er eh, moeten plaatsvinden. Dus dat moet je ergens gaan eh, ontsleutelen he, offloading. Eh, he, op het moment dat je het offload, betekent dat alles in te zien is. Eh, betekent ook dat je analyse kan uitoefenen op dat verkeer, he, dat gaat geautomatiseerd. Dus dat gaat met apparaten en met software he, die analyseert wat voor dingen er gevraagd worden, wat eroverheen loopt eh, waar de verbindingen naar toe gaan. Eh, he, en dat doet het op verschillende manieren. Wat natuurlijk ook nog kan, he, er was vroeger een bedrijf van, dat is failliet gegaan helaas, dat analyseerde bijvoorbeeld hoeveel verbindingen erop werden gesteld en hoeveel foutmeldingen er kwamen eh, naar DNS-verzoeken, die ja, eerst niet werkten. En het idee erachter was dus dat als men bijvoorbeeld eh, een grote eh, DDoS aanval wilde gaan raadplegen, moet je dus eerst allerlei apparaten infecteren en je wil eh, he, die aansturen, dus een soort van command and control center gaan bouwen. En je wilt ervoor gaan zorgen dat die op een gegeven moment natuurlijk actief worden, maar niet allemaal gelijktijdig, want dat valt op, of in ieder geval niet allemaal buiten moment van infectie, want dan heb je niet een groot genoeg kritische massa. Dus wat deden die apparaten, die zaten in het netwerk, of dat kon je laten implementeren eh, die zochten nou vaak nou ineens eh, eh, niet bekende of bijna niet bestaande eh, DNS-verzoeken kwamen naar eh, webserver en als dat heel vaak ineens naar onbekende omgevingen waren, dan was dat waarschijnlijk dus een webserver die eh, door eh, malware werd aangevraagd, maar die nog niet actief was. Derhalve he, kreeg je die eh, kreeg je die foutmelding, dat is ook een vorm van beveiliging natuurlijk. Maar dan hebben we het over zeg maar hele geanalyseerde netwerken eh, of hele geavanceerde analyses. Eh, het meest elementaire is gewoon de automatische

packetinspection op het verkeer, na ontsleuteling. Als je naar versleuteld verkeer kijkt, kan je ook nog wel wat doen, bijvoorbeeld het aantal eh, het aantal verbindingen dat opgesteld wordt, het aantal requests dat binnen komt of he, de sources, maar ja, dat, ja, is feitelijk een beetje waardeloos als je het vergelijkt met wat je kan eh, geautomatiseerd als je het verkeer in kan zien.

X: Ja. Oké. En dan een hele brede vraag. Met wat voor digitale dreigingen heb jij op een normale dag te maken?

Y: Haha. Even kijken, ik denk dat eh, als thuisgebruiker mijn digitale dreiging er niet anders uit ziet dan eh, voor iedereen anders en dat afhankelijk van wat voor bedrijf je werkt, en [the professional services firm] zou dat kunnen zijn he, een bedrijf waar je denkt hé, daar valt een hoop geld te halen of dat is leuk om het om te leggen en je ook nog eens in getarget kan worden. En nou dreigingen ja, die zijn ook ultrageneriek. Dus wij zullen vast wel geen beveiliging hebben blootstaan aan alle vormen van eh, van malware en dan kan je natuurlijk ja, denken aan alles, mensen die verkeer proberen af te luisteren, mensen die eh, proberen informatie te extraheren, mensen die proberen eh, toegang te krijgen tot systemen, tot applicaties, tot eh, de laptop in dit geval eh, mensen die dingen versleutelen om daarvoor geld te halen, ransomware, eh, ja, alles. Op die manier specifiek.

X: Oké-

Y: Om een heel breed antwoord terug te geven op je vraag.

X: Ja. En hoe verandert de soort dreiging door een VPN-verbinding?

Y: Nou ja, kijk, de soort dreiging he, we hebben natuurlijk te maken over de threat actors of threats, en we hebben natuurlijk te maken met kwetsbaarheden. Eh, ja, he, gebruik of geen gebruik eh, van VPN verandert niets aan mijn threats. He, dus als dat geautomatiseerd gaat of men wil doen, dat blijft bestaan. Het is niet dat ik een VPN-verbinding heb en ineens alle malware uit de wereld is. Eh, wat wel zo natuurlijk is dat eh, heel veel kwetsbaarheden die ik misschien zou hebben, bijvoorbeeld he, dat iemand een manier heeft gevonden om het verkeer tussen mij en in dit geval mijn ISP, waarschijnlijk een webserver ergens anders, en dan [the professional services firm] in te zitten, eh, ja, die kwetsbaarheid of die threat verandert niet, maar dat zij verkeer kunnen luisteren of meenemen of inzien wel. Omdat de VPN-verbinding het versleutelt in dit geval. Eh, dus dat verandert op die manier.

X: Oké. En heeft de VPN-verbinding nog meer invloed op de soort dreiging?

Y: Even kijken. Heeft de VPN-verbinding- Ja, wat, nou ja, wat je nog zou kunnen zeggen, stel dat ik maak gebruik van een bepaalde type VPN, stel nou dat andere mensen weten dat wij gebruik maken van die bepaalde type VPN, dat voor dat bepaalde type VPN een kwetsbaarheid bekend is eh, ja, dan zouden wij natuurlijk specifiek getarget kunnen worden. En alsnog steeds de vraag als het alternatief geen VPN is he, dan is het natuurlijk om het even. Dus theoretisch gezien op die manier wel, maar praktisch gezien vervang je dan natuurlijk de ene dreiging voor de andere.

X: Ja. Oké. En dit ging dan over digitale dreiging, heb jij ook op een normale dag te maken met een sociale dreiging?

Y: Ja, nou ja, voorheen meer dan nu natuurlijk, ik zit nu voornamelijk thuis. Dus mensen die met mij meelopen naar binnen heb ik niet echt heel erg. Mensen die mij afluisteren eh, en dat ik toevallig zeg of kunnen overheoren wat ik zeg maar zeg, heb ik natuurlijk ook niet meer, want ja, ik zit op die manier in een afgesloten en gecontroleerde omgeving. Eh, mensen die mij misschien proberen informatie te ontfutselen of iets dergelijks, ja, nee, ook niet. Eh, nee, ik denk het niet nee. Sociale dreigingen, nee, niet van threat actors zo ver ik weet en ook niet intentioneel. Zo ver ik weet.

X: Oké. En heeft een VPN-verbinding invloed op deze sociale dreigingen?

Y: Ik denk niet dat de VPN-verbinding invloed heeft op deze sociale dreigingen.

X: Oké.

Y: Behalve, ja, ik wil nog wel een ding opperen. Eh, als dat niet erg is. Stel nou, dit is natuurlijk niet het geval. Maar stel dat ik op een openbare locatie ben he, [0:35:03 until 0:35:04 has been omitted], in ieder geval niet thuis of bij [the professional services firm] kantoor en eh, iemand bemachtigd mijn laptop en op een of andere manier kan hij binnen komen en eh, dan zorgt de VPN natuurlijk wel voor dat eh, alles wat hij in kan zien beperkt is tot de gegevens die op mijn laptop staan. Aangezien door de twee-

factorauthenticatie hij de VPN nog niet kan opzetten en dus ook geen informatie kan verschaffen tot gegevens die op het [the professional services firm] netwerk staan. Als dat de bedoeling was van de vraag.

X: Ja, dat was de bedoeling van de vraag.

Y: Oké. Ja.

X: Bedankt. Als we kijken naar deze digitale en sociale dreigingen-

Y: Ja.

X: Wie of wat is dan de aanvaller die achter de dreiging zit?

Y: Ja, dat zal natuurlijk he, eh, eh, heel verschillend kunnen zijn. He, als je kijkt naar het landschap, dan heb je helemaal bovenaan heb je zeg maar nation states he, in de film altijd afgebeeld als [country], nou dat is het zeer zeker natuurlijk ook, maar he, natuurlijk ook een [country], [country] en eh, ja, met een zekerheid grenst er waarschijnlijkheid aan onze eigen burens en onze vrienden. He, dus door overheid eh, getraind en geleide eh, gespecialiseerde omgevingen. Nou, ik verwacht niet dat ik als persoon daar onderdeel van ben, ik verwacht wel heel stiekem dat [the professional services firm] daar misschien een klein beetje een target van is. Dat is een. Dan heb je nog gespecialiseerde hackersgroepen die dingen tegen betaling doen. Die vinden zich vast plaats in [country]. Denk ook niet dat wij daar onder zitten. Dan heb je een groep daaronder, dat zijn zeg maar hackercollectivism eh, ja, groepen. He, mensen die om wat voor reden dan ook eh, eh, vinden dat eh, wie dan ook eh, iets niet goed doen, daarvoor gestraft moet worden, op een miljard manieren kan dat natuurlijk. Daarvan denk ik wel dat wij als [the professional services firm] onderdeel eh, zeg maar ook een target van zijn. He, dat zou je dan kunnen benaderen aan het feit natuurlijk dat onze [role] schandalig veel geld verdienen, maar dat we waarschijnlijk ook wel prominentere klanten hebben eh, die sowieso op hun lijstje staan. En derhalve zeg maar, medeschuldig zijn. Mij persoonlijk denk ik niet. Nou daaronder heb je dan gewoon losstaande hackers zeg maar he, daar kan je natuurlijk wel verschillende gradaties in vinden eh, van echt zeg maar scriptkiddies en mensen die misschien ook professioneel doen. Nou ja, daar zullen we vast wel ook een target van zijn, maar he, eh, niet op de manier dat echt eh, belangrijk is. En natuurlijk andere organisaties. Met andere organisaties bedoel ik eh, concurrenten of andere partijen. Eh, ja, he, die, die zullen allemaal het wel op [the professional services firm] gemunt hebben ergens op de wereld. Hebben natuurlijk meer dan [number] medewerkers. Nou, ik verwacht eigenlijk zelf niet dat ik daaronder val. Het enige waar ik wel verwacht misschien onder te vallen zijn eh, he, wanneer een van die actoren besluit gewoon om geautomatiseerd een beetje te scannen om te kijken wat open is. Zeg maar eh, he, dan toevallig ergens op uitkomt. Even kijken, we hadden het over dreigers he, over threat actors toch nu?

X: Ja.

Y: Oké, ja, ja. Eh, nou ja, voor alle aanvallen die zij gebruiken, want ik ga vast vervolgvragen beantwoorden. Eh, denk ik dat de VPN mij beschermt op de manier die we hiervoor al zijn uitgelegd.

X: Oké. En wat is de motivatie van een aanvaller?

Y: Eh, de motivatie van een aanvaller kan natuurlijk verschillend zijn. He, eh, he, zoals we net al eh, eh, bespraken, hebben we natuurlijk de nation states, die zouden dingen doen om diplomatieke eh, eh, economische en militaire belangen eh, dan laat het eh, daaronder hadden we net ook alweer gezegd, hadden we de getrainde doelen, die doen het voor geld, eh, de hackers eh, groepen, die doen het vanuit een morele slash ethische eh, omgeving eh, vinden zij. Eh, die andere organisaties zouden het doen vanuit een commercieel belang. Scriptkiddies vanuit een intrinsiek belang. Volgens mij heb ik dan iedereen benoemd die we net benoemd hebben. En natuurlijk kan het gecombineerd zijn he, dus een goede ransomware aanval om een voorbeeld te noemen geleid vanuit een eh, een nationstate of een door een nationstate geleide groep, met als doel om eigenlijk een land plat te leggen en als bijkomend voordeel om heel veel geld op te halen, is natuurlijk een valide combinatie op die manier.

X: Ja. Oké. En wat voor achtergrond heeft een aanvaller?

Y: Ja. Nou ja, hij of zij zal natuurlijk wel eh, eh, op die manier goed moeten kunnen zijn met de techniek en de kwetsbaarheden en de beheersing van bepaalde tools. En de achtergrond voor de rest zeg maar he, waar je het hebt over demografieën of overtuigingen of iets ja, zou afhangen van in welke threat actor hij of zij zit.

X: Oké-

Y: Dan hebben we het over het technische verhaal, he. En het sociaal verhaal is natuurlijk eigenlijk hetzelfde, alleen dan ja, is het eh, he, als iemand natuurlijk met je mee wil lopen en ik hoor hem overduidelijk [country] praten of in ieder geval over duidelijk iets praten waarvan ik denk dat het [country] is en ik vind dat die heel verdacht dicht achter mij loopt, eh, he, dat is natuurlijk dan anders. Eh, maar voor de rest, ja, dat is qua achtergrond wat ik denk zeg maar. Zullen wel ja, attacksavvies zijn. Hoeft niet per se hoog- of laagopgeleiden te zijn of iets dergelijks.

X: Oké. En eh, over deze aanvaller, verandert de soort aanvaller door een VPN-verbinding?

Y: Ik denk niet dat de soort aanvaller verandert door de VPN-verbinding, wel dat de pogingen die het soort aanvaller doet door de VPN-verbinding verandert. He, dus eh, iemand met weinig kennis of iemand die denkt hé, het is wel grappig om even te kijken, eh, zo stuiten op die VPN-verbinding en door gaan naar een klant die makkelijker is. He, of een omgeving die makkelijker is. Eh, ja, he, een echt getargete aanval he, eh, he, dus zeg maar die eerste paar threat actors die ik benoemde, ja dat zou toch niet veranderen want die zijn he, niet gemotiveerd vanuit een perspectief dat ze even aan het kijken zijn zoals een scriptkiddie met een hé, wat is leuk om te doen he, dat is een hele andere motivatie. Dus die zullen niet ophouden. Of in ieder geval, die zullen niet weggaan omdat de VPN-verbinding er is. He, misschien dat ze niet eh, niet slagen in hun poging he, maar ja, dat zou niet betekenen dat ze niet ophouden of dat ze geen andere manier vinden.

X: Duidelijk. Wat zou de impact van een aanval kunnen zijn?

Y: Nou ja he, in ons geval zou dat eh, zou de impact van een aanval op verschillende manieren kunnen uitwerken. Denk aan eh, commercieel belang he, dus in dit geval zou dat bijvoorbeeld het niet kunnen gebruiken van bepaalde middelen kunnen zijn eh, waardoor wij ons werk niet kunnen uitoefenen. Het zou ook een ... belang kunnen zijn he, dus wij kunnen het niet gebruiken maar we zijn bijvoorbeeld gegevens kwijt. Eh, he, allemaal economische verhalen eh, he, we zouden data kunnen verliezen van klanten of het kan openbaar worden, zijn ook allemaal nog economische verhalen. Eh, ja, in ons eigen geval he, mensen zouden misschien een beetje bangig(0:42:54) kunnen worden, maar de impact denk ik bij [the professional services firm] zal altijd zijn economisch eh, aangezien wij geen ziekenhuis zijn waar daadwerkelijk mensen van afhankelijk zijn. Dus ik denk dus economisch en afhankelijk van hoe je het ziet kan het het verlies zijn van he, eh, het gaat natuurlijk een stuk verder. He, je hebt natuurlijk improductiviteit(0:43:14) of verlies van data of het weggaan van data, maar ja, als wij natuurlijk geen werk kunnen uitoefenen, zullen klanten als onprofessioneel zien en misschien niet meer bij je komen et cetera. Dat kan natuurlijk door blijven lopen. He, eh, wat nog wel kan schelen, kan gelden overigens, is ook het verlies van integriteit, eh, want als het hen lukt om bijvoorbeeld allemaal persoonsgegevens openbaar te maken eh, ja, dan hoeft het niet per se natuurlijk een economisch probleem te zijn he, commercieel probleem, maar zorgt het er ook voor dat de privacy van mensen aangetast kunnen worden.

X: Ja-

Y: Kan natuurlijk ook wel weer een commercieel probleem hebben, dat je dan eh, als je het een beetje slecht gedaan hebt, terecht de AVG aan je broek op hebt, aan je broek hebt. Maar he, dat dan zeg maar, dan hebt je niet iets wat op die manier direct in geld uit te drukken is, wat wel echt een probleem is.

X: Ja. Oké. En als we dan gaan kijken naar de VPN-verbinding zelf-

Y: Ja.

X: Hoe veilig is een VPN-verbinding?

Y: Eh, nou er, ervan uit gaande zeg maar dat he, dat alles wat men doet, men goed doet. Dus je zou vast een miljard instellingen hebben eh, die je moet kunnen uitvoeren. Dat is de beveiliging van de VPN-verbinding zelf he, dus dan hebben we het niet over het feit dat je met een ander netwerk verbonden bent, maar echt de VPN-verbinding zelf eh, is eh, even sterk als de manier van versleuteling. Dus maak jij of een fout met het versleutelen aan het begin waardoor iemand dus kan achterhalen eh, hoe je kan versleutelen of iemand zich kan voordoen als dat die jij hem bent eh, he, dus dan ontvang je alle informatie. Eh, is natuurlijk veel kwalijker als jij een manier van versleutelen hebt die eh, mathematisch te kraken is, waardoor dus iemand wel kan meelezen en je dus oorspronkelijke eh, eh, oorspronkelijke gevaar of oorspronkelijke dreiging weer terug hebt, namelijk dat alle informatie die je hebt ingelezen kan worden. Dus het hangt allemaal af van die

twee factoren, dus implementatie en werking. Eh, in hoeverre je daarin kan variëren en natuurlijk daadwerkelijke eh, eh, rekenkundige sterkte van de versleuteling zelf.

X: Zijn er naast de versleuteling nog andere manieren waarop een VPN mogelijk niet veilig is?

Y: Eh, we hebben het natuurlijk al, we hebben het natuurlijk gehad he, we hebben het over de pure verbinding zelf gehad, we hebben het gehad over eh, andere configuratiezaken he, dus eh, he, als een VPN verbinding eh, ik noem maar wat, om wat voor reden dan ook vanuit meerdere apparaten gelijktijdig opgezet kan worden vanuit verschillende omgevingen en dat wordt niet gezien als iets vreemds bijvoorbeeld he, dan, dan, dan eh, zou dat iets kunnen zijn. Maar dan zitten we eigenlijk weer in een configuratie, dus ik kom terug he, geconfigureerd, dus op de manier dat eh, het alleen voor bekende users, bekende apparaten he, eh, werkt eh, op een manier waarop die initiële eh, wachtwoorduitwisseling goed gaat met een beveiligde verbinding, denk ik niet dat er andere manieren zijn waarop een VPN-verbinding veiliger of onveiliger ingericht kan worden.

X: Oké. En eh, je hebt enkele manieren genoemd waarop een VPN-verbinding mogelijk onveilig is, of minder veilig-

Y: Hmhm.

X: Veranderen jouw handelingen hierdoor?

Y: Nee, want ik heb als eindgebruiker eh, weinig invloed op. He, stel dat, dat eh, he, laten we beginnen met het meest voor zichzelf sprekende, dat eh, de type versleuteling van een VPN-verbinding slecht is he, mathematisch te kraken, ja, dan kan ik nog steeds niet niet gebruik maken van die VPN, want ik heb hem nodig om het werk uit te oefenen. Wat natuurlijk wel kan zijn is he, stel, dat tweede, stel dat ik weet dat het op ons van toepassing is, zal ik gezegd van oké, he, dan ga ik ook niet meer mijn eigen mail bijvoorbeeld benaderen vanuit eh, [the professional services firm] he, vanuit mijn werklaptop, want ik weet niet of iemand dat kan meelezen. Maar ik kan er zelf weinig tegen doen natuurlijk. Eh, als ik geen controle heb. Het enige wat ik kan doen is mijn wachtwoord invoeren. Eh, dus ja, als eindgebruiker zal ik waarschijnlijk wat ander gedrag vertonen, omdat ik dan he, puur alleen eh, eh, het verkeer eh, hoe noem je het, het verkeer beperk tot het hoogstnoodzakelijk, hoogste hoogstnoodzakelijke he, en indien er geen andere manieren zijn. Eh, maar voor de rest blijf ik gebonden aan het feit dat ik moet kunnen werken, aangezien mijn werkgever dat ja, op prijs stelt. Laten we het maar zo noemen.

X: Ja, en doe jij dat ook? Maak jij alleen gebruik van het hoogstnoodzakelijke dingen met VPN-verbinding?

Y: Eh, nou ja, dat gaat om twee aannames in. Ja, er zijn zaken die ik he, en dan he, het klinkt misschien heel deur opener, is helemaal niet zo, maar die ik gewoon überhaupt niet doe op mijn werklaptop. Eh, he, bepaalde sociale websites en dergelijke, eh, en dat heeft misschien niet iets per se met de beveiliging te maken, maar omdat ik het gewoon onprofessioneel vindt dat je ook een klein beetje die brandbreedte moet beperkt moet houden. Mocht ik nou weten bijvoorbeeld dat de verbinding niet veilig genoeg is, dan zou ik bijvoorbeeld ook niet meer snel even paar mailtjes van mijn eigen eh, eh, via het Internet benaderbare mails beantwoorden en dergelijke. Eh, maar voor de rest, ja, ik gebruik hem op die manier niet voor het hoogstnoodzakelijke, ook omdat het bijna eh, niet te doen is. Want je moet gewoon soms dingen regelen en je moet soms dingen opzoeken. Eh, anderzijds gebruik ik hem niet als een vrije verbinding, dus ik zit er tussenin. Wat ik wel gedaan heb-

X: Oké. Ja.

Y: En zeker toen aan het begin van de coronacrisis, he, toen was het ook zo dat onze capaciteit niet zo heel erg groot was, toen heb ik wel eigenlijk een VPN alleen maar gebruikt echt op het moment dat ik met het [the professional services firm] netwerk verbonden moest zijn. Dus in dat eigenlijk een gouden zet gevonden dat eh, eh, onze mailserver geen VPN meer nodig had en daardoor hoef je ook dus niet constant verbonden te zijn met de VPN-omgeving. Eh, en nu nou ja, we zeggen het eigenlijk wel, maar als ik erover nadenk moet ik eigenlijk toch terugkomen, want ik zet nu de VPN eigenlijk ook alleen maar aan als ik echt specifiek intern systeem nodig heb. Dus ik gebruik het eigenlijk wel voor het hoogstnoodzakelijke, ja. Haha, bedenk ik mij nu, want eh, ik heb hem vandaag nog niet aangehad.

X: Oké. Eh, dan waren dit tot zo ver mijn vragen-

Y: Hmhm.

X: Zijn er dingen over VPN die wij niet besproken hebben nu?

Y: Eh, even kijken, ja, er zullen vast wel dingen zijn. Er zullen vast ook een miljard dingen zijn die ik niet weet over VPNs. Eh, ja, ik denk het eigenlijk niet, het is geconfigureerd, het is ingesteld, we loggen in, we maken een verbinding, we gebruiken het ergens voor, we hebben gesproken over mogelijke aanvalsvectoren, factoren, wie het kunnen zijn, welke kwetsbaarheden zouden kunnen eh, eh, misbruiken en hoe we het zouden kunnen oplossen. Ik denk het niet, denk ik.

X: Oké. Dan was dit tot zo ver het interview.

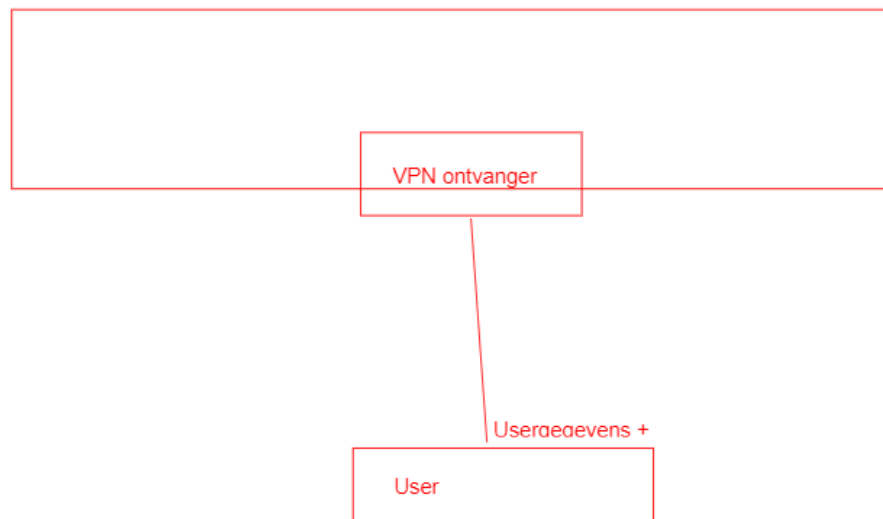


Figure C.11.1: Drawing 11_1

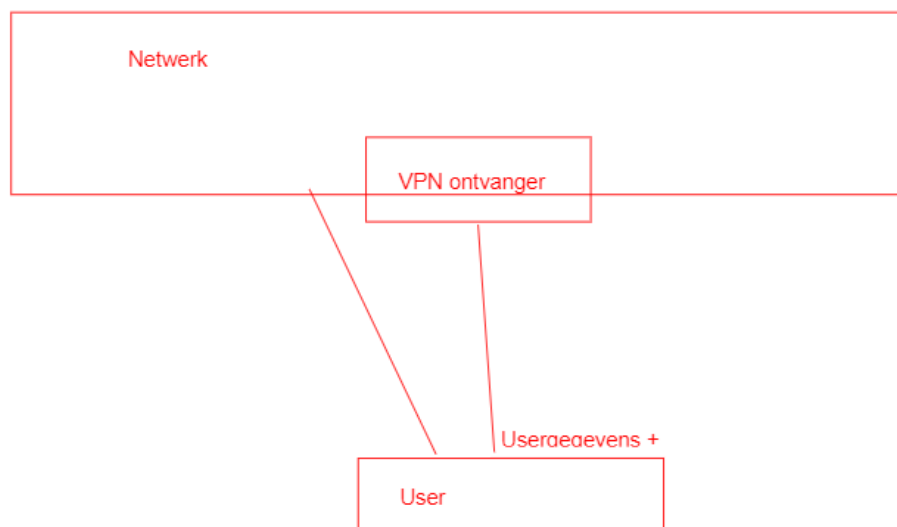


Figure C.11.2: Drawing 11_2

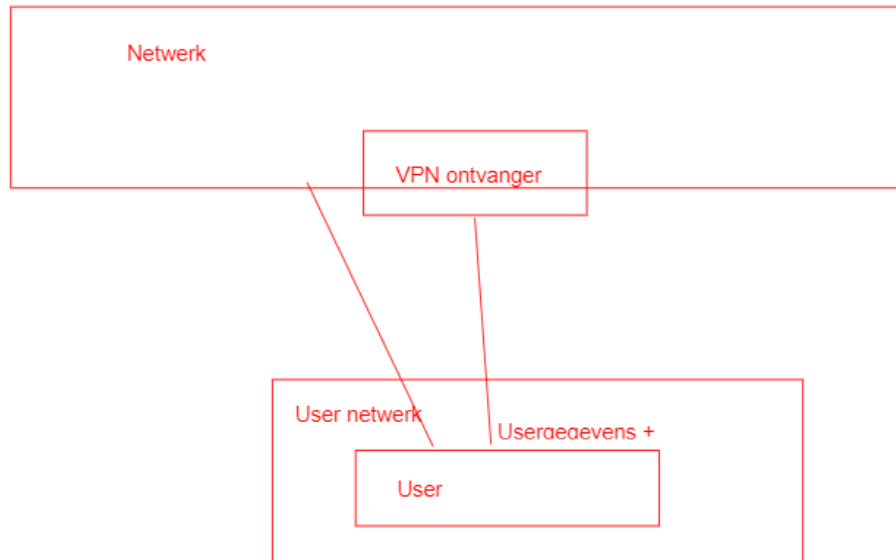


Figure C.11.3: Drawing 11_3

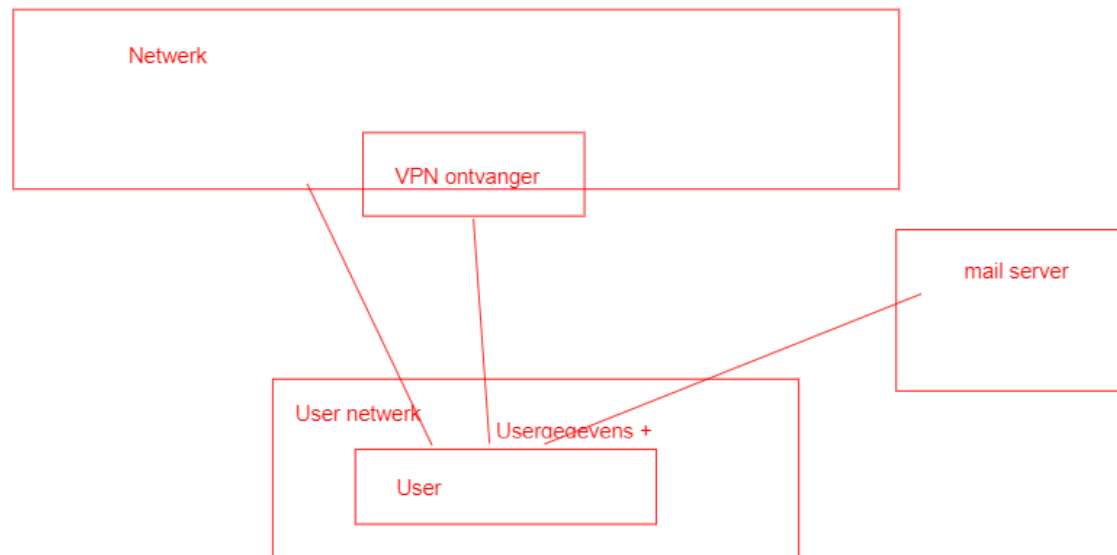


Figure C.11.4: Drawing 11_4

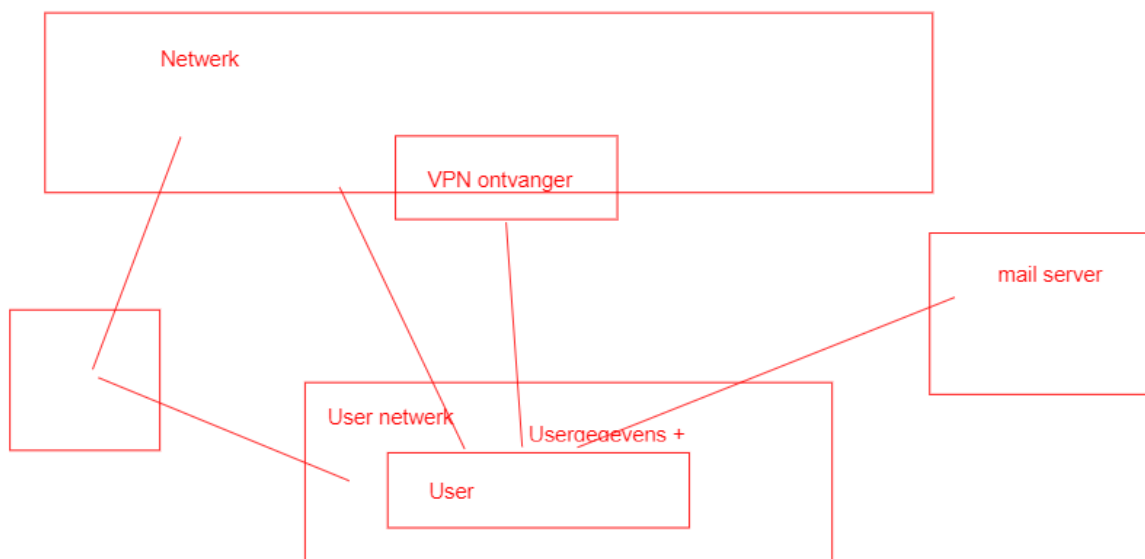


Figure C.11.5: Drawing 11_5

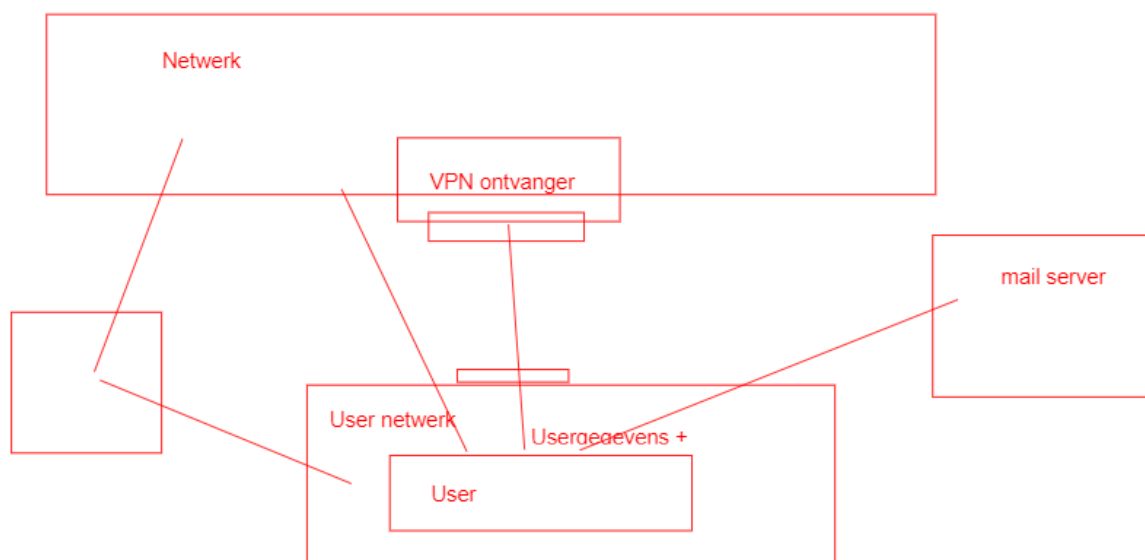


Figure C.11.6: Drawing 11_6

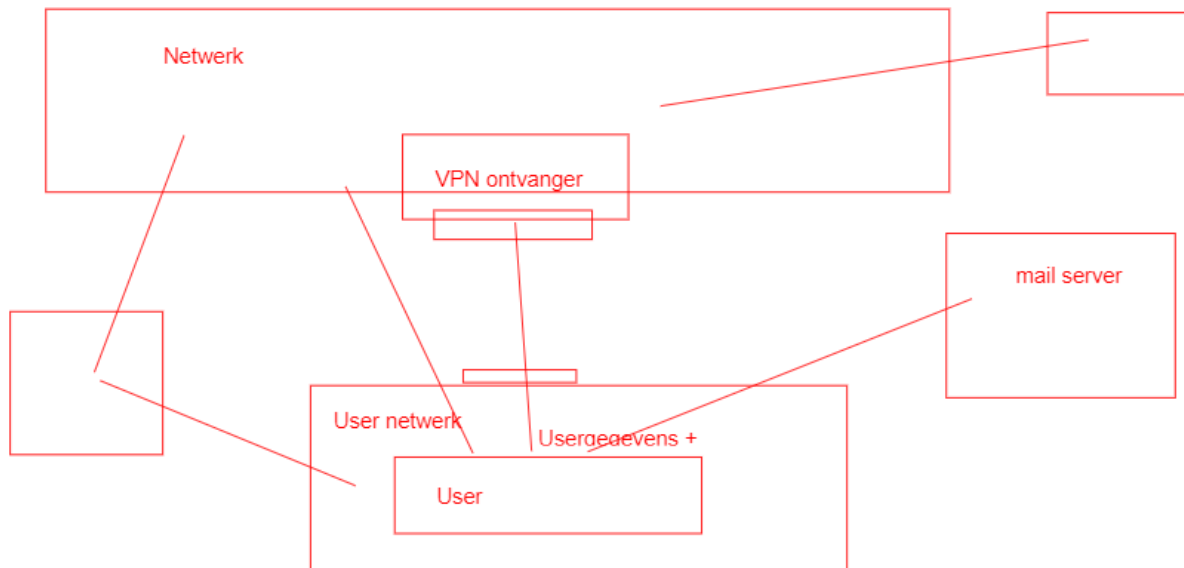


Figure C.11.7: Drawing 11_7

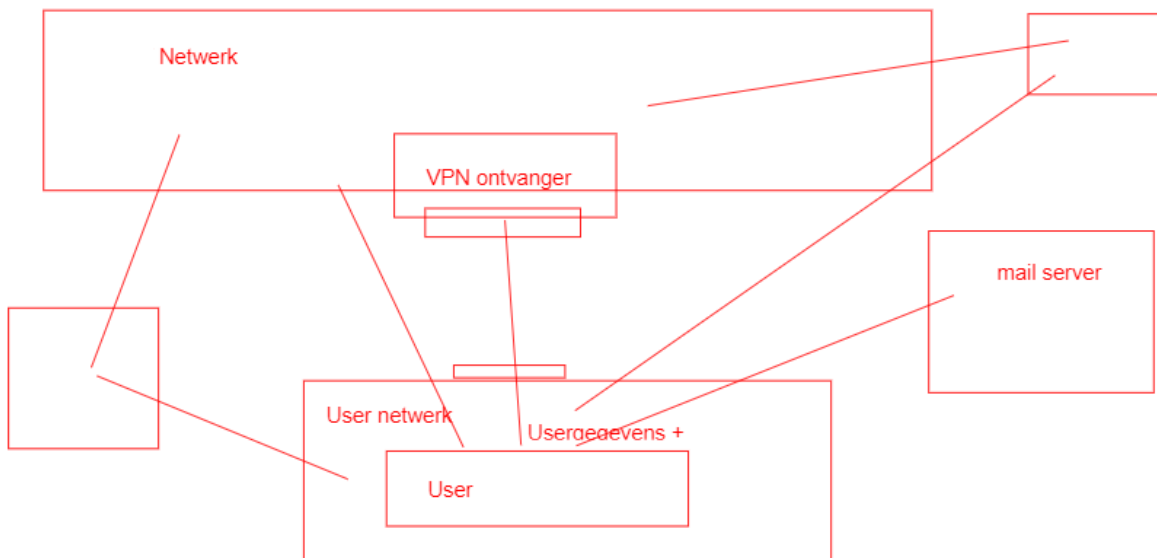


Figure C.11.8: Drawing 11_8

C.12: Transcript Laypeople 1

Duration: 28 minutes

Language: Dutch

Number of drawings: 0

X: Dan de eerste vraag. Kun je aan mij uitleggen wat een VPN is?

Y: Eh, ja, denk ik. Eh, een eh, ja, een IT mogelijkheid om op een veilige manier vanaf een onafhankelijke, flexibele plek in een netwerk te kunnen inloggen, zoiets.

X: Ja. En wat bedoel je met een veilige manier?

Y: Eh, dat je toegang krijgt omdat je ook recht hebt om toegang te kunnen krijgen. He, dus je hebt een code nodig om vaak, he, om een VPN eh, om binnen te komen als het ware. Dus dan bedoel ik met veilig in de zin van privacy, dat soort dingetjes.

X: Oké. En wat voor code heb je daarvoor nodig?

Y: Bij [the professional services firm] is dat een eh, ja, een zes-cijferige code, plus een ja, dat is een deel, en een wachtwoord. Dus een wachtwoord plus code.

X: Oké. En je zegt dat je op een flexibele plek kan inloggen, wat bedoel je daarmee?

Y: Nou ja, kijk, vroeger was het denk ik zo dat eh, dat je natuurlijk altijd op kantoor aan een kabeltje moest om eh, ja, Internet, intranet, dat soort dingen, ten minste, zoals ik mij dat kan herinneren. En eh, waar ik- En wat in mijn beleving voor mij zeg maar VPN betekent, is dat ik bijvoorbeeld thuis kan werken en dan kan inloggen op ons eh, ons [the professional services firm] netwerk. Dus ja, je kan eigenlijk op elke plek op de wereld inloggen op het intranet, terwijl dat vroeger denk ik eh, ja, maar daar moet je me ook op corrigeren als dat niet zo is, want ik heb geen technische achtergrond, dat dat volgens mij alleen kon als je achter een computer op kantoor zat of met een kabeltje op kantoor je laptop eh, ja, aanschakelde.

X: Zijn er nog andere redenen waarom jij een VPN gebruikt?

Y: Nee.

X: En op welke locaties gebruik jij een VPN?

Y: Eh, eigenlijk alleen maar thuis. Ja.

X: Welke handelingen voer jij uit om een VPN verbinding te maken als gebruiker?

Y: Eh, dan moet ik op ja, welke handelingen voer ik uit. Dan moet ik dus eh, naar de tool toe waarop ik mijn wachtwoord kan invullen, dus dat is eh, ja, dat heet [the VPN of the professional services firm], daar moet ik op klikken op mijn desktop en dan moet ik een eh, gebruikersnaam staat er al, en dan moet ik het wachtwoord invullen, samen met die code die ik via een app op mijn telefoon krijg. Dus ik moet eerst wachtwoord invullen eh, nou zeg eens wat, blauw bij wijze van spreken, en dan geeft mijn telefoon een code van zes cijfers, wat natuurlijk steeds wordt verversd om de zo veel seconden. Eh, dat moet ik er dan aan toevoegen en dan moet ik op oké klikken en dan wordt de VPN verbinding gemaakt.

X: Oké. En is er nog een andere manier om aan die code te komen?

Y: Eh, niet dat ik weet, volgens mij niet.

X: Oké. Eh, op welke apparaten gebruik jij een VPN?

Y: Eigenlijk alleen op mijn laptop. Ja, laptop van werk.

X: Heb je ook een mobiel van werk?

Y: Ja, maar daar probeer ik eigenlijk zo min mogelijk eh, met mail en zo dingen te doen. Dus daar doe ik niets met een VPN verbinding.

X: En eh, zou je mij kunnen uitleggen hoe een VPN werkt? Je kunt hier als je wilt het whiteboard voor gebruiken.

Y: Hoe bedoel je die vraag precies? Eh, goed. Kan je misschien-

X: In de situatie dat jij vanaf huis een VPN verbinding maakt-

Y: Ja.

X: Hoe ziet dat er meer op technisch gebied uit?

Y: Eh, ja, eigenlijk wat ik net omschreef. Dus ik voer een wachtwoord in eh, klik op een dingetje op mijn desktop, ik voer een wachtwoord in, ik klik op oké, dan zie ik dat er geconnect wordt, en dan heb ik toegang.

X: Oké. En weet je ook waarmee een verbinding wordt gemaakt?

Y: Eh, ja, volgens mij naar een, naar een intranetomgeving. Bedoel je, ja, bedoel je, bedoel je dat, of ja, ik weet het niet-

X: Ja.

Y: Ja, ik denk met een eh, met een eh, ja een soort van eh, beveiligde eh, [the professional services firm] omgeving waarin alleen medewerker van [the professional services firm] die daar toegang toe hebben, tot die informatie kunnen komen. Dus eigenlijk een informatie eh, ja, een informatieplatform waar je toegang tot krijgt, wat afgesloten is van eh, van andere gebruikers dan de eh, gebruikers die daar toegang tot hebben. Zoiets, haha.

X: En hoe denk je dat deze verbinding tot stand komt?

Y: Eh, hoe die verbinding tot stand komt. Dat weet ik eerlijk gezegd niet. Zo ik niet weten. Eh. Nee, zou ik niet durven zeggen, ik heb geen idee.

X: Oké, geen probleem. Eh, dan ga ik door naar de volgende vraag-

Y: Ja.

X: Wat is de invloed van een VPN verbinding op jouw computerbeveiliging?

Y: Mijn computerbeveiliging. Eh, nou ja, kijk, ik kan bijvoorbeeld bepaalde documenten uiteindelijk op een server zetten, die alleen toegankelijk is, de documenten op die server zijn alleen toegankelijk als er een VPN verbinding gemaakt kan worden. Dus dat is, dat zou mijn antwoord dan zijn. Dat je bepaalde documenten dus eh, eh, ja, toegankelijk maakt voor mensen die ook toegang hebben tot eh, tot die VPN verbinding zeg maar, tot dat platform waar ik het net over had.

X: Wat is een server?

Y: Eh, een server, daarmee bedoel ik een eh, een eigenlijk een eh, eigenlijk een map op eh, dus, ja, gewoon echt een documentenmap eh, die ja, eh, wat is een server eh, ... helemaal goed met een map, want het is eigenlijk ook weer een link naar een bepaalde eh, plaats, waar, waar mappen staan, waar beveiligde informatie, nou beveiligde informatie, waar informatie in staat die je, zo via die VPN verbinding nog he, op die manier wordt beschermd, omdat, zodat niet iedereen toegang daartoe kan krijgen. Dus als ik nou bijvoorbeeld een document op mijn desktop zet, dan is dat een stuk minder beveiligd dan dat ik het op een server zet. Dus daarmee bedoel ik dus een map, die eh, bereikt kan worden eh, als je een VPN verbinding eh, ... hebt ...

X: Duidelijk. En dan een hele brede vraag. Met wat voor digitale dreiging heb jij op een normale dag te maken?

Y: Eh, ik denk dat dat misschien wel meer is dan ik zelf zie. Dus ik zou als ik zeg maar wat zie ik, dan zie ik niets. Maar ik kan wel vermoeden dat eh, dat [the professional services firm] in het algemeen of eh, dat, dat er wel is. En dat daar wel risico's in zitten. Eh, vanuit [department] werken we natuurlijk ook met privacygevoelige informatie, dus dat kan ook nog wel het risico iets vergoten. Maar dit is misschien meer vanuit extern dat je de vraag stelt. Eh, meer vanuit externe, hoe noem je het, partijen zeg maar, die proberen, iets eh, intern te bereiken. Eh, ja, ik vind het lastig om zo te beantwoorden, maar ik denk dat eh, ik vermoed dat het erger is dan ik zelf denk.

X: En zou je kunnen nadenken over voorbeelden? Wat voor soorten dreigingen?

Y: Eh, ja, nou ja, wat je bijvoorbeeld eh, dat je bijvoorbeeld, kijk, er was laatst iets bij een universiteit, ik weet even niet meer wat dat nou was, was een, een of ander virus geloof ik of zo eh, op een eh, uiteindelijk op een ook ergens terecht gekomen, volgens mij was dat universiteit Leiden of zo, waarbij je dus ziet dat er eh, ja, wat was daar ook al weer het gevolg van, dat informatie van mensen wat natuurlijk zo maar verspreid kan worden, privégegevens eh, bepaalde examens konden toen geloof ik niet doorgaan of, of studenten konden niet op het intranet van de universiteit, ja, dat soort voorbeelden dus, dat, dat bij wijze van spreken ook ons intranet van [the professional services firm] niet zou werken, omdat er bijvoorbeeld een aanval wordt gedaan. Ik weet niet of ik nou de, of ik jouw vraag nou goed begrijp, maar-

X: Ja, dat is zeker een voorbeeld.

Y: Oké, oké. En meer vanuit zeg maar [department], maar volgens mij is dat niet echt een antwoord op jouw vraag, is het meer dat ik zit met privacygevoelige informatie. Dus stel ik zou bijvoorbeeld een verkeerde mail sturen eh, over bijvoorbeeld eh, [0:10:56 until 0:11:07 has been omitted]. Dat soort informatie, dat is natuurlijk heel erg privacygevoelig ook, en daar werk ik veel mee. Eh, maar ik zie niet zo snel, zeg maar de fout ligt dan meer aan mijn kant, he, dus dat ik het verkeerd gebruik waardoor het, waardoor het in verkeerde handen komt en jouw vraag zie ik volgens mij meer op wat ik net zei op dat een externe partij iets richting [the professional services firm] wilt doen.

X: Ja, het kan allebei. Een volgende vraag. Heeft een VPN verbinding invloed op deze digitale dreigingen?

Y: Invloed, eh, ja, dat denk ik uiteindelijk wel. De invloed zit hem er gewoon op dat je denk ik minder snel eh, toegang kunt krijgen als externe partij eh, op bepaalde informatie die hangt in een platform achter een VPN verbinding, dan dat het gewoon op iemands desktop allemaal staat. Dus stel we zouden niet met een VPN verbinding werken en we zouden inderdaad gewoon alles maar eh, ja, op de computer zetten, bij wijze van spreken. En naar elkaar mailen, in plaats van dat we bijvoorbeeld met een VPN verbinding werken waarin we documenten met elkaar kunnen delen en waarbij iedereen elk moment van de dag kan. Ja, dat heeft wel invloed op de veiligheid denk ik. Dus ik denk dat het een positieve invloed heeft op de veiligheid, een VPN verbinding.

X: Oké, duidelijk. En dit is dan over digitale dreiging. Heb jij daarnaast ook nog te maken op een normale dag met een sociale dreiging?

Y: Eh, nee, eigenlijk-

X: Als in meer, niet-digitale dreigingen.

Y: Nee, eigenlijk niet. Nee. Zou niet weten, nee, geen idee, nee, niet dat ik weet, komt niets in mij op in ieder geval.

X: Oké. En als je dan teruggaat naar de digitale dreigingen-

Y: Ja.

X: Wie of wat is de aanvaller die achter deze dreiging zit?

Y: Ja. O, wie dat is?

X: Ja. Ja, of-

Y: Eh-

X: Voorbeelden.

Y: Ja, hoe wil je, hoe noem je dat, hackers of eh, of criminele organisaties die eh, bij wijze van spreken eh, eh, iets willen, iets, iets van [the professional services firm] willen en eh, onder digitale dreiging in plaats van he, zeg maar met een eh, met een pistool op je kop, met digitale dreiging iets voor elkaar krijgen. Dus bijvoorbeeld dat [the professional services firm] geld zou betalen om eh, zodat die hackers bijvoorbeeld bepaalde dingen terugdraaien ten aanzien van digitale platforms of eh, ja, zoiets. Dan denk ik vooral namelijk aan criminele organisaties of eh, je hebt ook van die hackers die dat voor hun plezier doen geloof ik. Eh, maar net als bij dat voorbeeld van de universiteit die ik noemde, daar zat volgens mij ook een partij achter die aangaf je krijgt het netwerk weer terug of eh, er worden dingen hersteld onder de voorwaarde dat je een bepaald geld bedrag betaald. Nou, dat is denk ik, dat zou voor mij ook een voorbeeld zijn als antwoord op jouw vraag.

X: En je zegt al dat sommigen het voor hun plezier doen en anderen die vragen geld, kan je meer andere motivaties van een aanvaller bedenken?

Y: Eh, nou ja, ik kan, nou ja, misschien, eh, he, je kan wel voorstellen, stel iemand zou bijvoorbeeld bij ons ontslag krijgen en eh, zou dat zo erg vinden, dat die zo boos is op [the professional services firm] dat die bedenkt van he, ik ga [the professional services firm] stangen en ik ga ze kapot maken haha en ik ga een eh, ik ga eh, een van mijn vrienden dat is een goede hacker en ik ga samen met hem of haar tegen de, het netwerk van [the professional services firm] platleggen bij wijze van spreken. Dan zou je aan zoiets moeten denken. Dat zit misschien meer in het [department] straatje. Gaat heel ver, maar het zou kunnen.

X: Ja, oké. En wat voor achtergrond heeft een aanvaller?

Y: Achtergrond, nou ja, omdat het om digitale en VPN zou je toch een, zou je toch een technische achtergrond moeten hebben. Ik weet niet of dat, of dat, of je dat met achtergrond bedoelt. Ik denk wel eh, wat betreft degene die het uitvoert moet ook ja, dan toch wel een beetje ook wat hoger opgeleid zijn, in die zin dat je echt specifieke technische kennis moet hebben om dat te doen. Wil natuurlijk niet zeggen dat degene die dat doet, dat die hacker of degene die de technische vaardigheid heeft ook de bedenker van het plan is en ja, de achtergrond van eh, ja, de achtergrond van zo een bijvoorbeeld een criminele organisatie kan natuurlijk van alles zijn met eh, ja. Wat eh, dat weet ik niet.

X: Duidelijk. En eh, wat zei de impact van een aanval kunnen zijn?

Y: Eh, ja, de impact zit hem dan voornamelijk denk ik op dat dingen stil komen te liggen en dat zou dus impact kunnen hebben op dat we bepaalde werkzaamheden voor klanten niet kunnen afronden. Eh, dat is denk ik voor de business vooral het belangrijkste, als zij een afspraak hebben gemaakt om op een bepaalde dag iets op te leveren. [0:16:29 until 0:16:37 has been omitted]. En je zou daarmee in de knoei komen omdat het netwerk bij wijze van spreken, en daarbij alle toegang tot alle tools die je daarvoor gebruikt niet bereikbaar is, dan kan ik me voorstellen dat dat aardig wat schade kan opleveren. Eh, ik denk dat dat eh, het belangrijkste zou zijn. Voor de rest inderdaad ook het voorbeeld wat ik eerder noemde, dat de schade ... dat als er bijvoorbeeld bepaalde informatie door degene die dat doet eh, publiekelijk komen, daardoor individuen zoals ja, werknemers eh, daardoor misschien schade kunnen leiden.

X: Duidelijk. En eh, teruggaand naar de VPN verbinding-

Y: Ja.

X: Heeft de VPN verbinding invloed op de soort aanvaller? Verandert de soort aanvaller door een VPN verbinding?

Y: Eh, nee, ik denk het niet. Ik denk in die zin, als we het dan meer over IT hebben dat of het nou een VPN verbinding nou wel of niet is, dat je toch altijd wel die eh, dat je toch altijd wel die specifieke vaardigheden moet hebben. Ik zou bijvoorbeeld of er nou wel of niet een VPN verbinding is, ik, ik zou dat sowieso niet eh, ik zou daar helemaal niets mee kunnen. Dus eh, je moet ja, ik denk dat dat in die zin niet heel veel uitmaakt. Het zit er met name in dat gewoon een extra horde wordt ingebouwd door zo een VPN verbinding om het voor elkaar te krijgen. Dus het maakt eigenlijk, het maakt het gewoon wat moeilijker, het maakt het niet anders denk ik. Eh, ja.

X: En als we naar een VPN verbinding zelf gaan kijken-

Y: Ja.

X: Hoe veilig is een VPN verbinding?

Y: Kan ik niet echt beoordelen. Ja. Ja, dat kan ik echt niet beoordelen, geen idee. Ik heb daar nooit iets van gemerkt dat het niet goed zou gaan ofzo. Dus ik denk dat het goed is, maar ja, daar kan ik eigenlijk geen uitspraken over doen. Ik zou het niet weten hoe goed onze VPN verbinding is.

X: Kan je een situatie bedenken dat er bijvoorbeeld misbruik van wordt gemaakt?

Y: Eh, nee, nou, nee, ik denk het niet. Ik zou zelf niet iets weten waardoor je er misbruik van zou kunnen maken. Ik zit even te denken. Nee. Ik zou het niet weten, geen idee.

X: En eh, heb jij verder nog dingen over VPN die jij denkt dat belangrijk is om te zeggen, maar die nu niet ter sprake zijn gekomen?

Y: Eh, nee, ik zit even te denken. Eh, nou, ja, ik weet niet, ik ben niet zo technisch, dus ik weet ook niet bijvoorbeeld of er alternatieven zijn. Is VPN iets wat op zichzelf staat, of eh, ja. Weet ook niet, is er bijvoorbeeld een keuze in eh, in VPN verbindingen of providers, die VPN verbindingen eh, ik heb daar geen, ik heb daar totaal geen verstand van. Dus ik weet niet wat voor een keuze [the professional services firm] daarin bijvoorbeeld heeft gemaakt eh, en of dat nog relevant is, maar dat zou ik nog kunnen voorstellen. Maar daar heb ik, dat weet ik ook eerlijk gezegd niet. Dus een beetje een zinloze vraag, maar-

X: Nee, zeker. Belangrijk om te zeggen.

Y: Ja. VPN, is dat iets eh, he, is dat bijvoorbeeld hetzelfde dat als je, je hebt bijvoorbeeld Apple en je hebt bijvoorbeeld Microsoft, en je hebt dus allebei een organisatie die iets, die hetzelfde soort product leveren. En ik weet niet hoe dat bij VPN zit, is VPN, dat is een titel denk ik voor iets he, dus bijvoorbeeld eh, wat leveren Apple en Microsoft, die leveren een softwaresysteem als ik het goed zeg eh, en ik weet niet of eh, of er partijen zijn die VPN verbindingen, ja, of daar verschil in zit bij wijze van spreken.

X: Zeker goed om over na te denken.

Y: Haha. Ik zeg maar ja, ik weet het ook niet hoor, ik zit maar hardop te denken. Ik weet het niet.

X: Nee, dat is zeker goed. Dat helpt bij mijn beeldvorming. Zijn er zo verder nog dingen die je kunt bedenken?

Y: Eh, nou, misschien ook, ik weet niet of dat he, we gebruiken bij VPNs en dat is in mijn beleving sinds dat het eigenlijk is ontstaan eh, codes, en je zou misschien kunnen afvragen van eh, bijvoorbeeld met vingerafdrukken, tegenwoordig kan je steeds meer dingen ook met de bank bijvoorbeeld met vingerafdrukken ... is dat ook iets, misschien dat het het ook iets veiligers maakt. Ik denk dat dat ook nog iets is. Ik vind altijd wel al het lijkt een beetje een ouderwetse manier altijd vind ik. We hadden voordat we het met de telefoon met de app deden hadden we een token, dus echt zo een soort van een apart klein dingetje wat aan mijn sleutelbos hing, waar ook die code steeds op versprongen. Nou dat is inmiddels naar een app toegegaan, dus dat vind ik al een hele modernisering. Je zou je ook kunnen afvragen van eh, kan een VPN verbinding bijvoorbeeld ook via een eh, he, met een vingerafdruk op een telefoon als het ware je VPN verbinding tot stand laat brengen op je computer.

X: Dat dingetje dat aan de sleutelbos hangt, dat is nu niet meer beschikbaar?

Y: Nee, die, die, dat dingetje dat inderdaad wat aan je sleutelbos hing, dat is vervangen door een app inmiddels, ja.

X: Oké-

Y: Dat is echt al wel even kijken hoor, ik denk, misschien is dat zelfs al twee jaar.

X: Kan je verder nog dingen bedenken?

Y: Eh. Nee. Nou ja, ik zit nog, even kijken, ik weet ook niet of dat een relevant iets is. Eh, ik weet niet of het logisch is of misschien uitmaakt ook nog voor veiligheid of je, wat je eigenlijk toch moet doen bij een VPN verbinding is in de eerste instantie een verbinding ook moet zijn met een wifi netwerk. Dan kun je vervolgens je VPN verbinding gebruiken, ten minste zo werk ik altijd. Ik heb dat ook nog nooit anders ervaren. Ik vraag me af, is het ook mogelijk dat je bijvoorbeeld direct eh, zonder dat je ergens een wifi verbinding bij wijze van hebt, dat je gewoon in een keer hup, je kan gelijk ergens op een intranet via een VPN verbinding komen. Ik weet niet, ik weet niet of ik nu iets raars of iets relevants zeg, maar eh- Dat is natuurlijk ook wel een dingetje, dus als ik bijvoorbeeld, stel ik zou een keer ergens in een café ofzo een VPN verbinding willen maken, dan zou ik dus altijd bij dat café een Internet of een wifi nodig moeten hebben om vervolgens ook eh, dan die VPN verbinding daarna te kunnen leggen. En voor zo ver ik weet kan je niet direct een VPN verbinding aanmaken, maar dat, misschien zeg ik iets dat niet klopt.

X: Ja, en is het relevant of je een VPN op een wifi in een café gebruikt?

Y: Eh, nou, nee, dat niet maar he, kijk wat ik zei van eh, kijk, ik werk nu altijd vanuit huis, dus voor mij, ik gebruik de VPN verbinding vanuit huis. Nou, er zijn ook collega's die het bijvoorbeeld prettig vinden om in een café of eh, he, ergens in de stad eh, een ruimte willen zoeken waar ze gaan werken eh, dan is het ja, he, dat is natuurlijk een andere, toch weer net een andere omgeving. Ik kan me ook voorstellen dat bijvoorbeeld het wifi, een wifi bij iemand thuis misschien beter beveiligd is dan een wifi van een openbare gelegenheid, maar dat, dat kan ik ook niet beoordelen hoor, maar dat zou misschien kunnen. En het is in eerste instantie via een wifi verbinding vervolgens een VPN verbinding aanlegt, dat dat misschien nog impact heeft, maar dat, dat kan ik niet beoordelen. Maar dat zou een vraag zijn die ik zou hebben als het over eh, ja, VPN verbindingen gaat en veiligheid daaromtrent en eh, ja.

X: Als je dan bedenkt eh, wat zou de invloed van een VPN op zo een wifi netwerk kunnen zijn?

Y: Nou, ik denk niet zo zeer dat de VPN verbinding invloed heeft op het wifi netwerk, maar meer andersom. Dus als je een, een onveilige wifi eh, en misschien is dat helemaal onterecht hoor, ik ben helemaal niet technisch wat dat betreft, maar ik kan me voorstellen dat als je een minder veilige eh, wifi daar he, je hebt natuurlijk bijvoorbeeld en je kunt ook he als je een wifi verbinding hebt, kun je daar ook een wachtwoord aan koppelen. Nou, er zijn ook openbare wifi's waar je soms zonder wachtwoord gelijk kunt inloggen, kan me voorstellen dat dat misschien impact heeft he, op vervolgens de, de VPN verbinding. Dus stel dat bijvoorbeeld, je zit bijvoorbeeld in de trein en je doet het NS eh, de NS wifi, nou daar hoeft je niet een wachtwoord volgens mij voor in te typen. Nou, stel dat je dus dan vervolgens een VPN verbinding aanlegt, dan zou mijn vraag zijn is dat minder veilig dan dat ik thuis zou zitten op een netwerk waarvoor iedereen een wachtwoord moet invullen om toegang tot dat wifi netwerk te krijgen en vervolgens moet je nog een wachtwoord gebruiken om een VPN verbinding in stand te brengen. Dat zijn toch alweer twee hordes, in plaats van een zeg maar.

X: En in die situatie dat je in de trein zit, is het dan juist veiliger of minder veilig om een VPN verbinding te gebruiken?

Y: Ik zou zeggen minder veilig.

X: Sorry?

Y: Ik zou zeggen minder veilig, dat denk ik, dat zou mijn verwachting zijn.

X: Ja. Oké, duidelijk, zeker.

Y: Ja. Ja, heb ik dan nog meer over VPN, ik eh, ik weet niet, ik heb er nooit, ik heb er geen studies over gedaan, dus ik eh, het is voor mij allemaal abracadabra, het is mooi dat het er is.

X: Zeker, het is heel behulpzaam.

Y: Ja.

X: Oké. Dan waren dit tot zo ver mijn vragen. Heb jij nog vragen voor mij?

Y: Eh, nee, eigenlijk niet. Ik eh, ik hoop dat je input en dat je er een mooi resultaat uit kan krijgen. Want daar ga je nu mee aan de slag zeker.

X: Ja, ik zal even de opname stoppen in ieder geval.

C.13: Transcript Laypeople 2

Duration: 48 minutes

Language: Dutch

Number of drawings: 5

X: Wat is een VPN?

Y: Een VPN is een beveiligde tunnel waar je Internet eh, verkeer overheen gaat zeg maar vanuit jouw eigen computer eh, gaat, gaat dat wat je over het Internet verzendt via die tunnel naar een volgend punt. Maar goed, dat vanaf daar is het weer eh, die tunnel is natuurlijk wel beperkt tot je eigen computer. Het gaat niet door eh, zeg maar het is niet alsof je een e-mail stuurt eh, en je hebt je VPN aanstaan dat dan de e-mail door een hele tunnel van jouw computer naar de computer van eh, de server van degene die de e-mail ontvangt gaat. Maar het is een stukje eh, beveiliging van jouw computer naar het Internet, dan gaat het verkeer door die tunnel heen.

X: Oké. En je zegt dat de tunnel naar een volgend punt gaat, wat is dit volgend punt?

Y: Ja, dat weet ik ook niet precies. Ja, volgens mij, ik denk eh, tot het moment dat het echt zeg maar, ik denk tot aan de server.

X: Wat is een-

Y: De eerstvolgende server die je tegenkomt.

X: Wat is een server?

Y: Ja. Een server is eigenlijk gewoon een computer. Eh, en vaak is die server eh, volgens mij, nou, in dit geval sowieso zal het een server moeten zijn die verbonden is met het Internet. Servers hoeven niet per se met het Internet verbonden te zijn, maar in het kader van VPN eh, zou dat weinig zin hebben als dat niet zo is.

X: Ja.

Y: Eh, ja, een grote computer waarin data wordt verwerkt, opgeslagen en zo voorts.

X: Duidelijk. En u beschrijft de verbinding als een tunnel, wat bedoelt u met een tunnel?

Y: Ja. Ik zie het dan een beetje voor me als een soort beschermende hoes, die om de data heen gaat. Of ten minste, ja, dat, dat is, afgeschermd van eh, eh, ja, hoe ga ik dat eens even, eh, ik weet eigenlijk niet hoe ik dat beter moet, moet omschrijven als een tunnel. Ja, op de een of andere manier visualiseer ik het dan ook een beetje, maar-

X: Dat is geen probleem.

Y: Ja, als een soort bescherm laag, waardoor je die, waar zeg maar van buitenaf niet doorheen gekeken kan worden en waar die data dan doorheen gaat. In plaats van dat het gewoon open is. Op je computer. En ook het Internet, nou ja, kijk, dat is natuurlijk wat betreft een- Als je een VPN gebruikt en je bent verbonden ... (0:04:15) naar je Internetrouter en-

X: Ja.

Y: Daar op die Internetrouter kan het anders worden ingezien, gaat alle data open doorheen, normaal gesproken. Maar als je het via een VPN tunnel stuurt, dan gaat het, dan is het vanuit die, vanuit die router niet toegankelijk. Dan is daar zeg maar die beschermende laag eromheen. Dus zeg maar degene die toegang hebben tot de router, kunnen dan niet zien welke data vanaf jouw computer daar overheen gaat, want daar zit die VPN tunnel dan omheen. En daar kunnen ze niet door.

X: Duidelijk. En op wat voor manier kunnen ze dat dan niet zien?

Y: Ik denk dat dat een vorm van encryptie is, maar zeker weten doe ik dat niet.

X: Oké. En waarom gebruik jij een VPN?

Y: Nou-

X: O, sorry?

Y: Nou, ik zit even te denken of het voor, ja. Een beschermde laag, het is niet zo dat de data die daar inzit dan geencrypt is, alleen die laag daaromheen. Maar ik weet niet of dat nou encryptie is of een ander soort techniek.

X: Ja. Oké. Waarom gebruik jij VPN?

Y: Nou ja, wisselend eh, voor mijn eigen gebruik is dus inderdaad om die data af te schermen voor eh, mensen die per ongeluk toegang zouden hebben tot eh, tot de router. He, tot dezelfde Internetomgeving.

[0:05:43 until 0:05:54 has been omitted], dus daar heb ik geen zin om mijn data onbeveiligd overheen te sturen, daarom doe ik dat zelf. Voor [the professional services firm] geldt, speelt die reden natuurlijk ook eh, voor zo ver he, als je gebruik maakt van een openbare Internetverbinding. Overigens is het dan ook als ik het goed begrijp afgeschermd voor de Internetprovider, die kan dan ook niet zien wat je doet eh, online, als je dat via een VPN verbinding doet. Eh, en verder praktisch gezien doe ik het ook vanuit [the professional services firm] omdat ik op die manier toegang tot [an internal page] enzovoort. Zeg maar een aantal functionaliteiten binnen [the professional services firm] werken alleen maar als je via de VPN verbinding hebt gemaakt. Die [the VPN of the professional services firm].

X: Ja. En je noemde kort ook een openbare Internetverbinding, wat is-

Y: Ja.

X: De rol van de VPN hierin?

Y: Eh, zorgen dat eh, het Internetverkeer eh, dat wat jij over die Internetverbinding doet niet zichtbaar is voor anderen, gewoon het afschermen, in de tunnel houden, waar anderen niet bij kunnen. Want eh, nou ja, goed, je, je kan het ook wel zien als er demonstraties worden gegeven van eh, ik heb wel ook eens een demonstratie gezien in het theater dat eh, dat er werd gekeken naar hoe veilig iedereen met zijn dingen omging en dat dat gewoon eh, konden onderscheppen wat er eh, wat er allemaal eh, voor berichtjes, voor websites werden bekeken- Berichtjes verstuurd weet ik even niet zeker, maar in ieder geval de websites die werden bekeken en door wie en wat, wanneer eh, van mensen die op de eh, mensen die op de wifi hadden ingelogd eh, van de locatie. ...

X: Ja.

Y: Ja, digitaal dan.

X: Zijn er nog andere redenen waarom jij de [the professional services firm] VPN gebruikt?

Y: Ja, praktisch dus, om de systemen eh, omdat dat een voorwaarde is voor toegang voor een deel van de systemen. Maar verder gewoon veiligheid, afschermen.

X: Ja, oké. En welke handelingen voer jij uit om een VPN verbinding te maken?

Y: Eh, binnen [the professional services firm] is dat eh, eh, de god hoe heet het, o, nou heb ik mijn password incorrect ingetikt, zo, nou kan ik even kijken hoe het ook alweer heet. Eh, dan ga ik naar de [the VPN of the professional services firm], daar vul ik dan mijn eigen wachtwoord in eh, dan pak ik mijn token daarbij, [access token provider] token, en dan eh, het nummer wat op dat moment op die token staat dat vul ik daarachter in en dan enter.

X: Duidelijk. Kun jij meer vertellen over deze token?

Y: Ja. Deze token eh, die verandert elke 5 minuten geloof ik, geeft die een nieuwe code eh, dus dat is dynamisch. Eh, het is daarom ook belangrijk dat de batterij vaak wordt vervangen, want als die een beetje achterloopt met het genereren van die code, dan klopt de code niet en krijg je geen toegang meer. Eh, het is natuurlijk in het kader van de veiligheid dat er steeds een andere code verschijnt, dat dat niet dezelfde code is steeds. Dus eh, op het moment dat iemand ook eh, je wachtwoord zou kennen, zonder die token daarbij is het waardeloos en andersom ook. Met alleen de token zonder het wachtwoord eh, ja, kan je niet eh, die VPN verbinding eh, kraken of eh, gebruiken. Want nou ja, goed, zodra je die VPN verbinding open hebt staan heb je natuurlijk gewoon toegang tot meer [the professional services firm] informatie dan je anders hebt. Dus dat is eh, dat is vanuit dat oogpunt ook heel belangrijk, met name vanuit dat oogpunt voor deze computer.

X: Zijn er verschillende soorten tokens?

Y: Eh, ja, ik heb een eh, fysieke token, maar je kan ook eh, je kan ook een token generator op je telefoon zetten.

X: Oké, beide opties zijn beschikbaar binnen [the professional services firm] ook.

Y: Ja.

X: Oké. En op welke apparaten gebruik jij de [the professional services firm] VPN?

Y: Alleen op mijn laptop. [0:10:43 until 0:10:45 has been omitted].

X: Oké. En kun je aan mij uitleggen-

Y: ...

X: Sorry?

Y: Ik weet ook niet of het via de smartphone of daar überhaupt ook dezelfde functionaliteit voor beschikbaar is, maar goed. [0:11:00 until 0:11:04 has been omitted].

X: Ja. En kun je aan mij uitleggen hoe een VPN verbinding werkt? Ik kan mijn tekeningen hier even weghalen. En dan kunt u het whiteboard gebruiken als u dit wilt.

Y: Hmhm. [\[start drawing 13_1\]](#). Nou, ja, hoe ik het een beetje in mijn hoofd visualiseer, maar goed, of dat klopt, dat weet ik dus niet. Hallo. Nou. Eh, nee. Heb ik ook een gum?

X: Er is een mogelijkheid om eerdere handelingen ongedaan te maken door op het pijltje te klikken, alleen is de laatste lijn die je dan tekent het eerste dat-

Y: Ja, dat schiet niet op. Oké. Eh. Ja, ik denk dat dit dus dan de router is. Nou, die tools, dingen, is niet heel responsive.

X: O, oké, goed om te weten.

Y: ... lijntjes blijf zitten.

X: Het is niet mogelijk om op een ander vakje te klikken?

Y: Nou ja, ik heb het nu eh, o. a. Nee, ik zit nou, a, oké. Ik denk dus dat dit de router is. Router, of de server, dat weet ik niet zeker. O, dit zijn colors, nee. O, dus je moet niet, juist niet op dat pijltje gaan lopen klikken in dat vakje, maar op het dingetje zelf. [\[start drawing 13_2\]](#). Eh, nee, o. Eh, eh. O, nee. Zoiets.

X: Oké. En kun je mij uitleggen wat alle onderdelen van de tekening zijn?

Y: Nou ja, het begint dus eh, op je eigen device. De PC heb ik die maar even genoemd.

X: Ja.

Y: En eh, dat wat je daar doet zoals dit he, we zitten nou in een online eh, omgeving. Eh, dus alles wat he, wat je dus online doet vanaf je computer, dat gaat niet open over je eh, richting het, richting de router en richting het Internet, dat stukje is afgeschermd, dat gaat dus door die tunnel. Eh, zodat dat van buitenaf niet zichtbaar is voor anderen mensen die op die Internetverbinding eh, op die router of eh, anderszins op die Internetverbinding zitten. Ja, want er is natuurlijk ook dus de Internetprovider die die toegang tot het Internet verstrekt, die kan er evenmin bij. Dus dan is het waarschijnlijk tot de server van de Internetprovider. Eh, waar die tunnel toe loopt, dat dat laatste punt is. En ja, op dat moment dat het het Internet opgaat, dan eh, ja, dan, dan zijn die data niet meer afgeschermd. Volgens mij. Is dat zeg maar waar de bescherming ophoudt, daar ben je gewoon weer op het Internet. En eh, afhankelijk van natuurlijk he, dan ben je weer afhankelijk van het platform of dat een eh, HTTPS heeft of iets dergelijks, dan gaat de bescherming verder, maar dit gaat alleen maar op dat stuk. Dacht ik.

X: Oké. En stel dat je nu verbinding maakt, of je wilt toegang tot een interne applicatie, hoe zou dat in deze tekening eruit zien?

Y: Eh, ja, dan gaat de tunnel misschien tot die interne applicatie. [\[start drawing 13_3\]](#). Dus dan zou hierbij komen, de interne applicatie. Dat dat ook gewoon op het eigen netwerk is, op de eigen server.

X: Ja. Oké. Zijn er verder nog dingen eh, die je weet van hoe een VPN werkt?

Y: Nou, denk het eigenlijk niet, haha.

X: En wat is de rol van een router?

Y: Eh, die, jemel, dat is het Internetkastje. Eh, die dus de signalen vanaf jouw computer omzet denk ik op een manier dat ze het Internet opgestuurd kunnen worden. Ja, of die die verbinding eh, het is het toegangspunt, nou ja, goed, eerst gaat er natuurlijk nog een stukje kabel richting het kastje in de straat vanaf je eigen router, daar gaat het dan de systemen van de Internetserviceprovider op. Eh, en vanaf daar naar het wereldwijde web, het netwerk van computers. Waar we alles overheen sturen.

X: Dan nu een hele andere vraag. Wat is de invloed van een VPN verbinding op jouw computerbeveiliging?

Y: Eh, ik denk vrij weinig. Eh, ja, ik heb wel eens de illusie dat dat me dan ook een beetje beschermt eh, van buitenaf, nou ja, tegen hacken en dergelijke beschermt het niet. Op het moment dat iemand toegang heeft tot mijn computer en dat kunnen ze zich verschaffen of ik nou met een VPN of niet zit, nou ja, dat is afhankelijk van hoe goed ze kunnen hacken en de beveiliging op je computer zelf. Oe, wacht, mijn batterij is wel bijna leeg, momentje.

X: Ja.

Y: Eh, maar goed, ik hoop, ik heb dan wel een beetje de illusie dat er op het moment dat ik met het Internet communiceer via een VPN tunnel, dat het dat dan ook iets lastiger maakt voor iemand van buitenaf die toch

immers via het Internet op jouw computer zal moeten komen. Eh, dat het dat wel lastiger maakt. Want hoe komen zij dan die tunnel weer in als zij geen eh, authenticatie daarvoor hebben en is die tunnel dan inderdaad de enige, op dat moment de enige toegangspoort tot jouw computer, nou ja, het is in ieder geval voor eh, maar misschien dat dat ook weer afhangt van of je netwerkblocade hebt en of je dat aanhebt of niet. Maar goed, dat, dat zijn meer dingen dat ik hoop dat het ook iets doet, maar weten geen.

X: Ja. En heeft een VPN nog op een andere manier invloed op jouw computerbeveiliging?

Y: Eh, ja, volgens mij moet je ook iets eh, verandert het ook nog iets aan je proxy-instellingen, maar dat weet ik niet precies. Maar ik heb in ieder geval wel eens gezien dat er iets was met een proxy en dat dat weer anders moest vanwege de VPN. Maar hoe dat eh, hoe dat precies zit, geen idee.

X: Wat is een proxy?

Y: Ja, dat weet ik eigenlijk ook niet, haha.

X: Oké. Nog een vraag over de tekening. Wat zijn deze lijnen hier, aan de bovenkant. En de onderkant.

Y: Ja, eh, dat zijn invloeden van buitenaf. Eh, mensen die willen kijken eh, ja, of ten minste, indringers. En die dan afketsen.

X: Oké.

Y: Ik ben denk ik een beetje geïnteresseerd door wasmiddelreclames en dat soort dingen, haha.

X: Haha, oké. En dan een andere vraag weer. Met wat voor digitale dreiging heb jij op een normale dag te maken?

Y: Ja, daar merk ik gelukkig heel weinig van. Eh, dus eh, nou ja, goed, je hebt natuurlijk wel eens phishing mails die je ontvangt. Eh, ik krijg ook wel eens een melding, maar eigenlijk is het bijna altijd een false positive dat er iets van een programma, dat mijn malware beveiliging me ergens voor waarschuwt. Maar vaak is dat gewoon eh, in het kader van een update van een programma wat ik gewoon gebruik en eh, wat eh, betrouwbaar is. Eh, ja, heel af en toe raakt mijn eh, mijn malwarebeveiliging ook wel echt eh, echt iets op. Ik heb wel eens iets voorbij zien komen van een eh, een cryptocurrency-achtige scam. Ik weet niet meer precies wat dat was. Maar eh, dat dat in quarantaine werd gezet door mijn malwarebescherming, dacht ik dacht nou dat lijkt me wel heel goed.

X: Ja, zeker. En hoe verandert de soort digitale dreiging door een VPN verbinding?

Y: Eh, ja, je hebt dan minder, je hebt dan minder te maken met dreiging eh, qua eh, zeg maar, de dreigingen die, die op dat stukje waar de tunnel lopen spelen, daar heb je dan gewoon minder last van. Want normaal gesproken kan je daar dan ook gewoon worden bespioneerd en dat gaat dan niet meer. Dat is een van de makkelijkste eh, manieren om te hacken als ik het goed heb begrepen, dat je het Internet eh, verkeer afvangt. Dat je gewoon eh, doet, dat een hacker doet alsof hij de, de router is, het wifi access point, en dat die gewoon het verkeer naar zijn eigen access point eh, omleidt en daar alles kan inkijken. En ja, daar heb je dan, nou goed, dan gaat je verkeer daar misschien wel overheen, maar het zit in die tunnel, dus dan kan de hacker er alsnog niet inkijken. Tenzij die daar weer bijzondere manieren voor heeft, maar goed, dat eh, daar moeten we maar op hopen van niet.

X: Verandert de dreiging ook nog op een andere manier door de VPN verbinding?

Y: Eh, niet dat ik weet. Nou ja, wat natuurlijk wel zo is, is een VPN, dat hangt er een beetje vanaf, een VPN verbinding is natuurlijk wel iets wat ook weer een dienst is van een derde partij. Eh, dus als die niet betrouwbaar blijkt, ja, dan heb je dus je afgeschermd Internetverkeer altijd aan zo een derde partij beschikbaar gesteld en eh, je moet natuurlijk ook een beetje, ja, je moet daar dan ook weer een stukje vertrouwen hebben. Maar goed, als dat eh, onterecht blijkt te zijn, heb je dus je e-mailverkeer aan een onbetrouwbare derde partij ter beschikking gesteld. Dat is een potentiële dreiging.

X: Oké. Tot zo ver digitale dreiging. Heb jij ook te maken met een sociale dreiging op een normale dag?

Y: Nou ja, die phishing e-mails zijn natuurlijk een soort van social eh, hacking. Krijg ik niet vaak overigens. Eh, ja, als je in een openbare plek eh, zit, dan zou je mensen kunnen hebben die proberen mee te kijken op je scherm. Eh, ja, sociale dreiging, ja, als je je computer ongegrendeld achterlaat, is natuurlijk ook een stukje sociale dreiging voor de beveiliging. Eh, ja, ik ben heel eh, dwangmatig met eh, met het, het windowsknopje L, als ik een seconde wegliep van mijn computer. Eh, ja, dat zijn denk ik wel de grote sociale dreigingen. Ja, je kan natuurlijk zelf eh, meer sociale dreigingen creëren door allerlei dingen te gaan doorsturen naar je

Hotmail of je Gmail of whatever. Eh, of via WeTransfer en als dat soort eh, appjes(0:28:05). Maar ik weet niet of dat onder sociale dreiging valt. Dat is meer gewoon je eigen eh, dat je zelf beveiligingsrisico's creëert.

X: Ja, zeker. En hoe verandert de sociale dreiging door de VPN verbinding?

Y: Ja, niet. Eh, ten minste niet de voorbeelden die ik net noemde, wat dat eh, als iemand dan op die manier op je eh, op je device kan, ja, op de device is het allemaal aanwezig, daar verandert die tunnel niks aan. Eh, op het moment dat je het via een VPN tunnel op eh, op zo een filesharing platform gooit, ja, eenmaal op dat platform, is het gewoon daar en aldaar aan allerlei dreigingen onderhevig. Dus dat eh, nee, daar zie ik niet echt eh, hoe de VPN verbinding moet helpen. Het enige is misschien dat je, op het moment dat je, je moet actief die verbinding maken met VPN, misschien dat je daar een momentje zelf een beveiligingsawareness momentje ontstaat. Maar eh, verder zie ik het niet helemaal, beïnvloedt.

X: En wat bedoel je dat er een beveiligingsawareness moment bestaat?

Y: Nou ja, je gaat toch eh, die handelingen ondernemen om met een VPN te verbinden eh, hoeveel mensen ook weten van VPN, of hoe weinig, iedereen weet toch wel dat het ... beveiliging. Eh, dus dat dan zeg maar actief bezig bent met een beveiliging op je eh, op je computer voor je dataverkeer en dat je dan dus misschien ook wat meer eventjes van o ja, beveiliging is belangrijk achtig, onderbewust momentje hebt.

X: Oké. En als we nadenken over deze verschillende soorten dreigingen, wie of wat is dan de aanvaller die de dreiging veroorzaakt?

Y: Welke dreigingen? De sociale dreigingen of de dreigingen waartegen VPN beschermt of eh-

X: Alle dreigingen.

Y: Eh, ja, je hebt dan de dreigingen van hackerachtige dreigingen, mensen die echt op zoek zijn of een bot, whatever, die echt op zoek zijn naar informatie of naar eh, he, toegang tot eh, die zijn natuurlijk ook vaak eh, op zoek naar toegang tot betaalgegevens en dergelijke. Dus ja goed, kwaadwillenden die op zoek zijn naar eh, data die zij kunnen exploiteren. Eh, en andere dreiging is eh, het Internet eh, service provider en wat die allemaal, een nieuwsgierige Internet service provider die eh, die interessante dingen wilt doen met de data die over zijn netwerk gaan. Nou is dat, nou mogen ze dat inmiddels niet meer echt analyseren, niet deep packet inspection wat ze in het verleden hebben geprobeerd(0:31:36), maar misschien dat ze alsnog toch iets er mee doen, willen doen. Dan zijn er ook de eh, de dreiging van eh, van autoriteiten die eh, toegang willen tot die data en toegang afdwingen tot data via de Internet service providers. Eh, he, of die dingen opvragen. Eh, trouwens VPN geeft vaak ook een ander IP-adres dacht ik. Tenminste, veel VPNs doen dat. Dus dat maakt ook weer eh, dat zorgt er voor dat de herleidbaarheid, dat er minder herleidbaarheid is van je, van je acties op het Internet.

X: En wat is het gevolg ervan? Als de herleidbaarheid minder is?

Y: Eh, nou ja, dan kan je beter eh, dat wat, dat wat alleen jezelf aangaat tot jezelf houden. Of als mensen op jouw persoon willen gaan zoeken of willen gaan kijken wie een bepaalde actie eh, willen achterhalen wie een bepaalde actie op een platform eh, website, whatever heeft eh, eh, heeft verricht, kunnen ze dat niet zo makkelijk achterhalen wie dat dan is. Dus je bent eh, je bent anoniemer op het Internet. Totdat je er een gebruikersnaam en weet ik veel wat er aan koppelt, dan eh, wordt het een ander verhaal.

X: En als we dan terugkijken naar de tekening, op wat voor manier eh, valt het stukje herleidbaarheid er dan in?

Y: Ja, dat is natuurlijk, dat heb ik er nog niet in verwerkt want dat bedacht ik me net pas. [\[start drawing 13_4\]](#). O, dus dan hebben we ook die PC eh, hallo, heeft de PC een IP-adres, en de router heeft ook een IP-adres, hallo, en dan geeft de VPN- Eh, o wacht, nee dat kan ik wel hier doen he. Hallo, nee. Dus eh, iemand die dan eh, hier naar kijkt, naar een van deze eh, datastroompjes wat jij doet op het Internet, die ziet dan dit IP-adres, wat een IP-adres is dat is uitgegeven door de VPN en niet deze of deze. Dus die kan niet zien waar dat verkeer dan he, waar die handelingen dan vandaan kwamen. Ja, die komen dan uit bij een IP-adres van een eh, VPN dienstverlener en eh, daar loopt het dan dood.

X: Oké. En heeft de VPN dienstverlener in deze tekening een plaats?

Y: Nee, ja, die zit natuurlijk hier. Die maakt, die, die, die creëert die tunnel. [\[start drawing 13_5\]](#). Dus dat- Geen idee of het, of de VPN bij [the professional services firm] in eigen beheer is.

X: Oké. En we kwamen op dit onderwerp door te praten over hoe, of wat voor aanvaller achter een dreiging zit.

Y: Hmhm.

X: Hoe verandert de soort aanvaller door een VPN verbinding?

Y: Eh, dan verandert met name, ja, de locatie van de aanvaller. Dan gaan de aanvaller meer hier op het Internetdeel zich richten, alleen werkt, nou ja, goed, afhankelijk van hoe goed je daar herleidbaar bent, kunnen ze dan nergens heen. Of ze gaan zich direct richten op jouw computer, maar ze richten zich niet meer op dat stuk eh, zeg maar dat stuk Internet, router, Internet toegangspunt en jouw computer. Zeg maar dat stuk daartussen dat eh, daar kunnen ze dan weinig meer uithalen. Dus de, de met een auto rondrijden en wifi signalen onderscheppen en proberen in die wifi eh, apparaten te komen, dat heeft dan geen zin meer.

X: En verandert de soort aanvaller nog op een andere manier door een VPN verbinding?

Y: Geen idee, ja, dan moeten ze de tunnel in zien te komen waarschijnlijk.

X: Oké. En wat is de motivatie voor een aanvaller?

Y: Eh, ja, meestal eh, geldelijk gewin uiteindelijk denk ik dan echt, denk ik. Je hebt natuurlijk, ja, geen idee of bijvoorbeeld dingen als plaatsen van eh, eh, hoe noem je die eh, van bots die miningbots of iets dergelijks, of dat ook nog door een VPN wordt beïnvloed of dat dat wel gewoon kan. Moeten ze toch echt op je systemen komen. Eh, sorry, wat was de vraag ook alweer?

X: De vraag was wat de motivatie is voor een aanvaller.

Y: O, ja. Nou ja, uiteindelijk dus bijna altijd geldelijk gewin, ja, nieuwsgierigheid zou ook wel eens voorkomen. Eh, maar uiteindelijk is het gewoon een business. Denk ik.

X: Oké. En heeft een motivatie nog andere- Of heeft een aanvaller nog andere motivaties?

Y: Ja, dat hangt ervan af. Kijk, als het gaat om de ex die eh, haha, dat soort hacks heb je natuurlijk ook wel, mensen die eh, dus dat uit wrok of he, gewoon omdat je iemand persoonlijk wilt treffen. Ik denk dat dat wel echt een veel minder groot aantal is. Eh, ja, ja, er zijn, je hebt natuurlijk ook de aanvallers die simpelweg willen laten zien van he, dit is niet op orde. Je hebt ook ongetwijfeld ook hobby aanvallers, die gewoon willen kijken wat is er allemaal niet op orde en misschien dat ze dat vervolgens ook ... maar misschien ook niet je hebt natuurlijk de white hat hackers, die hebben ook een ander motief. Eh, he, meer om aan de kaak te stellen, beveiligingsproblemen. Ja, en dan, en dan weet ik even niet of je eh, overheids eh, instanties die toegang willen ook als aanvaller moet zien, want die gaan meestal wel via de juridische route en niet via een aanval. He, er zijn wel enige terughack eh, rechten, maar ja, dan moet je ze eerst wel hacken. Of dan moet je eerst een hacker zijn om zeg maar teruggehackt te mogen worden. Dus ja, dat zie ik dan niet direct als een aanvaller. Dan een overheids eh, instantie die eh, eh, een autoriteit, justitieachtige autoriteit die toegang verzoekt. Via meestal de Internetprovider.

X: En wat voor achtergrond heeft een aanvaller?

Y: Ja. Geen idee. Ze kunnen zichzelf eh, het een en ander hebben aangeleerd. Er zijn ook allerlei tools die je kunt eh, downloaden om allerlei hacking acties te kunnen uitvoeren. Eh, dus het hoeft niet per se een hoogopgeleid iemand te zijn. Het hoeft niet per se de, de grootste computerwhizzkid op aarde te zijn. Al zullen de echte goede hackers dat waarschijnlijk wel zijn. En qua achtergrond, ja, kijk eh, de Nigeriaanse prinses die allemaal eh, die via allerlei e-mail scams, via phishing prachtige erfenissen uitdelen, ja, dat zullen ongetwijfeld mensen zijn die zelf van een, ja, minder goede afkomst zijn zeg maar, van een vrij arme achtergrond komen. Maar goed, dat weet ik ook niet eh, weet ik eigenlijk niet. En hoogopgeleid ook niet per se. Het zijn gewoon slimme, dat zijn de slimme, manipulatieve mensen, maar dat zijn dingen waarmee ze zijn geboren, haha. Vaardigheden, als je het zo mag noemen. En eh, ja, en, en de hackers dat zijn eh, he, die echt op systemen proberen in te breken, qua achtergrond ja, dat kan van alles zijn. Ik denk, maar goed, ik kan me voorstellen dat, dat je je eerder geneigd bent om tot dat soort acties over te gaan, of zo een richting te kiezen als je zelf minder goed af eh, bent. Dus dan toch van een armere en meer uitzichtloze afkomst bent. Al kan het ook natuurlijk zijn dat je het gewoon leuk vindt en makkelijke manier eh, om eh, een makkelijke om interessante manier om aan geld te komen en dat je dat gewoon verkiest boven een regulier job. He, dus achtergrond van die mensen, ja, kan van alles zijn denk ik. Maar het zullen geen mensen zijn denk ik met een goede baan, want eh, dat slokt dan al je tijd op en dan heb je geen tijd om daarnaast nog eventjes te gaan zitten hacken.

X: Oké. En wat zou de impact voor [the professional services firm] van een aanval kunnen zijn?

Y: Ja, enorm natuurlijk. Omdat er gewoon heel veel vertrouwelijke eh, gegevens binnen de systemen van [the professional services firm] aanwezig zijn. De eh, ja, alle cliëntdossiers, alle e-mailcorrespondentie, zo veel vertrouwelijke informatie. Dat zou echt, dat kan desastreus zijn. Als daar toegang tot wordt verkregen. Ja, dan is het vertrouwen, dat heb je allerlei confidentiality obligations waar je, waar je problemen mee hebt. Dus contractuele aansprakelijkheden eh, buiten het feit dat je reputatie naar de haaien is en eh, en alle klanten waarschijnlijk weglopen. Want op het moment dat je informatie niet veilig is bij [0:43:12 until 0:43:17] eh, maar goed, betrouwbaarheid en vertrouwelijkheid is natuurlijk ook een eh, heel belangrijk element. Ja, dat, afhankelijk van hoe ver de aanval gaat he, tot waar de aanval eh, weet te doordringen, desastreus.

X: Oké. En kan eh- Als we naar de VPN verbinding zelf gaan kijken, hoe veilig is een VPN verbinding?

Y: Ik heb geen idee hoe veilig deze VPN verbinding is of hoe veilig een VPN verbinding in het algemeen is. Het wordt altijd verkondigd dat dat de manier is om eh, om je Internetverkeer eh, af te schermen, maar of dat nou helemaal ondoordringbaar is, dat weet ik niet.

X: Oké. En zijn er manieren waarop je kan denken waardoor een VPN verbinding niet geheel veilig is?

Y: Nou ja, net zoals dat je op andere systemen kunt eh, kunt inbreken, kan je waarschijnlijk ook op een VPN tunnel inbreken. Ik bedoel overal zijn zwakheden, dus waarschijnlijk ook in die, die schil die daarom heen zit.

X: En als je nadenkt over deze onveiligheden, veranderen jouw handelingen hierdoor?

Y: Eh, nee, want dit is vooralsnog het enige wat ik voorhanden heb hiervoor. Dus ja, als er geen ander alternatief is, eh, ja, dan ga ik ook niet eens op zoek naar eh, van goh, is het allemaal wel 100% veilig, want ik kan niet, niets anders doen.

X: Ja.

Y: Behalve ja, behalve al je verkeer eh, apart nog een encrypten, maar goed, dan weet ik ook niet waar ik moet beginnen. Behalve dat je altijd dan via HTTPS eh, moet werken, maar dan heb je nog steeds dat stukje zwakte van jouw computer. Want dat HTTPS begint natuurlijk pas op dat platform. Daar moet je dan eerst nog heen. Of nou, nee, HTTPS gaat misschien wel verder dan dat. Nou ja, dus dat eh. Ja, dat is het lastige, ja, dan ga je misschien meer focussen op HTTPS, zorgen dat je alles eh, op die manier ook afschermt. Dus dat je dus, nou goed, nou zullen de meeste online platforms hebben dat ook wel, meestal is het toch op het platform veilig, afhankelijk van de aanbieder die daarachter zit.

X: Oké. Dit waren tot zo ver mijn vragen.

Y: Hmhm.

X: Heb jij nu nog dingen van een VPN verbinding waar we het niet over hebben gehad?

Y: Nee, er schiet me nou niet direct iets te binnen. Ja, ik vroeg me nog af dat ik dacht van goh, is er ook een risico dat die VPN verbinding, dat die hele tunnel wordt verlegd, dat het ergens anders heen gaat. Maar eh-

X: En hoe bedoel je dan dat die ergens anders heen gaat?

Y: Nou, dat het eindpunt hier verandert. Oftewel dat het alsnog via, ja, als je dit weet te, weet te kapen, dan kan je ook de data die eruit komt misschien naar je eigen punt, naar je eigen Internet access point leiden, en het daar alsnog aflezen. Dat weet ik niet hoor, maar goed dat eh, is iets wat ik me ineens bedacht.

X: Duidelijk. Zijn er verder nog andere dingen?

Y: Nee.

X: Oké. Eh, dan waren dit dus tot zo ver mijn vragen en dit gedeelte van het interview. Heb jij nog vragen voor mij?

Y: Eh, ja natuurlijk, het antwoord op alle vragen wat jij, die jij mij gesteld hebt, haha. In plaats van mijn gissingen.

X: In kan eh, in eerste instantie zal ik even de opname stoppen.

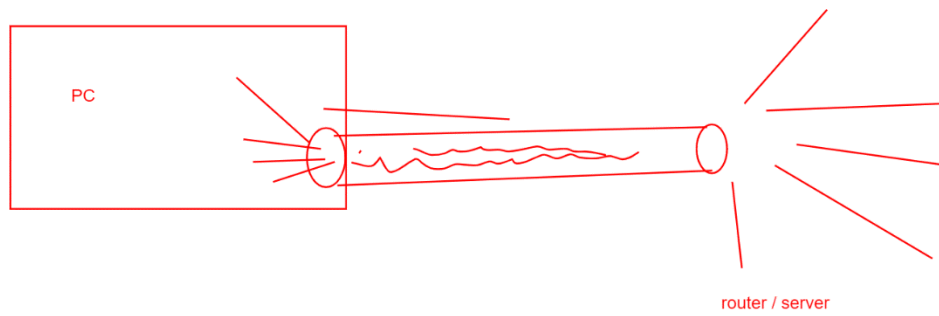


Figure C.13.1: Drawing 13_1

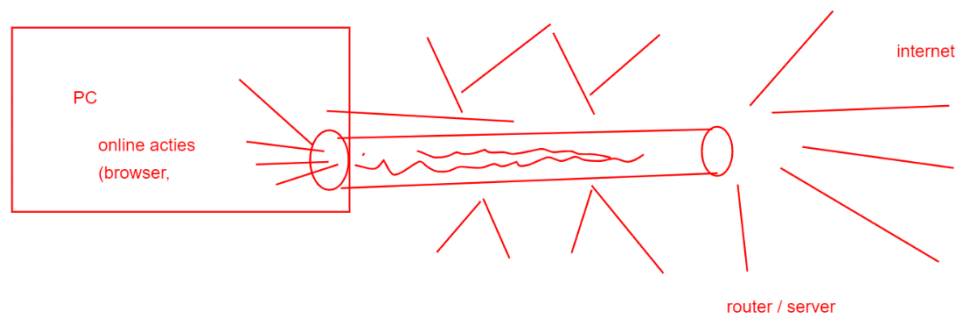


Figure C.13.2: Drawing 13_2

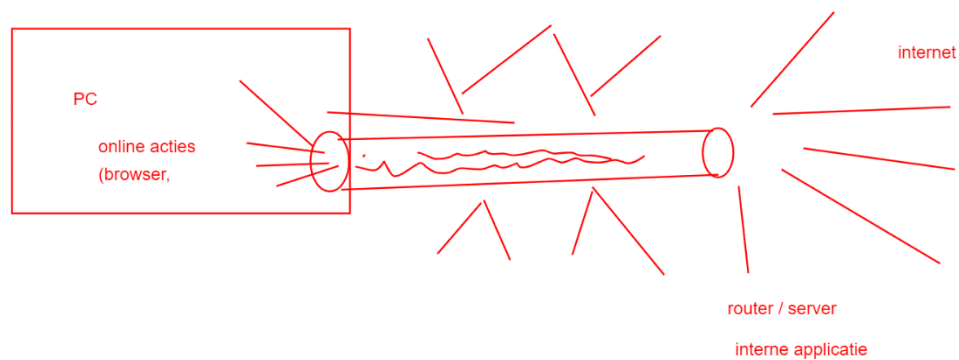


Figure C.13.3: Drawing 13_3

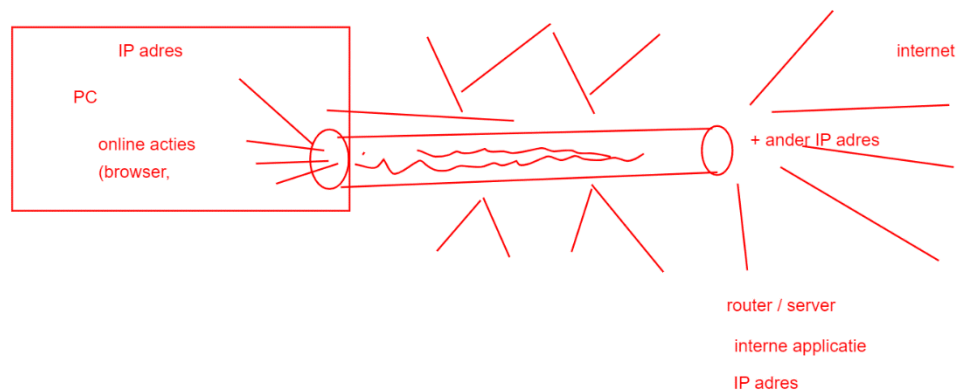


Figure C.13.4: Drawing 13_4

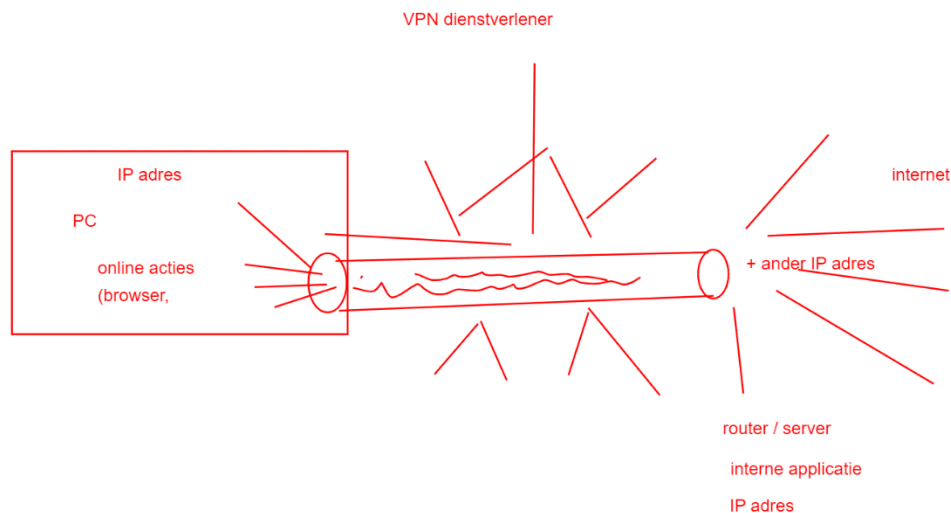


Figure C.13.5: Drawing 13_5

C.14: Transcript Laypeople 3

Duration: 13 minutes

Language: Dutch

Number of drawings: 0

X: Dan begin ik nu met de vragen van het interview.

Y: Ja.

X: Kan jij aan mij uitleggen wat een VPN is?

Y: Nou, dat is een goede vraag. Volgens mij is VPN de ja, ik hoop echt niet dat ik heel erg verkeerd zit, maar de verbinding die, of het netwerk of in elk geval iets wat ik nodig heb om contact te maken met het netwerk van [the professional services firm]. En daarin de schijven en programma's die ik nodig heb om mijn werk te kunnen uitoefenen.

X: Oké. En kan je voorbeelden geven van de programma's die je nodig hebt?

Y: Eh, nou, ik gebruik, als ik op VPN inlog dan maak ik gebruik- Waar ik dan gebruik van maak bedoel je?

X: Ja.

Y: Dan maar ik gebruik van [department] systemen, dus van [an internal page], [an internal page], ook [an internal page], dus het portal waar ik telefoonnummers en zo op zoek. SharePoint wat we vanuit [department] gebruiken, waar [0:01:45 until 0:01:46 has been omitted] en dat soort dingen op staan. Mijn schijven, de schijven die ik deel samen met collega's. Eh, waar we allebei gebruik van maken, waar onze teams gebruik van maken. Eh, dus eigenlijk eh, nou ja, alle plekken waar data op staat, die in een beveiligde omgeving staat.

X: Oké. Zijn er naast toegang tot deze applicaties ook andere redenen waarom jij een VPN gebruikt?

Y: Nee. Eigenlijk niet. Nee. Als ik mijn computer opstart kan ik gewoon bij mijn mail. Dus als ik alleen bij mijn mail, met mijn mail werk, dan gebruik ik het niet. Eh, en als ik op mijn persoonlijke schijf moet. Maar als ik op eh, alle andere dingen die ik net noemde, dan log ik in. Maar er is geen andere reden waarom ik dat zou doen, nee.

X: Oké. En je noemde net al dat je inlogt op VPN. Welke handelingen voer jij als gebruiker uit om een VPN verbinding te maken?

Y: Eh, ga ik naar rechts onderin de hoek, naar mijn Interneticoontje, dat klik ik dan open, dan doe ik [the VPN of the professional services firm], en dan eh, krijg ik een schermje waarin ik mijn wachtwoord en mijn VPN code moet invoeren. En dat doe ik dan. Ik heb nog zo een, zo een token, zo een klein grijs dingetje. Omdat ik eigenlijk nooit eh, de moeite heb genomen om dat te verwisselen voor een app, wat ik wel zou moeten doen. Maar die voer ik dan in en dan klik ik op oké en dan doet die het meestal.

X: Oké. En op welke apparaten gebruik jij een VPN?

Y: Op mijn laptop. En alleen op mijn laptop.

X: Oké. Zijn er nog andere mogelijke apparaten waarop je de VPN kan gebruiken?

Y: Niet dat ik weet. Ik denk dat het op de telefoon zou kunnen, maar dat wordt wel erg klein. De dingen die ik daar die ik zoek, die ik gebruik met VPN zijn over het algemeen grotere databestanden of dingen waar ik veel informatie vind, dus dat zou ik niet zo heel handig vinden op mijn telefoon. Als het zou kunnen, weet ik niet.

X: Ja. Oké. En kan je aan mij uitleggen hoe een VPN werkt?

Y: Nee. Denk ik. Nou ja, ik log in en op het moment dat ik erin zit, dan eh, dan heb ik het idee, maar dat kan ik helemaal verkeerd zien, dat ik door een bepaalde eh, dat er een bepaald iets open gaat, waar je dan doorheen komt, waar je niet doorheen komt op het moment dat je niet de VPN hebt ingelogd.

X: Oké.

Y: Ik heb het idee dat ik hele domme antwoorden geef, is dat zo?

X: Nee hoor, helemaal niet.

Y: O, oké.

X: Helemaal niet. En zou je enig idee wat er achter de schermen gebeurt? Als je een VPN verbinding maakt?

Y: Eh, nee, ja, ik denk dat de toegang wordt opgeheven tot iets waar ik niet bij kan zonder VPN. Maar, nee, wat er achter de schermen gebeurt weet ik niet. Zal een soort van geautomatiseerde eh, ja, ik stel het me zoiets voor van hekjes die dan omhoog gaan als je erdoorheen kan. Dat dat geautomatiseerd zeg maar is ingesteld, op het moment dat ik met de juiste code inlog.

X: Oké. Duidelijk. Eh, ja, normaal zou ik nu vragen voor een tekenopdracht, dat zag je misschien ook in het toestemmingsformulier. Alleen omdat je niet in de situatie, of in de omgeving kan komen, laat ik voor nu de tekenopdracht even zitten. Dan ga ik voor naar de volgende vraag. Eh, wat is de invloed van een VPN verbinding op jouw computerbeveiliging?

Y: Eh, dat, ik denk dat die heel groot is, de invloed. Dat zou voor mij overigens nog groter mogen. Bij mijn vorige werkgever moest ik ook op mijn mailbox met VPN inloggen en vooral, ik ben dan vooral bang dat als mensen mijn computer zouden vinden, of hij blijft ergens onbeheerd achter of wat dan ook, dat mensen toegang krijgen tot informatie, waar ze niet bij kunnen zonder VPN. Dus ik zou eh, ja, wat mij betreft zou de VPN verbinding nog sterker mogen zijn. Of vaker mogen worden toegepast. Maar dat is ook een beetje omdat ik dat zo gewend ben.

X: Ja, en je vindt het dus veiliger om wel een VPN te moeten gebruiken?

Y: Dan niet bedoel je?

X: Ja.

Y: Ja, zeker.

X: En waarom vind je dat veiliger?

Y: Omdat ik het idee heb, maar misschien is het schijnveiligheid, dat op het moment dat je dat de kans dat iemand namens mij, die daar niet bij hoort, bij die informatie kan, eh, dat de kans kleiner is dat dat lukt, met een extra barrière, zoals VPN.

X: Oké. En dan een hele brede vraag, met wat- O.

Y: Sorry. Nee hoor, ga maar door.

X: Oké. Met wat voor digitale dreiging heb jij op een normale dag te maken?

Y: Waarschijnlijkheid met een hoop meer dreiging dan ik mezelf, dan waarvan ik me bewust ben. Maar waarvan ik me bewust ben is dat ik eh, nou ja, als ik mijn computer op mijn werkplek laat staan, dat iemand die mee zou kunnen nemen en daarmee wat zou kunnen doen. Met de gegevens die daarop staan dan natuurlijk. Eh, en anders, en wellicht ook via het web, maar daar ben ik niet zo goed in thuis. Eh, dat mensen, nou ja, online op de verbinding kunnen binnendringen en bij informatie kunnen waar ze niet bij zouden moeten mogen.

X: En verandert de soort dreiging door een VPN verbinding?

Y: Eh, nee. De dreiging zelf niet. Alleen de mogelijkheid dat er daadwerkelijk iets mee gebeurt misschien wel.

X: En op wat voor manier verandert de mogelijkheid dat er iets mee gebeurt door een VPN verbinding?

Y: Eh, nou dat het een, omdat het een extra barrière is die moet worden ingevoerd en moet worden toegepast om tot bepaalde databronnen te komen, of bestanden te komen.

X: En dat geldt voor zowel via het web wat je noemde als fysiek?

Y: Ja. Voor mij zit daar niet een heel groot verschil in. Maar dat is puur omdat ik niet zo goed weet welke dreigingen via het web bij mij terechtkomen.

X: Ja. Heeft de VPN op nog een manier invloed op de dreigingen via het web?

Y: Eh, nee, ik zou het niet zo goed weten wat, eigenlijk.

X: Oké.

Y: Dus misschien wel, maar dat is mijn gebrek aan kennis van dreigingen via het web.

X: Prima. Oké. Eh, en als we dan over deze dreigingen nadenken, wie of wat is dan de aanvaller die achter de dreiging zit?

Y: Eh, ja, dat kan van alles zijn. Eh, nou ja, dat maakt op zich niet eens zo veel uit. Waar ik met name angstig voor ben is wat er dan vervolgens mee gebeurt. Omdat ik vanuit mijn functie natuurlijk met heel veel persoonsgegevens te maken heb, die niet altijd eh, even positief zijn. Soms ook wel, maar die gaan niemand anders wat aan. En het effect daarvan. En wie dat zou moeten zijn, dat kan ik eigenlijk nooit bedenken. Wie daar wat mee zou willen of wie daar kwaad mee zou willen. Eh, dus ik kan niet echt een, of iets benoemen wat daar, wat dat zou willen eh, doen.

X: Oké. En wat zou de motivatie van een aanvaller kunnen zijn?

Y: Eh, ja, chantage, of eh, informatie verspreiden over mensen die eh, waarmee iemand iemand anders wil schaden, denk ik. Of om er zelf beter van te worden.

X: Ja. En wat voor achtergrond heeft een aanvaller?

Y: Nou, dat kan volgens mij iedereen zijn die iets wil of er een bepaald belang bij heeft. Ik zou niet specifieke achtergrond kunnen bedenken, behalve dan dat ze enigszins thuis is in hoe die die data moet verkrijgen eh, via ofwel het web of via op een andere manier.

X: Oké. En heeft de VPN verbinding nog invloed op de achtergrond van een aanvaller?

Y: Nou, als die weet hoe het werkt en weet hoe die het moet manipuleren, dan waarschijnlijk wel. Eh, want als je weet hoe je dat kun manipuleren, dan is het waarschijnlijk een verbinding die schijnveiligheid met zich meebrengt en niet een eh, iets wat elke willekeurige aanvaller tegenhoudt.

X: Ja. En heeft de VPN verder nog invloed op de soort aanvaller?

Y: Eh, nou, dat denk ik niet.

X: Oké. En wat zou de impact van een aanval kunnen zijn?

Y: Eh, een impact van een aanvaller zou kunnen zijn. Dat die de informatie die die vindt verspreidt of tegen iemand gebruikt. Of gebruikt in het voordeel van eh, een andere partij. Dus denk bijvoorbeeld aan eh, [0:11:52 until 0:12:05 has been omitted].

X: Oké, duidelijk. En als we gaan kijken naar de VPN verbinding zelf, hoe veilig is een VPN verbinding?

Y: Ik heb geen idee eigenlijk. Of dat heel veilig is. Voor mij voelt dat heel veilig, omdat ik iets moet doen wat iemand anders niet kan doen. En wat ik ook niet kan doen als ik niet de middelen bij me heb om een verbinding te kunnen maken. Maar of het echt veilig is, dat weet ik niet.

X: Duidelijk. Oké. Eh, dit waren tot zo ver mijn vragen. Zijn er nog dingen die nu niet ter sprake kwamen, die wel belangrijk zijn om te vertellen over een VPN?

Y: Nou, voor mij niet. Ik ben alleen benieuwd naar hoe veilig een VPN verbinding eigenlijk is, weet jij dat toevallig?

X: Oké. Ik zal eerst even de opname stoppen.

Y: Ja.

C.15: Transcript Laypeople 4

Duration: 16 minutes

Language: Dutch

Number of drawings: 0

X: De eerste vraag. Kunt u mij uitleggen wat een VPN is?

Y: VPN betekent Virtual Private Network, als het goed is. Eh, en dat betekent eh, dat eh, de data is afgeschermd voor ongeoorloofd aftappen of inzien van onbevoegden.

X: Oké. En hoe is de data afgeschermd?

Y: Hoe dat technisch werkt weet ik niet.

X Oké. En waarom gebruik jij een VPN?

Y: Eh, in eerste plaats omdat dat de enige manier is om op het [the professional services firm] netwerk eh, te komen. En in die context gebruik ik ook een VPN verbinding.

X: Oké. Zijn er andere redenen waarom u de [the professional services firm] VPN gebruikt?

Y: Nogmaals eh, het is zeg maar de enige mogelijkheid om op een veilige manier op het [the professional services firm] netwerk te komen. Geen andere redenen.

X: Oké. En op welke manier bedoelt u hier op een veilige manier?

Y: Wat ik bedoel met een veilige manier is dat als je gebruik maakt van eh, eh, nou ja, eh, andere wifi of netwerk toegangen die buiten de beveiligde omgeving van [the professional services firm] zit, dat je toch op een veilige manier zeg maar het bedrijfsnetwerk kan benaderen.

X: Oké. En welke handelingen voert u uit om een VPN verbinding te maken als gebruiker?

Y: Betekent dat ik eh, zeg maar naar het icoontje van de netwerkverbinding ga, rechter eh, muisklik eh, dan heb je bovenaan eh, de optie eh, voor het kiezen van eh, de VPN verbinding, die klik je aan, dan verschijnt er een regel waar je een wachtwoord op kan eh, je opent desbetreffende tool, die [access token provider] tool he, dus je elektronische token op je mobiel, die genereert iedere minuut een nieuwe cijfercombinatie, en die voeg je toe aan je eigen eh, aan je eigen wachtwoord. He, dus het is een combinatie van een eigen wachtwoord en een gegenereerd eh, gegenereerde cijfercombinatie via een elektronische token op je mobiel.

X: Ja, duidelijk. En is er nog een andere manier naast uw mobiel om de elektronische token te verkrijgen?

Y: Eh, vroeger was die er. Maar dat is in principe afgeschaft. Het werkt nu gewoon via de mobiel.

X: Oké.

Y: Dus er zijn geen- Vroeger hadden we van die nou ja, vergelijkbaar met de kastjes die je van de bank krijgt om eventueel nog toegang te krijgen via die oude manier via Internet naar de bank toe, maar die hebben wij niet.

X: Ja, oké. En op welke apparaten gebruikt u een VPN?

Y: Op eh, in feite twee apparaten. Op mijn laptop, als ik buiten [the professional services firm] omgeving werk en via mijn eh, tablet en via mijn [mobile phone].

X: Oké. En kunt u aan mij uitleggen hoe een VPN verbinding werkt?

Y: Eh, ik neem aan dat in feite eh, eh, he, ik kan niet uitleggen hoe dat technisch werkt. Laten we daar gewoon even kort en simpel over zijn.

X: Oké. Heeft u enig idee wat er zich achter de schermen afspeelt?

Y: Eh, ik neem aan dat de data encrypted wordt die in die zin gewoon niet eh, te kraken, te herleiden is voor mensen die op dat moment meekijken met de verbinding. Maar dat is een veronderstelling en geen kennis.

X: Ja. Duidelijk. Eh, dan een andere vraag. Wat is de invloed van een VPN verbinding op uw computerbeveiliging?

Y: Voor mij niet waarneembaar. Ik weet dat die er is en je vertrouwt erop dat dat het doet. En dat eh, eh, als het niet doet, wat wel een keer voorkomt, op dat moment heb je dan ook geen toegang tot het [the professional services firm] netwerk.

X: Duidelijk. En heeft de VPN nog op een andere manier invloed op uw computerbeveiliging?

Y: Niet dat ik weet.

X: Oké. Dan een hele brede vraag. Met wat voor digitale dreigingen heeft u op een normale dag te maken?

Y: Eh, nou, ik denk dat het [the professional services firm] netwerk op een hele goede manier is eh, eh, beveiligd. Eh, het komt hoogst zelden voor dat er een keer een, een bepaalde spammail in je mail komt, maar dat is eh, echt een eh, een, een uitzondering. He, dus de firewalls, die doen op, die doen hun werk zeg maar goed. Ik heb nog niet meegemaakt binnen [the professional services firm] dat we eh, he, dat we onze systemen zijn overgenomen door, door anderen of dat er op afstand datamanipulatie of wat dan ook heeft plaatsgevonden. Dus met andere woorden, ik voel dat wij in een hele veilige eh, eh, omgeving werken.

Dat kan natuurlijk allemaal schijnveiligheid zijn, dat kan ik niet beoordelen. Maar als gebruiker voelt het goed beveiligd aan.

X: Ja. En heeft de VPN invloed op de soort dreiging?

Y: Eh, daar heb ik de technische kennis niet voor om dat te kunnen eh, beoordelen.

X: Oké. En dit ging eerder over digitale dreiging, heeft u ook te maken met sociale dreiging op een normale dag?

Y: Nee.

X: Oké, duidelijk. Eh, dan werden er net wel enkele aanvallen genoemd, eerder ook wat u vertelde. Eh, wie of wat is de aanvaller die de dreiging veroorzaakt?

Y: Ik zou het niet weten. Dat is buiten mijn waarnemen.

X: Oké. En wat zou de impact van een aanval kunnen zijn?

Y: De impact van een aanval zou kunnen zijn dat je business interruption eh, eh, hebt. Eh, dus met andere woorden dat je op dat moment je bedrijfsvoering niet kan eh, continueren. Het kan zijn dat er gevoelige data van [the professional services firm] eh, bij derden komt, eh, eh, te liggen. Nou ja, het kan zijn dat je he, [0:08:47 until 0:08:50 has been omitted]. Er zijn natuurlijk heel veel dreigingen eh, mogelijk die impact hebben op je bedrijfsvoering.

X: Ja, oké. En is er een manier waarop de VPN impact hierop heeft? Of ja, invloed op de impact?

Y: Nee, kijk, jij stelt mij een hoop technische vragen he, eh, waar ik gewoon het antwoord niet op heb.

X: Oké.

Y: Kijk, he, ik ben gewoon een [role] die maakt gebruik van systemen he, maar de techniek daarachter van VPN ja, die weet ik niet. En eerlijk gezegd eh, nou ja, boeit dat je als gebruiker ook minder. Laat ik het even zo zeggen.

X: Ja, dat snap ik. Dat snap ik. Dan heb ik nog één vraag over de VPN zelf. Hoe veilig is een VPN verbinding?

Y: Moet ik je antwoord op schuldig blijven.

X: Oké, prima. Dan waren dit tot zo ver mijn vragen. Zijn er nu nog dingen die u weet over VPN en die nu niet naar voren zijn gekomen?

Y: Nee. Het is meer een geïnteresseerde vraag van mij naar jou toe-

X: Ja.

Y: Van eh, he, van kijk, tot op heden stel je relatief eh, technische vragen. Eh, eh, waarvan ik me afvraag van ja, zit je dan bij de juiste doelgroep om deze vragen op los te laten. Dat intrigeert mij gewoon.

C.16: Transcript Laypeople 5

Duration: 36 minutes

Language: Dutch

Number of drawings: 6

X: Wat is een VPN?

Y: Nou, VPN, dat is de connectie waarmee onze computer eh, jeetje, hoe moet ik dat, dan moet ik even, even uitleggen natuurlijk. De eh, de veiligheids eh, eh, connectie zeg maar, tussen, tussen mijn laptop en het [the professional services firm] netwerk. Eh, he, dus een soort schild he.

X: Oké. En wat bedoelt u met een schild?

Y: Nou ja, een soort, een soort eh, eh, veiligheids eh, ja, hoe noem je dat. Eh, veiligheidssysteem voor [the professional services firm]. He, dat we eh, veilig onze data heen en weer kunnen sturen. He, dat je daardoor op een veilige wijze kan inloggen eh, op, op alle systemen eh, van het [the professional services firm] netwerk. Nou, op het moment dat je geen connectie maakt met VPN, dan eh, dan, dan kom je niet verder.

X: Ja. En hoe bedoelt u dat u niet verder komt?

Y: Eh, nou ja, goed, dat is er veel data, de [the professional services firm] data, die is op dat moment niet eh, niet bereikbaar, niet beschikbaar.

X: Oké. En u zegt veilig data heen en weer sturen, op wat voor manier bedoelt u veilig?

Y: Eh, nou veilig in de zin van he, je bent op afstand verbonden met elkaar, eh, en eh, we willen niet dat data die [the professional services firm] heeft dat die bij derden terecht komt. Daarvoor eh, moeten wij in een veilige omgeving werken, dus waar, waar derden eh, geen toegang tot hebben. Daarvoor wordt, wordt VPN gebruikt.

X: Oké. En weet u hoe derden geen toegang kunnen hebben tot de verbinding? Tot de data?

Y: Eh, nou ja, het meest logische wat ik daarin kan bedenken is wij moeten een bepaalde code invoeren eh, en anderen hebben die code niet.

X: Ja. Oké. En waarom gebruikt u VPN?

Y: Eh, om in te kunnen eh, om, om bij de data eh, te komen waar wij toegang toe moeten hebben. Die ik nodig heb om mijn werk te kunnen doen.

X: Ja. Zijn er nog andere redenen waarom u een VPN gebruikt?

Y: Nee, voor mij niet. Eh-

X: Oké.

Y: Ik weet niet of die er zijn, maar-

X: Ja.

Y: Kennelijk wel, als je zo de vraag stelt.

X: Niet per se hoor-

Y: Een aantal van mijn systemen die draaien enkel als ik ingelogd ben op het netwerk. Eh, dus he, onder andere via de Citrix omgeving, op het moment dat wij geen connectie hebben, dan eh, dan kan ik, dan kunnen wij ons werk niet uitvoeren. Daarnaast onze shared drive, die eh, die heeft ook eh, he, daar kom je ook niet op zonder VPN, zonder het netwerk.

X: Ja, oké. En als gebruiker, welke handelingen voer jij uit om een VPN verbinding te maken?

Y: Eh, nou, ik eh, ja, dat moet je natuurlijk heel gedetailleerd weten gok ik.

X: Ja, wat u kunt vertellen.

Y: Haha. Nou ja, rechtsonder klik eh, klik ik op zo een mooi icoontje en dan geef ik aan eh, mijn wifi icoontje zeg maar, en dan geef ik aan dat ik met [the VPN of the professional services firm] wil verbinden eh, he, dan open ik mijn eh, [access token provider] token, mijn [access token provider] [the professional services firm] software token, eh, nou dan vul ik mijn code in, ik zeg connect en vervolgens gaat het helemaal goed komen.

X: Oké. En u zegt uw software token, zijn hiervoor nog andere mogelijkheden?

Y: Ja, je hebt ook een hardware token. Eh, de ervaring leert dat dat eh, een mindere connectie geeft. En een deel van mijn team heeft daarmee te maken. En die hebben daardoor eh, veel, veel connectie issues.

X: Wat bedoelt u daarmee, dat het een mindere connectie geeft?

Y: Eh, dan wordt die, dan wordt die met enige regelmaat uitgelogd.

X: Oké. Oké. En op welke apparaten gebruikt u de [the VPN of the professional services firm]?

Y: Eh, enkel op mijn laptop. Op mijn telefoon eh, daar heb ik, daar raadpleeg ik enkel met name mijn mail. Eh, en dan, en [conferencing software] eh, he, de [conferencing software] omgeving en dan heb je geen [the VPN of the professional services firm] nodig.

X: Oké. En kunt u aan mij uitleggen hoe een VPN verbinding werkt? Als u wilt kunt u hiervoor het whiteboard gebruiken. Ik zal mijn tekeningen weghalen.

Y: Nou, dat vind ik een hele leuke vraag. Even kijken hoor. Dus dan moet ik hier een tekeningetje gaan maken, oe. [\[start drawing 16_1\]](#). Eh, even kijken. Nou, dan hebben we, nou ja, allemaal verschillende gebruikers. He, ik teken er even een paar. Eh, en we hebben hier, hebben we zeg maar de router eh, van eh, [the professional services firm]. Ik had het wel dichterbij mogen tekenen. Eh, he, dus dan heb je eh, tweerichtingsverkeer. Hebben ze eh, nou ja, ik log in op, op, eh, op mijn laptop en dan gaat die heen en weer zenden. Eh, he, dus dit is de [the professional services firm] router, tja, schitterend mooi getekend. Eh, nou ja, goed, en op het moment dat ik de code heb ingevoerd eh, dan, dan heb ik uiteindelijk connectie. En tot dat moment heb ik geen connectie. [\[start drawing 16_2\]](#). Dus er zit hier zeg maar een soort eh, een soort schild voor. Dat is eh-

X: Ja.

Y: Even heel plat gezegd zo, zo kijk ik ernaar.

X: Ja, prima. En waar in deze tekening zouden wij de [the professional services firm] omgeving vinden, de interne applicaties waar u bij moet komen?

Y: [\[start drawing 16_3\]](#). Eh, hier. Dus hier, ja, jeetje. Eigenlijk zou ik hem dan overnieuw moeten tekenen. [\[start drawing 16_4\]](#). Maar hier heb je een soort eh, he, dit is dan je, je VPN. He, dat is een soort schild, noem ik het maar even. En hier heb je eh, alle data van [the professional services firm]. Eh, is natuurlijk een hele grote server. Volgens mij staat die in [country]. Eh, in ieder geval voor Nederland. En eh, op het moment dat je he, je logt in op VPN eh, en vervolgens he, op het moment dat het oké is, dan mag je door. En kan je bij de data.

X: En u noemt een server, wat is een server?

Y: Eh, ja, dat is een eh, ik ben zo IT onderlegd he, not. Eh, eh, ik zou dat omschrijven als een eh, een IT systeem waar eh, waar alle data opgeslagen wordt. Eh, en die gekoppeld kunnen worden met andere servers eh, waardoor je onderling data kan uitwisselen.

X: Ja. En waar ik deze tekening vinden we een server?

Y: Eh, ja, voor mij zit dat allemaal hierin. Maar misschien eh, zouden we dat wat groter moeten tekenen.

X: Ja, duidelijk. En wat is het verschil tussen een router en een server?

Y: Eh, een router, ja, voor mij zou dat zijn, een router is eh, datgeen waarmee je een connectie maakt tot het Internet. He, dus dat staat bij mij hier thuis. Eh, en een server is he, dat is wat ik net zei, de, de eh, dat systeem he, waar eh, waar de gegevens van [the professional services firm] worden opgeslagen.

X: Ja. En dit is ook de router van [the professional services firm] zei u toch?

Y: Nee, dat heb ik nog niet gezegd. Maar eh, ik zou wel zeggen dat dat zo zou zijn. [\[start drawing 16_5\]](#). Dat dat hier, ja, weet je, ik denk dat je onderaan de streep zal er eh, he, dan heb je hier bij wijze van een serverpark eh, he, dus daar zit de connectie met eh, even kijken, dan heb je hier, nou ja, verschillende serverparken, ongetwijfeld. He, dus eh, zo zit het allemaal een beetje met elkaar verbonden.

X: En eh, als dit niet een router is, wat is dat dan?

Y: Eh, moeilijke vragen joh, voor mij als en IT-leek. Nou ja, dat zou prima, ik, ik zou zeggen van nou ja, goed, hier thuis heb ik een router. He, dus daarmee maak ik verbinding met het Internet. Nou, in principe, [the professional services firm] maakt ook verbinding met het Internet, dus dan zou er prima een router kunnen zijn. Eh, nou ja, goed, daarvoor zit die, zit die, database, of sorry, de VPN connectie, nou goed eh, er wordt hier onderling allerlei data wordt er uitgewisseld. Eh, dus dan zou dat prima ook een router kunnen zijn, ja.

X: Oké. En u tekent verschillende serverparken zei u, waarom tekent u verschillende serverparken?

Y: Eh, risico mitigerend.

X: Op wat voor manier mitigeren zij risico's?

Y: Eh, door elkaars back-up te zijn.

X: Hebben die serverparken nog een andere functie?

Y: Ongetwijfeld. Eh, weet je, de, de systemen draaien daarop, je zal er een, een stukje data storage hebben he, waar alle gegevens eh, en, en, van [the professional services firm] staat opgeslagen. Eh, nou, ik weet voor een van de systemen die wij gebruiken he, daar eh, daar hebben we ook een server en een back-up server. He, dus, nou ja, die lopen synchroon met elkaar, gaat het mis met de een he, dan hebben we de ander nog om eh, om daar eh, vanuit te kunnen werken. Eh, dus onderaan de streep eh, voorkomen we daarmee dat we data, gegevens kwijt kunnen raken. En eh, heb je dat wel nodig.

X: Oké. En stel we gaan nu naar een andere locatie eh, stel je bent bijvoorbeeld in een café, verandert er dan iets aan deze tekening?

Y: Eh, wauw, eh, nou, misschien wel, maar hetgeen wat, kijk, in een café, als je in een café inlogt, eh, he, formeel gezien he, moet je goed checken of dat je eh, of dat je een veilige verbinding hebt. [\[start drawing 16_5\]](#). Eh, nou zit ik even te twijfelen he, stel je voor he, dan, dat dit eh, je laptop is he, dus dan eh, dan is dit de vraag van normaal gezien is dit de router thuis. Eh, en op het moment dat dat in ene keer de café eh, router gaat worden, geeft dat dan een veiligheidsissue. Als het goed is niet. Eh, want je hebt nog steeds die VPN connectie eh, waardoor je eh, waardoor je veilig kan eh, kan Internetten. Anders zou je bijvoorbeeld ook niet op een Schiphol of waar dan ook eh, connectie kunnen maken.

X: Ja. En je zegt dat je moet controleren of het een veilige verbinding is, wat bedoel je daarmee?

Y: Nou, ja, heb ik altijd gehoord. Goed eh, nou, kijk, als ik kijk bij mijn thuissituatie dan eh, dan wordt er eh, dan heb ik meerdere, ten minste, heb ik maar een persoon die daar op inlogt zeg maar, eh, he, die wachtwoord heeft tot de betreffende router. Eh, bij een café verbinding of nou, Schiphol, whatever, eh, dan heb je eh, meer mensen die op eh, op hetzelfde netwerk inloggen. Eh, ik weet niet of dat per definitie of dat, dat eh, eh, veilig is of niet. Ik ga ervan uit dat op het moment dat je je VPN gebruikt, dat dat veilig is.

X: En wat is dan het verschil tussen de situatie dat je geen VPN gebruikt en dat je wel VPN gebruikt?

Y: Nou, op het moment dat ik wel VPN gebruik, dan kan ik bij al mijn eh, mijn systemen en programma's. Op het moment dat ik dat niet doe, dan kom ik daar niet bij. Dus dan heb ik geen eh, geen toegang tot de beveiligde gegevens van [the professional services firm].

X: Ja, en als je dan denkt op het gebied van de veilige verbinding-

Y: Ja, waar doel je op?

X: Wat is dan het verschil tussen een verbinding met VPN en zonder VPN?

Y: Eh, zonder VPN heb je eh, vermoedelijk niet altijd een veilige verbinding. En met eh, ja, voor de, voor de programma's eh, en gegevens van [the professional services firm] heb je dat wel. Maar is dat ook maar weer net hoe je er mee omgaat.

X: Ja. Oké. Dan ga ik door naar de volgende vraag. Wat is de invloed van een VPN verbinding op jouw computerbeveiliging?

Y: Wat de invloed is van een VPN op mijn computerbeveiliging. Eh, eigenlijk verschrikkelijk. Op het moment dat ik, dat ik, dat mijn VPN uitvalt he, en, en, nou neem even wat ik eerder al aangaf, een deel van het team werkt met een, een hardware token eh, he, als dat uitvalt, dan heb je geen connectie tot de programmatuur die wij gebruiken. Nou, dat kost tijd en zorgt voor een inefficiënte geheel. He, dus vanuit dat perspectief heeft dat invloed.

X: Ja, oké. En heeft de VPN op een andere manier ook nog invloed op jouw computerbeveiliging?

Y: Eh, niet dat ik weet.

X: Oké. Dan een hele brede vraag. Met wat voor digitale dreiging heb jij op een normale dag te maken?

Y: Met wat voor digitale dreiging.

X: Ja.

Y: Eh, nou, eigenlijk best nog wel wat, zegt de theorie. Eh, wij hebben de mogelijkheid op eh, eh, [0:19:49 until 0:20:31 has been omitted]. Wij hebben eh, te maken met een stuk databreach he, op het moment dat eh, dat we per ongeluk met de verkeerde partij communiceren. Eh, nou ja goed, en er is altijd een risico he, we hebben eh, pak en beet zo een paar honderd e-mails per dag die er binnen mijn team worden behandeld eh, en er zit altijd een risico, een behoorlijk risico op, dat je, dat je toch een eh, een soort van paard van Troje binnenhaalt.

X: Ja. Oké. En hoe verandert de soort dreiging door een VPN verbinding?

Y: Eh, niet.

X: Duidelijk. Oké. En dan een andere vraag. Met wat voor sociale dreiging heb jij op een normale dag te maken?

Y: Eh, sociale dreiging. Wat verstaan jullie daar normaal gezien onder?

X: Alle dreigingen die niet digitaal zijn en die eh, waar jij op een normale dag te maken hebt als een [the professional services firm] medewerker.

Y: Eh, nou ja, goed, onze, wij zijn een communicerend team he, dus wij eh, wij eh, hebben veel contact met klanten, [0:22:11 until 0:23:05 has been omitted]. Maar goed, daar nemen wij, in beiden gevallen nemen wij daar specifiek actie op, om te voorkomen dat dat nog een keer gebeurt en he, dat collega's of wij zelf onheus worden bejegend.

X: Ja. Oké. En heeft een VPN verbinding invloed op deze sociale dreigingen?

Y: Eh, nee, geen enkele.

X: Oké. Wel vervelend om te horen, dat wel. Ik kan me voorstellen dat dat niet leuk is.

Y: Nou ja, weet je, dat is eh, tegelijkertijd, aan de ene kant is dat het spel dat we spelen en eh, het werk dat we doen. Eh, tegelijkertijd, ja, blijft het het minst nette kant van de andere kant. Gelukkig komt het, het is net niet dagelijks dat je ermee te maken hebt, maar eh, ja, weet je, dat, het is, soms zijn mensen ook

gewoon bang [0:24:12 until 0:24:19 has been omitted]. Ja, weetje, dat eh, daar hebben we gewoon mee te maken. Covid helpt daar niet bij, zeg maar.

X: Nee, dat kan ik mij voorstellen. Dat is vervelend. Oké. En dan terugkijkend naar de digitale dreiging die je eerder noemde, verandert eh, daarbij de soort aanvaller- Of wie of wat is de aanvaller die de dreiging veroorzaakt, bij de digitale dreigingen?

Y: Eh, digitaal. Dat is eh, nou ja, zowel klant als [the professional services firm] medewerker, maar met name klant. Eh, en nee sorry, digitale dreiging dat is even, excuus, nee dat is eh, ja, netjes gezegd de hacker die eh, die bijvoorbeeld een klantsysteem over heeft genomen of daarin heeft ingebroken. Dat kan zijn, een tijd geleden hebben we te maken gehad met [0:25:24 until 0:25:40 has been omitted]. He, dus dat zou een optie kunnen zijn. Maar ja, digitaal, digitale dreiging is voor mij wat meer de boefjes en de, he, dat ze echt eh, inbreuk maken op onze systemen, danwel op de systemen van de klant. En op basis daarvan gewoon [0:26:05 until 0:26:18 has been omitted].

X: Ja, oké. En wie of wat is dan de aanvaller die de dreiging de veroorzaakt? De boefjes?

Y: Ja, die ken ik niet persoonlijk. Maar je hoort tegenwoordig, je leest veel over eh, Russische, Chinese hackers, maar goed, dat gaat wat mij betreft meer over, over landen level. Ik zou eh, ik zou eh, gewoon zeggen iemand die slim is eh, met IT en eh, denkt hiermee op een goede manier weg te kunnen komen.

X: Ja. En wat is de motivatie van een aanvaller?

Y: Eh, ja, dat kan meerdere zijn. He, dat kan bijvoorbeeld zijn om eh, eh, zelf geld binnen te halen. [0:27:09 until 0:27:14 has been omitted]. Dat is eh, misschien wel om een bedrijf eh, schade toe te brengen. Kan zijn dat ze, dat ze bijvoorbeeld een systeem hacken he, of een hele computer, of een range computers eh, en eh, die vrijgeven op het moment dat er losgeld wordt betaald. Eh, dat.

X: Oké. En wat voor achtergrond heeft een aanvaller?

Y: Eh, weet ik niet. Dat kan eh, dat kan van iedere klasse zijn. Ik denk niet dat ik eh, dat ik die aanvaller op dit moment kan identificeren.

X: Wat bedoel je ermee dat die van iedere klasse kan zijn?

Y: Je hebt meerdere sociale klassen. Ik heb eh, ik heb geen idee van eh, wie de, wie de uiteindelijke aanvaller van eh, van eh, voor een [the professional services firm] zou kunnen zijn.

X: Oké. En verandert de soort aanvaller door een VPN verbinding?

Y: Eh, nou ja, we maken het in ieder geval een stukje moeilijker. Dat de persoon of, of het type verandert. Eh, ja, dat eh, dat weet ik niet.

X: Oké. En op wat voor manier wordt het moeilijker gemaakt?

Y: Nou ja, je creëert een soort schild om, om in te loggen op het [the professional services firm] netwerk. En eh, daarmee maak je het moeilijker om, om aan de gegevens van [the professional services firm] te komen.

X: Ja. En wat zou de impact van een aanval kunnen zijn?

Y: Nou ja, de impact zou kunnen zijn dat ze een heleboel gegevens van [the professional services firm] eh, sorry, dat ze die eh, bloot kunnen leggen eh, eh, kunnen verspreiden, dus je hebt een gigantisch datalek. Eh, het zou kunnen zijn dat ze diverse systemen, eh, ... of weet ik veel wat he, dat ze die kunnen hacken en, en lamleggen en eh, vele collega's hun werk niet kunnen doen. Het zou kunnen zijn dat eh, ook specifieke collega's daardoor bijvoorbeeld geraakt worden. Persoonsgegevens, data breach, had ik al genoemd. Dat eh, dat eh, nou goed, het ransomware he, dat er een stukje of een deel van [the professional services firm] gegijzeld wordt. Eh, maar onder aan de streep, ja goed he, eh, het is ook een heel groot imagoschade wat er mee te maken heeft. Of waar je dan mee te maken hebt.

X: Ja, oké. En als we dan kijken naar de VPN verbinding zelf, hoe veilig is een VPN verbinding?

Y: Dat weet ik niet.

X: Zijn er redenen die je kan bedenken waarom een VPN verbinding mogelijk niet veilig is?

Y: Eh, ja. Eh, simpel voorbeeld. [0:30:50 until 0:31:34 has been omitted]. En goed, vanuit dat perspectief ben ik eh, ben ik dingen gaan benaderen, van ja goed, alles is te hacken, alles is te kraken. Eh, maar je zal er continue eh, eh, als bedrijf mee bezig te moeten zijn om dat, om dat eh, om dingen veilig te houden en lekken te voorkomen.

X: Ja, zeker. En heeft encryptie zelf nog iets te maken met de VPN verbinding?

Y: Eh, dat weet ik niet precies.

X: Oké. Zijn er nog andere redenen waarom jij kan bedenken dat een VPN verbinding mogelijk niet veilig is? Of minder veilig?

Y: Eh, nou ja, weet je, je hebt, je hebt zelf een eh, het is de combinatie van een eigen password met een eh, random eh, random getal van zes cijfers eh, ja, ik weet niet of dat onder aan de streep, daarmee creëer je een heleboel combinatiemogelijkheden, ik weet niet of dat voldoende is, of dat daar nog over nagedacht moet worden. He, ik heb ook wel eens gehoord dat je daar bijvoorbeeld een dubbele eh, eh, he, codering in zou moeten gebruiken, om het nog veiliger te maken. Eh, maar daar weet ik het fijne niet van verder.

X: Ja. En wat bedoel je met een dubbele codering?

Y: He, dat je, dat je eigenlijk twee keer een eh, verschillende VPN moet openen.

X: Oké, ja. En wat voor eh, effect zou dan hebben?

Y: Dat je eh, het eh, nou ja goed, je, je maakt het iemand die kwaad wilt maak je het verschrikkelijk veel moeilijker, doordat je de keuze, de keuze van eh, ten minste, dat veel eh, je hebt twee lagen waar je doorheen moet zeg maar. Nou goed en als eh, [the professional services firm] IT goed oplet dan eh, dan kan men een keer door de eerste heen komen, maar zeker niet door de tweede.

X: Ja. En wat bedoel je dan met deze lagen?

Y: Met die lagen, dat je twee verschillende eh, VPN eh, connecties opbouwt. Eh, he, en je zou dus ook twee keer een password moten invoeren om bij de gegevens te komen eh, en daarmee zou je het veiliger maken. Maar goed, verder weet ik daar ook eh, de details, of het exacte verhaal niet van.

X: Ja, oké. Dan waren dit tot zo ver mijn vragen. Heb jij vragen voor mij? Of zijn er nu nog dingen van VPN die je denkt zijn belangrijk om te noemen, maar komen niet ter sprake?

Y: Eh, nee. Maar zat ik een beetje goed?

X: Ja, nee, zeker. Ik zal de opname even stopzetten.

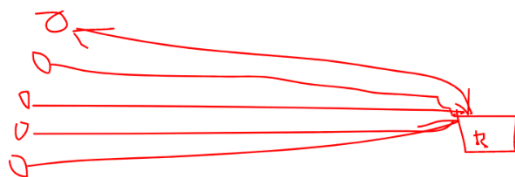


Figure C.16.1: Drawing 16_1

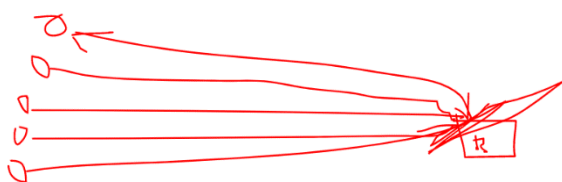


Figure C.16.2: Drawing 16_2

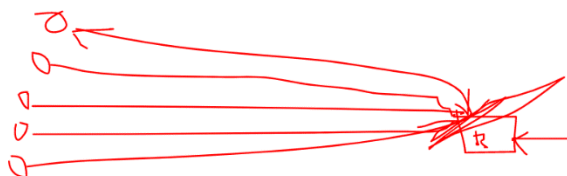


Figure C.16.3: Drawing 16_3

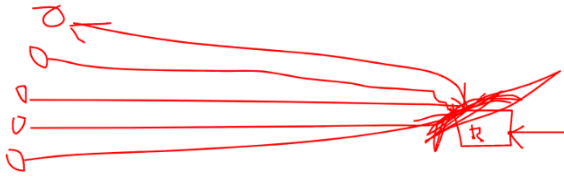


Figure C.16.4: Drawing 16_4

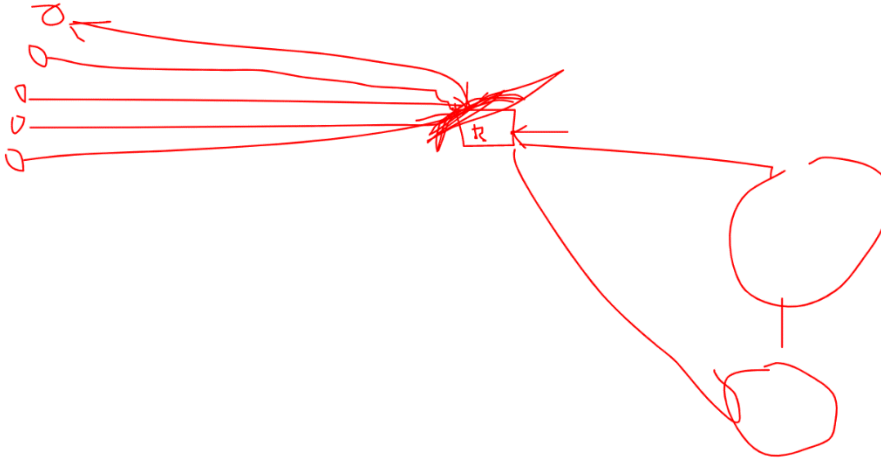


Figure C.16.5: Drawing 16_5

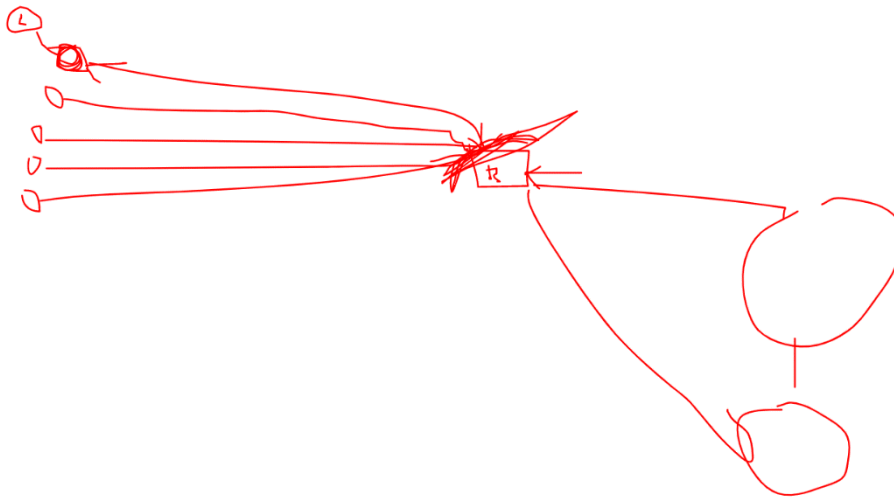


Figure C.16.6: Drawing 16_6

C.17: Transcript Laypeople 6

Duration: 35 minutes

Language: Dutch

Number of drawings: 5

X: Kunt u aan mij uitleggen wat een VPN is?

Y: Eh, dat hoop ik. Eh, voor zo ver ik weet is het een Virtual Private Network en wordt het gebruik om te zorgen dat je eh, binnen een netwerk eh, op in ieder geval op een veilige manier berichten kunt versturen door dan wel versleuteling meestal toe te passen of eh, en in ieder geval de berichten eh, los van het onderliggende netwerk te kunnen versturen.

X: En wat bedoelt u met los van het onderliggende netwerk?

Y: Nou dat eh, het eh, de bedoeling is dat op het moment dat iemand een bericht verstuurd vanuit eh, [the professional services firm] bijvoorbeeld eh, over het Internet. Dat eh, anderen op het Internet de berichten eh, niet kunnen onderscheppen.

X: En waardoor kunnen zij die berichten niet onderscheppen?

Y: Eh, ja, dat is een goede vraag, want dat is heel technisch volgens mij. Eh, volgens mij komt dat omdat je de berichten eh, via bepaalde lijnen laat lopen waar eh, anderen niet eh, bij kunnen komen. Dus afgesloten.

X: Ja. Oké. Eh, om welke redenen gebruik jij een VPN?

Y: Eh, ik gebruik VPN omdat ik daarmee veronderstel dat eh, mijn berichten niet eh, of in ieder geval niet heel eenvoudig door eh, door derde partijen kunnen worden eh, onderschept en gelezen. Als ik gebruik maak van VPN eh, over een VPN over Internet, ik weet dat VPN ook in een aantal gevallen gebruikt wordt binnen bedrijven, om in interne netwerken om meer beveiliging te krijgen. Maar ik gebruik het met name omdat ik ervan uitga dat de VPN die wij gebruiken ook de berichten versleuteld, dus als iemand al berichten zou kunnen onderscheppen, dan eh, dan zou die ze in ieder geval niet kunnen lezen, omdat die geen sleutel heeft om ze te ontsleutelen.

X: Ja, oké. En wat bedoelt u met eh, met het gebruik van VPN in interne netwerken?

Y: Nou ja, je kunt VPN natuurlijk ook binnen je eigen eh, organisatie gebruiken eh, zodat je dus eh, op het eigen netwerk, het lokale netwerk, eigenlijk op dezelfde manier berichten verstuurd. Waarbij je dus ook beveiliging maakt en ik neem aan dat je dat doet omdat als er iemand toch van buitenaf op jouw interne netwerk zou komen, dat die niet zomaar eh, gegevens kan eh, kan lezen.

X: En zijn er nog andere redenen waarom u een VPN gebruikt?

Y: Nee, dat is voor mij eigenlijk de belangrijkste reden, gewoon extra beveiliging, waardoor je in ieder geval geen risico loopt dat anderen jouw berichten kunnen onderscheppen. Of in ieder geval niet kunnen lezen als ze ze al onderscheppen.

X: Ja. Oké. Dan de volgende vraag. Als een gebruiker, welke handelingen voert u uit om een VPN verbinding te maken?

Y: Eh, dat eh, is in dit moment via een eh, het opstarten van eh, remote access en het gebruik op een mobiele telefoon van eh, van de, de access code. Dus ik log in via eh, op mijn eh, op mijn laptop. Dan moet ik een pincode invoeren en vervolgens een code die iedere minuut wijzigt. En daarmee leg ik de verbinding.

X: Oké. En hoe komt u aan deze code die iedere minuut wijzigt?

Y: Dat is een app op de telefoon. [access token provider] heet die geloof ik. En dat is een, een app die door eh, [the professional services firm] is verstrekt. Ter vervanging van voorheen eh, want hiervoor hadden we natuurlijk de mooie key waar die code op het schermje kwam, dat ding dat je aan je sleutelbos bij je had. En dit is de digitale variant.

X: Oké. En op welke apparaten gebruikt u een [the professional services firm] VPN?

Y: Eh, ik gebruik hem alleen op de laptop van [the professional services firm]. [0:06:47 until 0:06:58 has been omitted].

X: Oké. En kunt u aan mij uitleggen hoe een VPN verbinding werkt? U kunt hiervoor het whiteboard gebruiken-

Y: Hmhm.

X: Ik zal mijn tekeningen weghalen.

Y: Ja. Eh, hoe die werkt. Hoe ik hem opstart en hoe dan vervolgens mijn berichten gaan volgens mij, of-

X: Ja.

Y: [start drawing 17_1]. Oké. Ik heb dus mijn eh, mijn laptop. Dit moet mijn laptop voorstellen. Eh, die maakt verbinding met de VPN van [the professional services firm], even kijken hoor, kon ik tekst erin zetten makkelijk, o, die moet ik niet hebben. Even kijken hoor, kon ik de tekst selecteren.

X: Door op de pen te klikken en dan op een T te klikken-

Y: O, ja, ik heb hem.

X: En dan ook een vierkant te tekenen en daarin kunt u typen.

Y: O, oké. En- Even kijken hoor, dan moet ik weer tekenen. [start drawing 17_2]. En de VPN gaat dan terug en die vraagt dan een, ja, mijn mobiele telefoon, nou dit moet mijn mobiel voorstellen.

X: Ja.

Y: Eh, die vraagt dan de code op, en die code eh, die tik ik hier in en dat is de code die dus iedere minuut wijzigt en die geeft dan, laat ik even een ander kleurtje kiezen, en die geeft dan die code op. Dan is de VPN eh, verbinding wordt geopend. Even lastig om even snel te tekenen met dat ding. [\[start drawing 17_3\]](#). En dan eh, dan wordt zeg maar de VPN verbinding open gezet. Eh, ik heb aan mijn kant een sleutel. Volgens mij heet dat de private key als ik het goed heb. Nou, het vakje moet wat groter, maar- De private key, dus het bericht wordt dan hier ingezet en dan wordt die versleuteld en dan wordt die eigenlijk de VPN verbinding ingezet. En aan de andere kant heb ik dan hier ergens de ontvanger, wie dat dan ook is. Iemand die ook op het [the professional services firm] netwerk zit. En die krijgt dan eh, die heeft ook de, uiteraard, een key. Met het bericht gaat dan de public key mee als ik het goed heb. En dan kan degene die aan de andere kant zit, die krijgt dan het berichtje binnen, of in ieder geval eh- [\[start drawing 17_4\]](#). Volgens mij wordt het zelfs opgeknipt in verschillende pakketten. En die kan dan die pakketten via die, door die keys aan elkaar te koppelen, weer ontsleutelen. En lezen.

X: Ja.

Y: Ik kan hem geloof ik niet aanpassen, of wel. Nou, je begrijpt wat ik bedoel.

X: Ja, zeker.

Y: En die VPN verbinding die zorgt er in ieder geval voor volgens mij ook dat die pakketten worden gecreëerd en dat de pakketten weer ergens op, weer bij elkaar worden gevoegd.

X: Oké.

Y: Zo is ongeveer hoe ik het begrijp.

X: Ja. Oké. Een vraag hierover-

Y: Hmhm.

X: Voor de duidelijkheid. Is het eh, de bedoeling dat dit apart staat?

Y: Nou, dit is eigenlijk de tool, het tooltje dat ik opstart.

X: Oké.

Y: [\[start drawing 17_5\]](#). Het tooltje wat opgestart wordt om deze verbinding te openen en die verbinding maakt dan gebruik, ja, misschien moet ik, is het handig om nog even een pijltje inderdaad erbij te zetten. Dus eigenlijk zorgt deze ervoor eh, zal ik het er even bij zetten in tekst, zo.

X: Ja, ik kan het nog lezen.

Y: Ja. Dus die zorgt voor het openen van de verbinding en op het moment dat ik dan ga versturen, zorgt die verbinding ervoor dat die pakketten worden verstuurd en versleuteld zijn en aan de andere kant weer ontsleuteld kunnen worden.

X: Ja. En u zei dat de [the professional services firm] ontvanger iemand is die ook op het [the professional services firm] netwerk zit-

Y: Hmhm. Ja.

X: Wat betekent dit?

Y: Dat dat iemand is die dus eh, maar dat weet ik dus niet zeker, maar daar ga ik eigenlijk vanuit, dat die ook de VPN eh, verbinding heeft met [the professional services firm], maar dat hoeft trouwens, nee, dat is trouwens niet waar wat ik nu zeg, want volgens mij kan iemand gewoon de berichten lezen, ook al is die niet via VPN ingelogd. Maar dat weet ik niet zeker.

X: Ja. En hoe zou het werken als iemand die niet is ingelogd op de VPN wel de berichten kan lezen?

Y: Dan zou het volgens mij niet goed werken. Dus ik, ik denk dat als deze berichten via VPN verzonden worden, dat dat dan wel, want de [the professional services firm] ontvanger kan ook een systeem zijn he, in dit geval. Eh, want ik gebruik VPN bijvoorbeeld om verbinding te maken met Citrix en ik kan niet in Citrix als ik geen VPN verbinding heb. Dus de [the professional services firm] ontvanger, zit blijkbaar op het VPN netwerk, want anders kan die ook niet zeggen dat ik eh, dat die geen verbinding kan maken.

X: Ja. En zijn er nog meer voorbeelden waarbij de [the professional services firm] ontvanger een systeem is?

Y: Eh, ja, er zijn meer eh, meer systemen eh, ja, er zijn heel veel systemen die alleen maar via VPN benaderbaar zijn, bijvoorbeeld [an internal page] omgeving, waar je [0:15:44 until 0:15:48 has been omitted], kun je alleen maar via VPN benaderen.

X: Ja. En een [the professional services firm] ontvanger, kan dat ook een persoon zijn?

Y: Ja, dus dat zou ook een persoon kunnen zijn, alleen dat, dat is even voor mij een beetje onduidelijk nu, omdat ze heel veel dingen voorheen achter de VPN hadden staan en eh, bijvoorbeeld mail kon je alleen maar benaderen als je op het eigen netwerk zat of via een VPN was ingelogd, alleen dat hebben ze eh, ertussenuit gehaald vanwege de corona ellende. Waardoor blijkbaar de eh, de bandbreedtes enorm werden belast, dus ik weet dat dat in het begin, dat daar bepaalde dingen bij VPN weggehaald zijn, [conferencing software] is ook zo een voorbeeld.

X: Ja.

Y: Dus die zitten niet in het VPN netwerk, dus daar kan, zou in theorie dus iedereen gewoon mee kunnen kijken.

X: Ja. Oké. En eh, stel we wisselen van locatie, we gaan met de eigen laptop bijvoorbeeld in een café zitten-

Y: Hmhm.

X: Verandert dat iets aan deze tekening?

Y: Nee, in principe niet, want de VPN verbinding eh, die leg ik via het Internet. Dus in deze maakt het natuurlijk niet uit of dat het Internet is bij mij hier of eh, op een wifi eh, ergens bij een café. Ik zal alleen wel weer een VPN verbinding op moeten zetten om te zorgen dat ik in ieder geval eh, veilig ben. Het enige wat ik me kan voorstellen, maar ik weet dus niet waar de VPN ergens start, is dat er iemand tussen jou eh, ergens jouw wifi kan eh, kan omzeilen of kan afluisteren.

X: Ja.

Y: Maar dat weet ik niet of dat kan.

X: Oké. En dan ga ik door naar een volgende vraag.

Y: Hmhm.

X: Wat is de invloed van een VPN verbinding op jouw computerbeveiliging?

Y: Eh, ja, wat, wat versta je onder computerbeveiliging?

X: In de brede zin.

Y: Oké. Mijn computer op zich wordt niet beveiligd door VPN. Dus als ik mijn computer eh, aanzet en ik doe niets met, en ik zet VPN aan, dan kan iedereen nog steeds op mijn computer als die wil. Dus in die zin is het beveiliging alleen maar als ik eh, berichten ga versturen, dus mijn computer zelf wordt niet beveiligd door VPN. Dus als iemand hier binnenstapt en die zou mijn wachtwoord kunnen eh, ontcijferen of eh, iets, dan kan die nog steeds op mijn computer, dus daar heeft de VPN geen enkele waarde voor. VPN is alleen maar voor het berichtenverkeer. Dus die beveiliging is er wel, maar niet voor de computer op zich.

X: Oké. Dan de volgende vraag. Het is een brede vraag-

Y: Hmhm.

X: Met wat voor digitale dreiging heb jij op een normale dag te maken?

Y: Eh, heel veel denk ik. Eh, een is je eh, spam. En eh, phishing. Ook binnen [the professional services firm] zie je dat eh, het komt niet heel vaak voor, maar een hele enkele keer zie je toch nog wel eens een mail binnenkomen die eh, die phishing bevat. Eh, daarnaast heb je natuurlijk altijd het risico dat iemand eh, je password kan achterhalen. Als je een niet zo heel sterk password gebruikt, dan loop je het risico dat iemand jouw computer in kan en dus heb je altijd het gevaar dat ze op jouw computer kunnen en dan vervolgens al jouw bestanden kunnen benaderen. Dus als er zaken zijn waar je niet via VPN bij zou kunnen, volgens mij zijn die er niet als ik mijn bestanden op netwerken van [the professional services firm] zet. Maar als dat al zou kunnen, dan zou iemand daar dus gewoon bij kunnen. Nou ja, op je telefoon de bekende eh, whatsapp fraude en eh, hackers die proberen jou eh, software eh, naar binnen te schuiven om jouw computer over te nemen, of om je telefoon te hacken of- Nou ja, daarnaast eh, bankverkeer, waar je altijd risico's loopt. Eh, ja, je telefoon is natuurlijk eh, het uitlezen van je eh, wat is het, je RFI ofzo he, is dat RFI, het chipje, waarmee je je betaling kan doen en dergelijke.

X: Oké.

Y: Ja, dat zijn denk ik wel een beetje raken(0:21:03).

X: Ja. En als we nadenken over deze dreigingen-

Y: Hmhm.

X: Heeft een VPN verbinding hier invloed op?

Y: Eh, deels. Want eh, op het moment dat ik natuurlijk een VPN verbinding opzet en eh, ik heb software op mijn computer staan die eh, malware die eh, uiteindelijk alles kan meelezen of al mijn toets combinaties eh, kan opnemen, ja, dan heeft een VPN natuurlijk maar beperkt effect. Want mensen kunnen dan dus gewoon lezen wat ik doe. Kunnen waarschijnlijk niet alle berichten ontsleutelen en dat soort dingen, maar ze kunnen wel zien als ik aan het typen ben bijvoorbeeld. Dus het VPN is niet een, niet absolute veiligheid, als die er al zou zijn.

X: Ja. Heeft een VPN op nog meer manieren invloed op deze dreigingen?

Y: Eh, nou, in ieder geval is het een extra laag. Dus het is een stuk toegevoegde beveiliging.

X: Ja. Oké. En dan waren dit digitale dreigingen-

Y: Hmhm.

X: Heb jij daarnaast op een normale dag ook te maken met sociale dreigingen?

Y: Nou, nee, ja, wat, wat versta je onder sociale dreigingen? Social media berichten die eh, bijvoorbeeld verkeerd eh, kunnen uitpakken als je ze opent of iets dergelijks. Bedoel je zoiets of?

X: Ja, ik bedoel alle dreigingen die eh, niet digitaal zijn en waar jij mee te maken hebt als werkende voor [the professional services firm].

Y: Nou, ik zou, buiten het feit dat mensen je misschien een bericht sturen dat, waar een gevaar in zou kunnen zitten, niet echt eigenlijk nee.

X: Oké. En heeft een VPN verbinding op eh, ja, dat soort berichten?

Y: Nee, dat denk ik niet nee. Daar voegt VPN niet veel aan toe.

X: En als we dan kijken naar deze digitale dreiging en de sociale dreiging-

Y: Hmhm.

X: Wie of wat is dan de aanvaller die de dreiging veroorzaakt?

Y: Waarvan ik denk dat dat degene is die dat zou veroorzaken?

X: Ja.

Y: Ja, ik denk dat degene die die dreiging veroorzaken dat dat eh, hackers zijn die uiteindelijk op eh, op data of op financiële gegevens eh, dat die daarnaar op jacht zijn. Voorbeeldje waar wij werken met [0:24:00 until 0:24:42 has been omitted]. En dat gebeurt in de praktijk.

X: Ja, en wie zouden deze hackers zijn?

Y: Ja, als we dat wisten was het makkelijk he. Ik eh, dit zullen mensen zijn die eh, uiteindelijk een criminele achtergrond hebben over het algemeen, zeker degene die op financiële gegevens uit zijn. Eh, omdat die gewoon puur geld ermee willen verdienen. Mensen die echt op, op data van [the professional services firm] uit zijn, ja, het zou eh, bijvoorbeeld een concurrent kunnen zijn.

X: Oké. En is er naast het verkrijgen van financiële gegevens nog meer mogelijke motivaties?

Y: Nou ja, wat ik zeg, de data over bijvoorbeeld klantenbestanden. Prijzen die wij afspreken met leveranciers zou interessante informatie kunnen zijn voor anderen. Ja, personeelsgegevens, persoonsgegevens, het liefst natuurlijk voorzien van eh, van, van gegevens als adressen en hoe heet het, BSN ofzo. Ik kan me voorstellen dat dat data is waar mensen naar eh, naar opzoek zijn.

X: Oké. En wat voor achtergrond heeft een aanvaller?

Y: Ja, dat kan heel divers zijn. Dat kunnen jongens zijn van twaalf, dertien jaar, die het spannend vinden om proberen te hacken ergens. Tot aan eh, criminelen die gewoon op geld uit zijn en proberen je computer of het netwerk plat te leggen en daarvoor ransomware eh, te installeren en uiteindelijk losgeld vragen. Dus ik denk dat hackers in allerlei geledingen voorkomen.

X: Ja. Oké. En wat zou de impact van een aanval kunnen zijn?

Y: Eh, afhankelijk van het type aanval kan dat lopen van nou ja, goed, een vervelend dingetje dat je misschien software hebt die rare dingen op je computer doen, maar niet schadelijk zijn. Tot aan het volledig platleggen van je netwerk en daardoor loop je natuurlijk financiële schade, dat is een. Maar veel belangrijker denk ik zeker voor [the professional services firm] is natuurlijk reputatieschade. Als jij als [the professional services firm] door hackers platgelegd wordt, dat geeft niet echt een professionele indruk. Dus ik denk dat die schade nog vele malen groter zou zijn.

X: Oké. En als we an gaan kijken naar de VPN verbinding zelf-

Y: Hmhm.

X: Hoe veilig is een VPN verbinding?

Y: Ja, eh, durf ik niet te zeggen. Dat zal afhankelijk zijn van, van wat voor soort VPN verbinding, want ik heb ooit begrepen dat je ook een VPN verbinding kunt leggen maar zonder versleuteling. Ja, dan is dat eh, denk ik minder veilig dan eh, dan op het moment dat je ook nog aanvullend daarop bepaalde versleutelingen toepast en dan ligt het er ook nog aan wat voor versleuteling. Hoe geavanceerder je versleuteling, hoe groter eigenlijk de veiligheid is.

X: Ja. En zijn eh- Worden VPN verbindingen zonder versleuteling voor andere doeleinden gebruikt dan een VPN met versleuteling?

Y: Eh, dat, dat denk ik wel dan ja. Als je al zou kiezen voor het niet versleutelen, dan is dat waarschijnlijk omdat je alleen wilt voorkomen dat, dat niet willekeurig iedereen kan eh, je berichten kan onderscheppen. Alleen ja, op het moment dat iemand toch toegang krijgt en op de een of andere manier de berichten weet te onderscheppen, dan kan die ze dus wel gewoon lezen. Nou, kan me voorstellen dat je dat doet met minder gevoelige data, bijvoorbeeld niet-financiële data of eh, of iets dergelijks. Kijk, op het moment dat ik een mail naar een collega stuur, nou zit dat niet achter VPN, maar stel dat ik dat in VPN zet, dat ja, dat is wat minder spannend dan dat ik [0:29:12 until 0:29:25 has been omitted].

X: Ja. Oké. En als je nadenkt over deze mogelijk verschillende vormen en mogelijk verschillende niveaus in veiligheid dan ook-

Y: Hmhm.

X: Veranderen jouw handelingen hierdoor?

Y: Eh, ja, zeker. Op het moment dat ik weet dat een VPN niet gebruik maakt van versleuteling, dan ben ik me in ieder geval bewust van het feit dat ik daar dus geen hele gevoelige data overheen moet sturen. Omdat dat risico daarvan dus groter is, als iemand dat al kan onderscheppen, dat ook de data dus bekend is. Dus nog wel, ja, weer even als voorbeeld het mailtje naar een collega met een vraag ja, is dan wat minder eh, spannend dan eh, [0:30:18 until 0:30:23 has been omitted]. Wat je niet versleuteld zou versturen.

X: Oké. En weet jij of de [the professional services firm] VPN versleuteling gebruikt?

Y: Volgens mij wel. Ik ga daar overigens ook wel een beetje vanuit dat dat gebeurt. Ik heb het nooit opgezocht, maar ik ga ervan uit dat dat versleuteld is.

X: Oké. En zijn er nog andere manieren waarop jouw handelingen veranderen?

Y: Nou niet zo zeer door VPN, ik denk meer door een algemeen besef dat als je gebruikmaakt van Internet, dat je altijd risico's loopt. Dus dat betekent dat je op je laptop eh, op je [the professional services firm] laptop geen pagina's moet gaan openen waar eh, of zaken moet gaan downloaden waarvan je niet weet wat eh, wat de oorsprong is. Gratis programmatjes en dergelijke of eh, bepaalde websites gaan bezoeken waar je risico's loopt. Dat zijn dingen die je denk ik in zijn algemeen moet doen, los van of je nou wel of niet een VPN gebruikt.

X: Ja, zeker. Oké. Dit waren tot zo ver mijn vragen-

Y: Oké.

X: Zijn er nu nog dingen waarvan jij denkt dit is belangrijk om te vertellen over een VPN, maar is niet ter sprake gekomen?

Y: Nou, de vraag die je stelde van of [the professional services firm] gebruik maakt van versleutelde VPN, het feit dat ik het eigenlijk niet weet, geeft dus aan dat dat blijkbaar niet, eh, en ik denk dat meer mensen dat niet weten. En dat mensen misschien ook niet altijd de risico's eh, overzien, die gebeuren. Kijk het hacken van een website of de DDoS aanvallen en dergelijke, je hoort daar natuurlijk nooit, nooit heel veel over en dat hoeft ook niet. Maar, maar mensen weten niet of dit gebeurt. [0:32:38 until 0:33:06 has been omitted]. En ik vraag me dus ook af of binnen [the professional services firm] daar voldoende aandacht aan wordt besteed, behalve dat mensen natuurlijk wel altijd weer zo een berichtje krijgen van nou doe dit niet, doe dat niet, maar je krijgt zo verschrikkelijk veel e-mails, dat mensen lezen dat gewoon niet meer. En het risico wordt gewoon iedere dag groter, want ook de hackers stil natuurlijk.

X: Nee zeker niet.

Y: En ook niet alleen de digitale, maar ook de wat je zei, ja, noem het sociale dreiging, de bekende e-mailtjes met eh, [0:33:49 until 0:33:56 has been omitted]. Of een LinkedIn berichtje van iemand eh, binnen je netwerk, maar blijkt dat het geen LinkedIn is, maar een nagemaakte site, waardoor er binnen no-time

allerlei vervelende software op het netwerk staat, ja, dat, dat zijn wel risico's waar volgens mij niet heel veel aandacht aan besteed wordt. Althans niet zichtbaar, laat ik het zo zeggen.

X: Ja. Oké. En zijn er daarnaast-

Y: En meer eigenlijk niet.

X: Oké. Prima, dan tot zo ver het interview gedeelte. Ik wil je heel erg bedanken voor je deelname, wat dit helpt mij heel erg. En heb jij nog vragen voor mij?

Y: Nou, ik ben even benieuwd wat, wat ga je hier precies mee doen, wat is uiteindelijk je doel van je opdracht.

X: Ja, dat snap ik, ik zal de opname even stoppen.

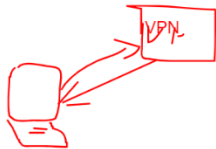


Figure C.17.1: Drawing 17_1

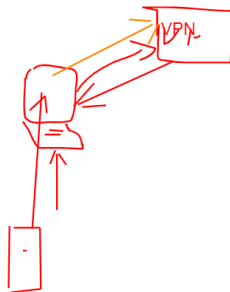


Figure C.17.2: Drawing 17_2

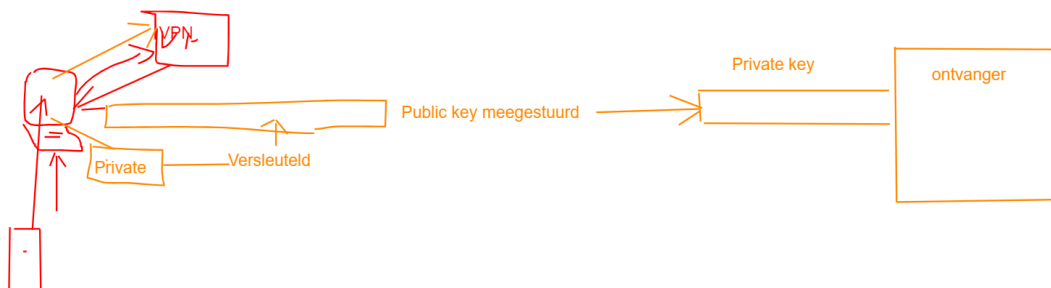


Figure C.17.3: Drawing 17_3

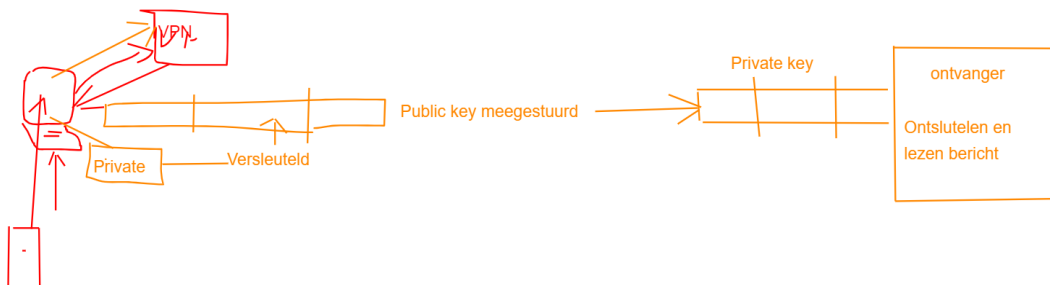


Figure C.17.4: Drawing 17_4

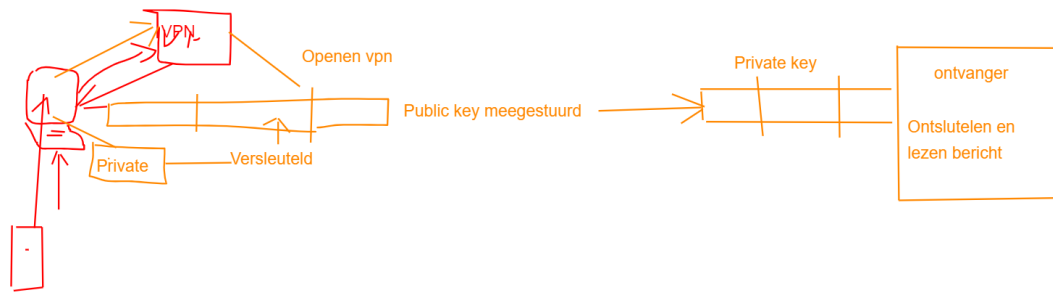


Figure C.17.5: Drawing 17_5

C.18: Transcript Laypeople 7

Duration: 41 minutes

Language: Dutch

Number of drawings: 6

X: Dan start ik met de eerste vraag van het interview. Kunt u aan mij uitleggen wat een VPN is?

Y: Ja, als ik het eh, heel simpel vertaal naar eh, Jip en Janneke taal, dan is het eigenlijk dat een gebruiker een soort masker op zet en daarmee eh, zich kan voordoen als iedereen op eh, op Internet. Voordeel is dat eh, berichten versleuteld worden eh, tussen de gebruiker, tussen de laptop van de, de pc van de gebruiker en de, en de VPN server. En dat ook de locatie er eigenlijk ook niet meer toe doet. He, zo zie je dat mensen waar nogal censuur op het Internetgebruik zit, zoals in sommige Aziatische landen, dat men daar vaak een VPN verbinding gebruikt om toch social media kanalen te kunnen gebruiken. Dat is een beetje het beeld wat ik er van heb. Eh, binnen de organisatie, [the professional services firm], wij gebruiken het ook, ik denk ook eh, vanwege dat eh, die global insteek eh, en, en uiteraard de versleuteling van de data. He, omdat-

X: En wat bedoelt-

Y: natuurlijk ook wel eens in hotels of op vreemde plekken op eh, op een openbare wifi zitten.

X: Oké. En wat bedoelt u met global insteek?

Y: Eh, nou ja, als je, ik heb bijvoorbeeld [0:02:08 until 0:02:10 has been omitted], dan moet je wel bij de Nederlandse servers kunnen. Ik kan me voorstellen dat er bepaalde locatievoorzieningen zijn, die zeggen waar zit jij, nou in mijn geval zat ik dan in [country] en ik moet iets benaderen in Nederland. Dan kan die verbinding niet worden eh, gemaakt, omdat ik dan buiten Nederland ben. Ik heb dat toevallig van de week gehad met Ziggo, ik weet niet of je Ziggo kent, maar dan start je die app op in Duitsland, dan zegt die ja je bent binnen, of je bent buiten Nederland, dus we kunnen die content niet laten zien. Je mag gewoon niet buiten eh, buiten het land, maar met een VPN verbinding kan je doen alsof je in Nederland bent eh, vanuit elke plek op aarde.

X: Oké. En u noemde ook een masker, wat bedoelt u daarmee?

Y: Nou, dat je min of meer incognito op eh, op het Internet kunt eh, kunt surfen, omdat je IP-adres, waarmee je je op het, het Internet surft van je PC, ja, die kun je iedere naam geven die je wilt, of ieder nummer geven die je wilt. Je kunt iedere IP-adres aannemen. En niet je vaste IP-adres waarmee je te herleiden bent naar je betreffende locatie.

X: Oké. En u zegt dat de berichten versleuteld worden tussen de gebruiker en de VPN server-

Y: Ja.

X: Hoe worden deze berichten versleuteld?

Y: Nou, hoe dat technisch precies gaat weet ik niet, maar het bericht wat je maakt wordt als het ware in een soort koker gestopt. En die koker eh, ja, die is, daar zit een sleutel op eh, en aan de andere kant eh, gaat die sleutel er weer af. Dus zou dat bericht onderweg ergens eh, of zou die koker onderweg ergens eh, geopend moeten worden, dan moet je die sleutel hebben om dat bericht dat erin zit te kunnen lezen. Dat is het voordeel, dat is eigenlijk het voordeel van een VPN verbinding. En dat is ook ja, ik zeg dat nu zo eh, het bericht gaat in een koker, dat is natuurlijk niet zo, maar eh, dat is eh, dat is eh, een beetje de visuele voorstelling die ik daarvan heb.

X: Ja, oké. En eh, dan noemde u ook nog VPN in verband met openbare wifi-

Y: Ja.

X: Wat is de relatie hiermee?

Y: Nou ja, als je, tenminste, dat is mijn beleving, als je via een openbare wifi in een of andere [example of restaurant] eh, voor je werk een bestand op wilt halen, dan gaat dat via die beveiligde verbinding, en omdat die eh, omdat dat Internetverkeer versleuteld is eh, gaat dat toch op een veilige manier. Is mijn idee eh, he, normaal gesproken kun je vrij eenvoudig meelezen op een openbare wifi verbinding met eh, wat iedereen daar aan het doen is. En dat is natuurlijk eh, dat brengt natuurlijk een risico met zich mee.

X: Ja. Oké. En voor welke doelen gebruikt u VPN?

Y: Nou, volgens mij heb ik niet eens een keus. Wij zitten altijd via een VPN verbinding, maar ik denk, omdat wij nu vanuit huis werken, het extra belangrijk is dat eh, dat de data versleuteld wordt. Niet iedereen heeft zijn thuisnetwerk goed beveiligd. We gaan met onze [the professional services firm] laptop op ons thuisnetwerk wat ooit eens een keer een slimme buurman heeft aangelegd eh, ja, dan is het wel belangrijk dat de data, die vaak eh, vertrouwelijk is. He, omdat het over cliënten gaat he, of over de organisatie als [the professional services firm] zelf, dat dat eh, dat dat niet voor anderen zo maar leesbaar is. En voor zo ver-

X: Ja. En wat bedoelt u ermee, o, sorry?

Y: En voor zo ver ik heb begrepen geldt dat ook voor de telefoons die wij ter beschikking hebben gekregen. He, ik heb een eh, ik heb een [mobile phone], ja, daar zit je natuurlijk eh, te pas en te onpas op onbeveiligde wifi. En, en, ja, die neem je ook mee als je, als je de stad in gaat. Ik noem maar wat. He, dus het is wel belangrijk dat die data juist op de mobiele telefoon versleuteld wordt en niet voor iedereen toegankelijk is. Vooral omdat de apps waarmee we toegang krijgen tot de [the professional services firm] systemen steeds eh, steeds meer toeneemt. He, onze volgende tijd, tijdschrijfsysteem, zal een app hebben. Het verantwoorden van expenses, dat zal via een app kunnen. [0:06:37 until 0:06:42 has been omitted]. Ja, dan is het wel belangrijk, omdat je natuurlijk je expenses op een, en je time ook, op een engagementnummer boekt, dat niet al die engagementnummers zo maar beschikbaar zijn eh, op je mobiele telefoon.

X: Ja. Oké. En gebruikt u dan ook de VPN verbinding op uw [mobile phone]?

Y: Nou, je kunt niet zonder. Want zonder die VPN verbinding, werken die apps niet.

X: Oké. En u gebruikt dan ook de [the VPN of the professional services firm]?

Y: Ja. Nou, of ik dat gebruik weet ik niet, maar ik heb [e-mail], dat moet je, dat moet je binnen een bepaalde appstore halen, een [the professional services firm] appstore en die [e-mail] app en de andere apps, we hebben er nog meer, [conferencing software] is er ook zo een. Eh, en de expense app. Die eh, die gaan allemaal via die, via die VPN verbinding, anders werken die apps niet eens. Want in je instellingen moet je ook toestaan dat die VPN verbinding gebruikt wordt, daarmee worden ook een aantal security settings ingesteld die je niet kun omzeilen, althans ik heb dat niet echt geprobeerd. Maar je ziet dat je telefoon ook binnen een minuut eh, vergrendeld wordt. He, terwijl je als normale gebruiker, als je hem alleen eh, privé gebruikt, ja, kun je dat geloof ik instellen tot wel 15 minuten voordat het scherm automatisch vergrendeld wordt.

X: Ja. Oké. En dan zei u eerder nog eh, wij zitten altijd via VPN.

Y: Ja, volgens mij wel.

X: En op welk apparaat bedoelt u dit?

Y: Nou ja, op eh, op de PC, op de laptop, die eh, die ik gebruik van [the professional services firm] en op de telefoon. De apps die ik voor [the professional services firm] gebruik he, als ik gewoon naar mijn eigen bank ga op de telefoon van [the professional services firm], dan gaat dat niet via een VPN verbinding.

X: Oké. Moet u dan weer de VPN uitzetten of gaat dat automatisch?

Y: Nee, nee hoor, daar hoeft je niets voor te doen, nee. Nee, het is ook niet zo dat ik op de laptop wel of niet kies voor een VPN verbinding.

X: Oké, dus eh-

Y: Volgens mij, volgens mij gaat dat via [the VPN of the professional services firm]. Als ik op de [the professional services firm] systemen wil, dan moet ik eerst via [the VPN of the professional services firm] een verbinding leggen, dan eh, dan kan ik bij de [the professional services firm] systemen zoals

[conferencing software] eh, [conferencing software] kan, [conferencing software] of nee SharePoint bijvoorbeeld. Eh, de [the professional services firm] apps, zoals [an internal page], daar kun je alleen maar bij, die op het intranet zitten, daar kun je alleen maar bij als je via die eh, via die [the VPN of the professional services firm] bent ingelogd.

X: En bedoelt u dan dat VPN automatisch opstart of wat bedoelt u met wij zitten altijd in VPN-

Y: Dat vermoed ik wel ja, want ik start, ik start het niet zelf op. Volgens mij gaat dat op de achtergrond van zelf. Dat vermoed ik hoor, ja dat eh-

X: Ja. Oké. En eh, als je dan de [the VPN of the professional services firm] opstart, welke handelingen voert u daarvoor uit?

Y: Nou, ik druk op een icoontje onderin mijn taakbalk, want die heb ik daarin gezet. Eh, nou ja, dan vul ik mijn persoonlijke wachtwoord in plus de eh, wat zijn het, vijf cijfers die eh, die op de [the VPN of the professional services firm] app verschijnen. En die samen eh, maken verbinding met het intranet van [the professional services firm]. Ik start niet specifiek VPN op. Maar mijn vermoeden is dat dat erachter zit. Dat die intranet toepassing allemaal via een VPN verbinding eh, worden benaderd en dat je dat automatisch met [the VPN of the professional services firm] opstart.

X: Oké. En is er ook als eh, [the VPN of the professional services firm] nog niet opgestart is, kunt u ook een VPN verbinding maken?

Y: Ik heb dat nooit geprobeerd. Maar dat ja, technisch eh, moet dat lukken. Want je kunt, je kunt als privé persoon ook gewoon een VPN verbinding aanvragen. Sommige zijn zelfs gratis.

X: Ja. Oké. En-

Y: Maar kijk, ik heb daar geen ervaring mee. Sorry.

X: Geen probleem. Gebruikt u naast uw mobiel en laptop nog andere apparaten voor de [the VPN of the professional services firm]?

Y: Eh, nee, nee. Ik heb wel een tablet, maar die gebruik ik nooit.

X: En kunt u aan mij uitleggen hoe een VPN verbinding werkt? Ik zal hiervoor een nieuwe dia pakken, dan kunt u het whiteboard gebruiken als u dit wilt.

Y: Oké. Ik ben wel mijn icoontjes kwijt om mee te tekenen.

X: O, ja. Nu niet meer.

Y: O. Eh, eens even kijken hoor. Ik zie hier- [\[start drawing 18_1\]](#). Je hebt de gebruiker die via een firewall het Internet opgaat, een verbinding maakt. Ja, nou dat tekenen, dat eh- Pak alleen het potloodje anders maar even hoor.

X: Oké.

Y: En daar ben ik niet best in hoor, in tekenen.

X: Prima.

X: Via Internet maak je verbinding met een- Ik lijk wel een kind van twee dat voor het eerst een tekening maakt. Nee, wacht even, die- He, dus je hebt hier firewall, hier ben je, dit is de laptop van de gebruiker hier links, dat rondje. Nou, dan ga je door een firewall heen, nou, dat is gewoon de firewall die ik hier he, geïnstalleerd heb op mijn eh, op mijn thuisnetwerk. He, dat anderen niet op mijn thuisnetwerk kunnen. Daarmee ga ik het Internet op en maak ik verbinding met eh, dit moet dan een VPN server voorstellen van [the professional services firm]. [\[start drawing 18_2\]](#). En daarmee eh, ja, ga ik naar de verschillende websites. Is mijn beleving hoor, maar ik ben geen eh- Want het gaat over experts en eh, en onwetenden, nou ik ben geen expert in ieder geval als het gaat om VPN, misschien is dat eigenlijk ook maar goed, want dat blijkt dat dat het achter de schermen wellicht allemaal zo veel vanzelf sprekend is, dat je daar als gebruiker ook niet heel veel last van hebt.

X: Nee, dit zie je natuurlijk niet aan de voorkant wat er allemaal gebeurt.

Y: Nee, je ziet aan de voorkant niet wat er eh, wat er allemaal gebeurt, nee.

X: Oké. En kunt u aan mij uitleggen wat een server is?

Y: Nou ja, wat een server is eh, een server die verzorgt het eh, die verzorgt de verbinding tussen de gebruiker en eh, het Internet en de systemen binnen [the professional services firm]. He, dat is eigenlijk een soort eh, ja, een soort draaideur, naar de eh, naar de verschillende, naar de verschillende websites en de eh, en de systemen van [the professional services firm].

X: Ja. Oké.

Y: Die zegt van wie ben jij en waar moet je naartoe en heb jij daar toegang. Nee, niet waar, heb jij daar toegang, want dat weet die server niet. Dat komt, dat komt dan terug vanuit eh, vanuit de toepassing zelf. Maar eh, die regelt dat verkeer.

X: Oké. Eh, dan zei u eerder ook dat er versleuteling wordt gebruikt van de berichten-

Y: Ja.

X: Waar in deze tekening vinden we de versleuteling terug?

Y: [\[start drawing 18_3\]](#). Nou de versleuteling die vindt volgens mij pas plaats vanaf de VPN server.

X: Ja, VPN. Dus dan bedoelt u, o sorry?

Y: Je gaat naar de websites, maar misschien heb ik het gruwelijk mis hoor, maar dat is mijn beleving bij een eh, bij een VPN. He, dus hier vindt de versleuteling plaats, hier doe ik een aanvraag voor de website he, [an internal page], nou, die draait op een [the professional services firm] server. [\[start drawing 18_4\]](#). En deze, deze verbinding is eh, is dan versleuteld. He, daar kan dan dus een ander niet op meelesen. Of dat ook geldt tussen de gebruiker en de VPN verbinding zelf, die ook over het Internet loopt, dat weet ik niet. Ik kan wel gokken, maar nee, dat weet ik niet.

X: Oké. En dan een andere vraag. Wat is de invloed van een VPN verbinding op jouw computerbeveiliging?

Y: Nou, het is niet echt merkbaar, maar het kan niet anders dan dat het allemaal iets trager verloopt, omdat dat versleutelen nou eenmaal tijd kost. En dat zal ongetwijfeld heel intelligent zijn tegenwoordig, maar het kost gewoon tijd. En eh, ja, wat dat komt de performance over het algemeen niet ten goede. Maar omdat ik de keuze niet heb, kan ik niet zien hoe snel mijn verbinding is met en zonder VPN.

X: En wat bedoelt u, dat u niet de keuze heeft?

Y: Nou volgens mij kan ik niet naar [an internal page] om te kijken hoe snel het is zonder VPN verbinding. Want dan werkt het gewoon niet, dan krijg ik gewoon geen toegang.

X: Oké. En heeft een VPN verbinding nog op een andere manier invloed op jouw computerbeveiliging?

Y: Nee, voor zo ver, nee, volgens mij niet, nee.

X: Oké. Dan een hele brede vraag-

Y: Nou ja-

X: O, sorry.

Y: Nou ja, in zoverre dat iemand die mijn laptop steelt he, er wordt ingebroken in mijn huis, mijn laptop, of neemt de [the professional services firm] laptop mee, die kan niet zomaar op de [the professional services firm] systemen, omdat je dan weer door die beveiliging heen moet.

X: Ja. En wat bedoelt u dan met beveiliging?

Y: Nou de beveiliging van eh, van eh, wat is het, [the VPN of the professional services firm]. He, ze hebben dan alleen maar de hardware, je hebt alleen maar de PC en je kunt niet bij onze klantenbestanden en dergelijke en bij onze rapportagesystemen. Bij alle systemen waar de gebruiker van [the professional services firm] toegang toe heeft.

X: Ja. Oké. En dan nog een vraag over deze tekening. Zijn deze verbindingen dan ook versleuteld, geldt dat voor alle verbindingen achter de lijn?

Y: Ja, volgens mij wel, ja.

X: Ja, oké. Dan een hele brede vraag. Met wat voor digitale dreigingen heb jij op een normale dag te maken als [the professional services firm] medewerker?

Y: Digitale dreigingen. Eh, nou ja, je, je e-mail adres dat vind ik een eh, ja, dat is, dat is een sleutel tot eh, tot [the professional services firm] die vrij makkelijk eh, ja, ik krijg, ik krijg tegenwoordig ook spam binnen op mijn [the professional services firm] mailbox. En misschien wordt er nog een hoop tegen gehouden. Eh, de andere dreiging is toch de, de mobiele telefoon, hoewel die ook steeds beter wordt met beveiliging, met gezichtsherkenning en dat soort dingen. Eh, ja, de, de dreiging, kijk, de, de VPN verbinding volgens mij is die maar twee uur actief he, dus zou mijn PC, mijn [the professional services firm] laptop in die twee uur gestolen worden, ja, dan kan men alles doen wat men wil. Als ik nu even boodschappen ga doen, en ik kom terug, mijn PC is gestolen, ja, dan kan in die twee uur kan iedereen alles doen wat men wil. Want ik sluit niet af.

X: En moet u dan na die twee uur weer op niet de [the VPN of the professional services firm] opstarten?

Y: Ja, dat moet ik opnieuw [the VPN of the professional services firm]. Ik zeg kan iedereen alles doen, maar dat is natuurlijk niet zo, want je scherm wordt wel beveiligd, of je laptop. Dus je moet wel die code invoeren, die pincode, dus dat valt qua dreiging denk ik nog wel mee.

X: Ja. Dus op een normale dag moet u ook meerdere keren opnieuw verbinding maken?

Y: Ja. Ja, heel veel eh, applicaties, zoals [e-mail] en [conferencing software] wat je tegenwoordig eh, wat ik tegenwoordig het meest gebruik, dat werkt ook zonder eh, [the VPN of the professional services firm]. Eh, dus ja, dat eh, ik start het soms niet eens op, maar dan ga ik naar een intranetsite en die werkt dan niet. Dan denk ik o ja, even een [the VPN of the professional services firm] verbinding maken. Eh, en dan merk ik soms ook, als ik dan later op de dag, als ik dat nog een keer heb, he, dat die weer verbroken is.

X: Ja. Oké. En heeft u op een normale dag met nog meer digitale dreigingen te maken?

Y: Eh, nou ja, kijk, digitale dreigingen, die zitten natuurlijk op het thuisnetwerk, en het thuisnetwerk is over het algemeen niet zo goed beveiligd he, en ook niet zo sterk als een eh, een kantoornetwerk. He, en ik moet altijd door mijn privé netwerk heen. Ja, daar, als ik, als ik van binnen naar buiten kan, dan is het wellicht ook mogelijk dat iemand van buiten naar binnen gaat. He, dus inbreekt op mijn eh, privé netwerk, ik heb hier ook een NAS. Ik weet niet of je- Een NAS, zo een netwerkdrive, ja, die heeft ook verbinding met buiten, dat gaat ook via een cloudoplossing, kan ik er overal ter wereld bij. Hartstikke handig. Maar daarvoor moet je wel bepaalde deuren openzetten in je, in je router. Die zeggen nou voor dit apparaat mag er van buitenaf verbinding worden gelegd. He, want die zit natuurlijk aan de binnenkant van je netwerk. Nou, dat, dat is natuurlijk een potentieel risico. Als je dat niet goed doet is het een potentieel risico.

X: Ja. Oké. En heeft een VPN verbinding invloed op deze soorten digitale dreigingen?

Y: Eh, ja, dat denk ik wel. Denk wel dat eh, dat als iemand een VPN verbinding gebruikt vanuit het buitenland, ten eerste is die dan niet meer terug te traceren, terwijl iemand eh, ja, een hacker die eh, die zonder VPN verbinding probeert in te breken, die is te herleiden aan zijn IP-adres, en zijn IP-adres is weer te herleiden naar een locatie eh, en uiteindelijk de bezitter van die, van die laptop. Eh, maar in ieder geval de locatie. Met een VPN verbinding is dat onmogelijk, dan kan het overal vandaan komen. Dan lijkt het iemand misschien uit Appelscha te zijn, terwijl die ergens op de Filipijnen zit.

X: Ja, en is dit ook mogelijk met de [the professional services firm] VPN?

Y: Dat weet ik niet. Dat weet ik niet. Maar ik mag hopen dat ze dat goed beveiligd hebben. Nou ja, mag ik allemaal wel hopen, maar vorige week zijn er natuurlijk weer een hoop Twitter accounts gehackt. En ik mag aannemen, maar daarvan zien we het tegendeel, dat Twitter zijn zaakjes ook niet echt goed op orde hadden. He, omdat medewerkers van intern daar eh, eh, hebben, aan mee hebben geholpen. Ja, als medewerkers hebben binnen [the professional services firm], die eh, die VPN servers beheren, eh, en het op een akkoordje gooien met hackers, ja, dan is eh, dan houdt het op natuurlijk. Je hebt altijd nog die menselijke factor.

X: Ja, oké. En over deze menselijke factor gesproken, heeft u naast digitale dreigingen ook nog te maken met sociale dreigingen op een normale dag?

Y: Sociale dreigingen. Nou, nee, ik heb daar niet mee te maken. Nee, ik heb daar niet mee te maken, maar ik, op [social media platform] bijvoorbeeld, ik heb een [social media platform] account, ik zal even een voorbeeld geven. Ik heb een [social media platform] account, nou ja, bij [social media platform] vragen ze ook eh, wat je doet, nou ik vul daar gewoon in [role] bij [the professional services firm], prima. Eh, maar wat ik op [social media platform] zet, ja, dat is over het algemeen natuurlijk zijn dat privé dingen. He, en die privé zaken, tegenwoordig is het natuurlijk allemaal heel zwart-wit wat er op eh, zijn hele zware discussies gaande. Je moet dan natuurlijk ook wel uitkijken wat je zegt. He, eh, wat je als privé persoon zegt, of schrijft op [social media platform]. En nou doe ik daar geen gekke dingen op, maar ja, dat kan altijd weer terug te herleiden zijn naar de organisatie waar je voor werkt.

X: Ja, oké. En heeft u daarnaast nog met andere sociale of niet-digitale dreigingen te maken?

Y: Nou ja, je hebt altijd te maken met inbraken natuurlijk. He, mogelijke inbraak. Je ziet dat tegenwoordig steeds meer zaken via de cloud gaan. Voor mijn privé, ik heb zelf privé een laptop, ja, daar zit ik nu op, heb ik nu met jou die verbinding. Ja, die eh, alle wachtwoorden die ik gebruik voor websites, en dat zijn er inmiddels [number], die gaan via de cloud naar mijn [mobile phone], naar mijn tablet, en naar de [mobile phone] van mijn [partner]. Die zijn gewoon daar leesbaar, die, die je ziet daar de login naam staan als je,

als je in instellingen naar wachtwoorden en accounts gaat, dan zie je daar gewoon de inlognaam en het wachtwoord staan. Nou, ik krijg het niet voor elkaar om dat af te schermen. Dat vind ik, vind ik een dreiging waarbij je, bij de [the professional services firm] hardware zie ik dat niet. En nogmaals, het wordt steeds beter versleuteld, want ik heb net een nieuwe laptop en de, die werkt alleen maar met een vingerafdrukscanner en de [mobile phone] tegenwoordig met gezichtsherkenning, maar daarvoor de, de ouder [mobile phone] van mijn [partner], dat was een [mobile phone], ja, die had het allemaal niet. Die had ook geen code, want dat vond [partner] vervelend. Eh, dus [partner] zette hem aan, en dan zag je gewoon die [number] wachtwoorden staan. Als je wist waar je moest kijken. Nou, dat vond ik nou niet bepaald prettig.

X: Nee, dat kan ik mij voorstellen.

Y: Maar dat is, ja, dat, dat heeft niet betrekking op de [the professional services firm] organisatie.

X: Ja. En heeft u vanuit uw rol in [the professional services firm] wel te maken met sociale dreigingen?

Y: Nee. Nee. Dat idee heb ik niet. Ja, wat, kun je daar een voorbeeld van geven, wat ik, waar ik dan aan zou moeten denken.

X: Ja, dat zou van alles kunnen zijn. U noemde eerder bijvoorbeeld inbraken.

Y: Ja.

X: Dat kan ook. Maar dan gaan we terug naar de digitale dreigingen. En wie of wat is dan de aanvaller die de dreiging veroorzaakt?

Y: Ja, dat kan iedereen zijn. Dat kan iedereen zijn eh, die, die baat heeft bij eh, het inbreken op het [the professional services firm] netwerk. En dat kan zijn bijvoorbeeld om onze clientgegevens buit te maken. He, we zijn daar natuurlijk heel zorgvuldig mee, en terecht. Maar als grote organisatie zoals, zoals [company] en dat soort bedrijven gehackt kunnen worden, ja, dan, dan durf ik niet te zeggen dat het bij [the professional services firm] niet lukt. Nou zit er bij bedrijven als [company] altijd nog een financieel gewin achter als je [0:28:14 until 0:28:14 has been omitted] kunt buitmaken, bij [the professional services firm] hebben we dat minder. Maar toch eh, ja, uiteindelijk is het altijd een wedloop tussen je beveiliging vanuit je organisatie en eh, en de boze buitenwereld die daar toegang toe wil krijgen.

X: Ja, oké. En wat zou de motivatie van een aanvaller kunnen zijn?

Y: Nou ja, de motivatie zou kunnen zijn het buitmaken van, van clientgegevens he, van onze cliënten. He, of daar ... zeggen, nou ik heb jullie, wat is het [number] cliënten op een USB stick staan, eh, wat heb je ervoor over. Het zou eh, ja, dat, de motivatie is meestal geld. En heel slecht gedacht, ja, zou het ook nog een eh, zou het ook nog een concurrentie eh, ding kunnen zijn. He, om te weten welke cliënten wij allemaal hebben. [0:29:23 until 0:29:46 has been omitted].

X: Ja, oké. En wat voor achtergrond heeft een aanvaller?

Y: Nou, dat is meestal een technische achtergrond. Dat, dat is vrijwel altijd een IT achtergrond. Die in opdracht werkt van eh, van iemand die daar financieel gewin uit haalt, maar zelf niet zo slim is om eh, om in te breken. Maar nou heb ik misschien, heb ik misschien een ouderwets beeld van een hacker hoor.

X: Ja. En wie zou dan de opdracht geven?

Y: Ja, wie is de opdrachtgever, dat, dat kunnen allerlei criminelen zijn natuurlijk. Ik kan niet zo specifiek een iemand aanwijzen he, of een groep aanwijzen die eh, die bij voorbaat verdacht, verdenk van eh, een potentiële inbraak op onze systemen, nee.

X: Er zijn er bepaalde ja, meer abstractere groepen in dit geval die je wel zou kunnen bedenken?

Y: En dan heb je het over [the professional services firm] specifiek?

X: Ja.

Y: Ja, nou, dat zou concurrentie kunnen zijn. Maar ook groepen, ook groepen die losgeld vragen he, data is tegenwoordig business. He, dat zien we aan bedrijven zoals [social media platform]. En dat zien we ook aan eh, gratis VPN eh, diensten. He, die jouw data he, want niks is gratis, maar het verdienmodel is dan jouw data, de websites die jij bezoekt. He, die kunnen allemaal verkocht worden eh, die gegevens. Eh, dus ja, data dat eh, dat is geld waard. En ik kan me voorstellen dat, dat er mensen zijn die interesse hebben in het klantenbestand van [the professional services firm]. En ik zeg nou steeds klantenbestand, maar ik kan me ook voorstellen het personeelsbestand wat wij hebben. Als je alle namen en adressen van onze

medewerkers eh, op een USB stick hebt staan, ik, ik zou persoonlijk niet weet wat je er mee moet, maar ja, wellicht dat mensen daar iets in zien.

X: Ja. En het risico dat u noemt bij gratis VPN, speelt dat ook bij [the professional services firm] VPN?

Y: Nee. Nee, dat eh, nou ja, ja, nee is altijd zo zwart-wit, maar eh, dat vermoed ik niet. Als er niet mensen van binnenuit eh, onze IT-ers die binnen onze organisatie werken, dat serververkeer op een USB stik en te koop aan bieden, nee dan denk ik dat eh, dat dat risico minimaal is. En ik zeg minimaal, want nul is het nooit. Als iemand kan inbreken op die VPN server, ja, dan eh, dan hebben we alsnog een probleem. Maar van binnenuit verwacht ik dat niet nee.

X: En als we dan kijken naar al deze aanvallen, wat zou de impact van een aanval kunnen zijn?

Y: De impact van de aanval is dat eh, dat de vertrouwelijkheid naar je cliënten toe geschaad wordt en daardoor kunnen cliënten weglopen. Wat natuurlijk vervolgens een eh, een financieel verlies voor ons zal betekenen. He, als wij een client als [0:33:08 until 0:33:12 has been omitted] waarmee wij werken, waarvoor we werken, naar buiten lekken, ja, dan zal [company] waarschijnlijk naar een andere [0:33:20 until 0:33:22 has been omitted] op zoek gaan. En ik zeg nou [company], maar dat geldt voor iedere, voor iedere klant die we hebben.

X: Ja, zeker. Oké. En als we dan gaan kijken naar de VPN verbinding zelf, hoe veilig is een VPN verbinding?

Y: Ja, op een schaal van 0 tot 100 ofzo, of eh, wat, hoe veilig, ja, ik denk dat het op dit moment het meest veilige is eh, wat je eh, wat je als organisatie kunt inzetten.

X: Ja, en zijn er redenen wat u kunt bedenken waarom een VPN verbinding mogelijk niet veilig is? Of minder veilig?

Y: Nou ja, we maken natuurlijk steeds meer beschikbaar van clouddiensten. En die clouddiensten, daarvan zie je dat de servers eh, beheerd worden door externe organisaties. He, daar gaat dus ook onze data naartoe. He, onze nieuwe [an internal page] bijvoorbeeld, ja, die draaien op [company] servers, ik dacht in [country], maar dat weet ik niet helemaal zeker, maar ik dacht in [country]. Die data, die gaat dus tussen die VPN verbinding en die eh, [company] server. Ja, wat er bij de [company] en natuurlijk zijn daar allerlei eh, afspraken over en eh, liggen daar eh, contracten aan ten grondslag, maar uiteindelijk hebben wij geen zicht op eh, op de infrastructuur binnen die externe organisatie. En dat heb je met clouddiensten natuurlijk steeds vaker. Het is niet meer alleen binnen je eigen netwerk. He, dus als ik ergens een gevaar eh, zie, dan is het binnen die clouddiensten, die niet door ons beheerd worden. En we vertrouwen het allemaal wel, maar ja, we zullen niet de eerste zien die eh, waarbij toch blijkt dat het minder veilig is dan we denken.

X: Ja. En zijn er nog andere redenen die je kunt bedenken waarom een VPN verbinding mogelijk niet veilig is of minder veilig?

Y: Eh, nee. Nou, nee, ja, ik, kijk, ik kan me voorstellen dat een gebruiker die weet dat die een VPN verbinding gebruikt misschien wat minder zorgvuldig is. He, in het gebruik, wat die doet. Die onzorgvuldigheid, ja, dat is natuurlijk een potentieel risico. Eh, he, je kunt denken van nou ja, ik ben toch niet te traceren, dus eh, ga maar weet ik veel, op websites waar ik normaal eh, op mijn privé laptop niet naar toe ga. Wat zoals ik nu reclame krijg binnen, op mijn, op mijn [e-mail] scherm, of binnen [e-mail], ik heb geen idee waar ik ooit die eh, die zakelijke eh, he, dat zakelijke e-mailadres achter gelaten heb. Ik ben daar toch wel heel zorgvuldig in, maar kennelijk eh, is het toch ergens een keer binnen gekomen. Krijg nu allemaal elke dag reclame voor thermometers, neustrimmers en dat soort troep.

X: Dat is vervelend ja.

Y: Ja, dat is vervelend ja. Dat krijg ik om mijn privé laptop ook, maar goed, ja, op mijn zakelijke laptop wil ik dat niet.

X: Nee, zeker. En als we naar deze tekening kijken. Zou je mij kunnen uitleggen hoe het werkt als je verbinding maakt met dan een [company] clouddienst?

Y: Ja. Dat gaat, dat gaat volgens mij ook via die VPN server. [start drawing 18_5]. Als gebruiker maak je contact met die [the professional services firm] VPN en die maakt eh, contact met eh, cloudservers van ja, ik zeg nou [company], nou [company]. Daar zit natuurlijk ook gewoon een eh, een server achter. He, die aanvraag die ik hier doe, via die VPN server leidt eh, en die zegt van he, [me], mag die toegang hebben tot die server, wat mag die dan en dat, dat verkeer loopt hier. [start drawing 18_6]. Ja, dit verkeer is versleuteld. He, dus iemand die hier op inbreekt, die kan niet lezen wat ik daar doe. He, want deze informatie gaat

natuurlijk twee kanten op, ik doe hier een aanvraag voor bijvoorbeeld [0:38:10 until 0:38:11 has been omitted] he, die gaat die kant op. Maar daar gaat de informatie over die [0:38:16 until 0:38:17 has been omitted], die gaat eh, die gaat uiteraard eh, weer terug naar mij toe. Want ik zie het uiteindelijk op mijn PC. Het wordt wel een eh, wordt wel een drukke tekening.

X: Ja, maar nog steeds heel duidelijk.

Y: Ja, misschien zit ik er helemaal naast hoor. Maar goed, jij vraagt mijn begrip van eh, van een VPN verbinding, en dat is wat ik ervan heb.

X: Ja, zeker. Oké. Dit waren tot zo ver mijn vragen. Zijn er nu nog dingen over een VPN die niet ter sprake zijn gekomen?

Y: Nee, volgens mij niet. Ja, nee. Nee, als het gaat om de [the professional services firm] organisatie, hebben we denk ik alles wel, wat ik weet eh, of denk te weten, laat ik het goed zeggen, hebben we alles wel gehad.

X: Ja. Oké. Dan eh, tot zo ver het interview. Ik wil u heel erg bedanken voor uw deelname, want dit helpt mij heel erg. En-

Y: Alsjeblieft.

X: Heeft u nog vragen ook voor mij?

Y: Eh, nou, ik ben wel benieuwd hoe je op een gegeven moment dat spectrum definieert van experts en eh, mensen die totaal niet, die niet eens weten wat VPN betekent.

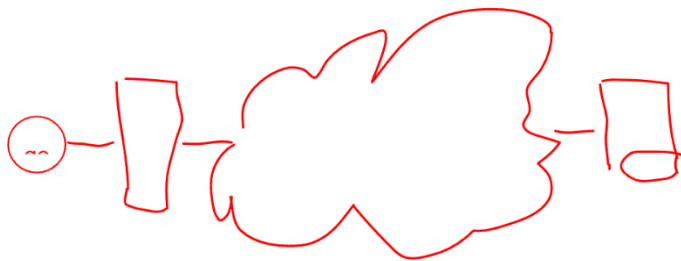


Figure C.18.1: Drawing 18_1

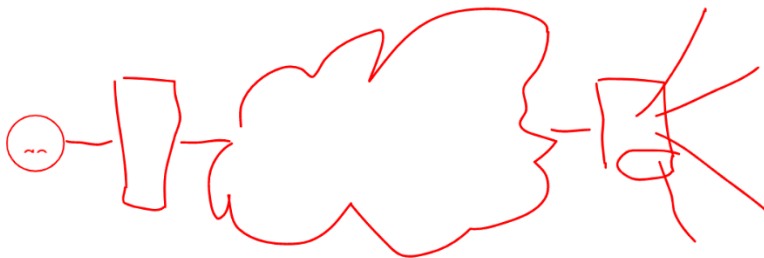


Figure C.18.2: Drawing 18_2

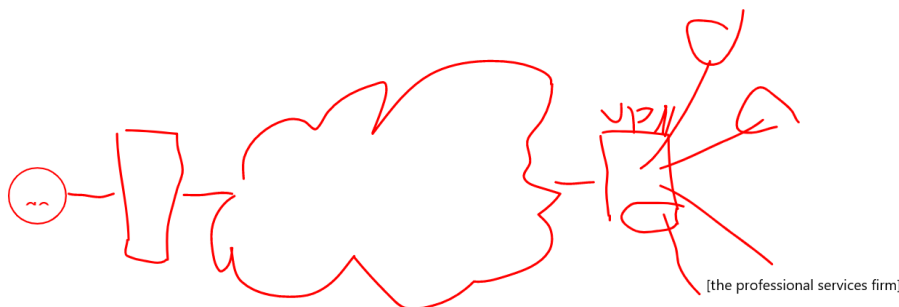


Figure C.18.3: Drawing 18_3

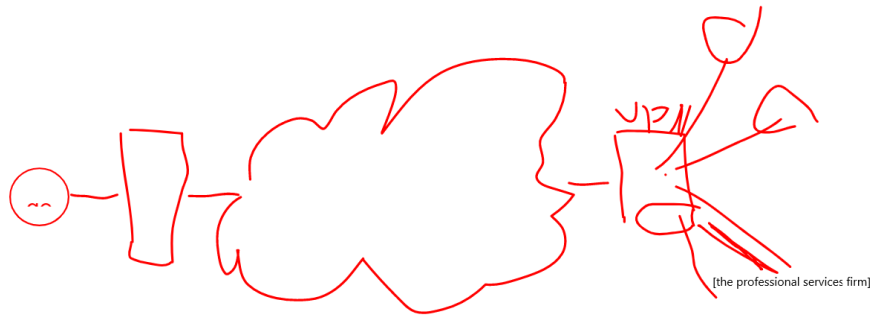


Figure C.18.4: Drawing 18_4



Figure C.18.5: Drawing 18_5



Figure C.18.6: Drawing 18_6

Appendix D: Code book and Frequency Distribution Codes

This appendix contains the codebook and frequency distribution of the codes. Codes do not indicate what was said, until a certain point. When for example a location of a VPN server is named this can mean that it is a possibility or that it is not a possibility. Thus the code frequency indicates that the topic is named, but not what was said.

The codebook is built in a tree structure, where possible a more specific code is used, but otherwise a higher-level, more general code can be used.

In the tables, the frequency indicates in which interview and how often a code is mentioned. Total represents the total amount a code is mentioned, % is percentage of interviewees mentioning code.

The belief was defined as a personal belief at the perceptual level about the effect or value of concepts or relations between them.

D.1: Code book perception of how a VPN works

This section presents the code book for the perception of how a VPN works and the frequency distribution of those codes in the interviews.

Table D.1.1: Code book perception of how a VPN works

Reason for use	
Virtual Private Network	Description: the abbreviation VPN full out is Virtual Private Network Inclusion criteria: statement is related to the corporate VPN connection AND names the concept Virtual Private Network. Exclusion criteria: -
Access internal network	Description: the purpose of a VPN is to access the internal network Inclusion criteria: this code is related to statements about the purpose of use of a corporate VPN connection AND refers to the purpose being accessing the internal corporate network (i.e. access internal network, access private network, access private websites, accessing internal page, accessing internal services, accessing internal resources). Exclusion criteria: NOT access from outside the network
Access from outside the network (location)	Description: the purpose of a VPN is to access the internal network when located outside the network Inclusion criteria: statement is related to the purpose of a corporate VPN connection AND refers to the purpose as accessing the internal network when located outside the network (i.e. from outside of the office or from anywhere in the world). Exclusion criteria: -
Not necessary when in office	Description: it is not needed to establish a VPN connection when you are in the office. Inclusion criteria: this code is related to statements about a situation which leads to not establishing the corporate VPN connection AND refers to not needing to establish a VPN connection when you are in the office. Exclusion criteria: -
Internal network: impossible to directly connect	Description: it is not possible to directly connect to the internal network Inclusion criteria: The statement is about a corporate VPN connection AND refers to the impossibility of directly connecting to the internal network OR to the internal network as only being accessible via a VPN connection Exclusion criteria: NOT describing the purpose of a VPN connection being to access the internal network
Internal network: accessible without VPN connection	Description: it is possible to directly connect to the internal network, without needing a VPN connection Inclusion criteria: The statement is about a corporate VPN connection AND refers to the possibility of directly connecting to the internal network Exclusion criteria: -
Security purpose general	Description: the purpose of VPN is security Inclusion criteria: statement is related to the purpose of use of a corporate VPN connection and refers to the purpose being security

	Exclusion criteria: NOT purpose being to secure the connection AND NOT to secure the communication
Secure connection	Description: the purpose of VPN is to secure the connection Inclusion criteria: this code is related to statements about the purpose of use of a corporate VPN connection and refers to the purpose being to secure the connection Exclusion criteria: NOT purpose being to secure the communication
Secure communication	Description: the purpose of VPN is to secure communication Inclusion criteria: this code is related to statements about the purpose of use of a corporate VPN connection and refers to the purpose being to secure communication Exclusion criteria: NOT purpose being to secure the connection
Used when using unsecured network	Description: a VPN connection is used when an unsecured network is used Inclusion criteria: the statement is about a situation which leads to establishing the corporate VPN connection AND refers to using a VPN connection when an unsecured network is used. Exclusion criteria: -
Mobile network used instead of unsecured network	Description: it is preferred to use a mobile network instead of an unsecured network Inclusion criteria: the statement is about a situation which leads or does not lead to establishing the corporate VPN connection AND refers to preferring to use a mobile network instead of an unsecured network. Exclusion criteria: -
Used when using mobile network	Description: a VPN connection is used when the mobile network is used Inclusion criteria: the statement is about a situation which leads or does not lead to establishing the corporate VPN connection AND refers to using a VPN connection when the mobile network is used. Exclusion criteria: -
Not used when using mobile network	Description: a VPN connection is not used when the mobile network is used Inclusion criteria: the statement is about a situation which leads to not establishing the corporate VPN connection AND refers to not using a VPN connection when the mobile network is used. Exclusion criteria: -
Use unsecured network if mobile network is expensive	Description: the reason of using an unsecured network are the costs for using a mobile network Inclusion criteria: the statement is about a situation which leads or does not lead to establishing the corporate VPN connection AND refers to the reason of using an unsecured network as being the costs for using a mobile network. Exclusion criteria: -
Device	
Mobile	Description: a VPN can be used on a mobile Inclusion criteria: the statement is about a device that is used to establish a corporate VPN connection AND names a mobile phone as such device. Exclusion criteria: -
Personal computer	Description: a VPN can be used on a personal computer Inclusion criteria: the statement is about a device that is used to establish a corporate VPN connection AND names a computer as such device (i.e. laptop or personal computer). Exclusion criteria: -
Tablet	Description: a VPN can be used on a tablet Inclusion criteria: the statement is about a device that is used to establish a corporate VPN connection AND names a tablet as such device. Exclusion criteria: -
User actions to establish a connection	
Access token	Description: an access token creates a code needed for authentication Inclusion criteria: statement is related to the corporate VPN connection AND names the concept access token. Exclusion criteria: NOT referring to hardware token AND NOT referring to software token AND not referring to enter code access token
Access token: hardware token	Description: a physical access token Inclusion criteria: statement is related to the corporate VPN connection AND refers to the existence of a hardware token as an access token. Exclusion criteria: -
Access token: software token	Description: software that serves as an access token Inclusion criteria: statement is related to the corporate VPN connection AND refers to the

	existence of a software token as an access token. Exclusion criteria: -
Click connect to VPN	Description: selecting the button to connect to the VPN after filling in the credentials Inclusion criteria: this code is related to statements about the user actions taken to establish a corporate VPN connection AND refers to selecting the button to connect to the VPN. Exclusion criteria: -
Connect to Internet	Description: connecting to the Internet to establish a VPN connection Inclusion criteria: this code is related to statements about the user actions taken to establish a corporate VPN connection AND refers to connecting to the Internet (i.e. connecting to the Internet, the router, the modem, Internet gateway, or access point). Exclusion criteria: -
Enter code access token	Description: entering the code presented by the access token Inclusion criteria: this code is related to statements about the user actions taken to establish a corporate VPN connection AND refers to entering the code presented by the access token. Exclusion criteria: -
Enter password	Description: entering the password Inclusion criteria: this code is related to statements about the user actions taken to establish a corporate VPN connection AND refers to entering the password. Exclusion criteria: -
Enter username	Description: entering the username Inclusion criteria: this code is related to statements about the user actions taken to establish a corporate VPN connection AND refers to entering the username. Exclusion criteria: -
Launch VPN software	Description: launching the VPN software before filling in the credentials. Inclusion criteria: this code is related to statements about the user actions taken to establish a corporate VPN connection AND refers to launching the VPN software. Exclusion criteria: -
Basic configuration	
Make connection	Description: a connection is made Inclusion criteria: this code is related to statements about the process to establish a corporate VPN connection AND refers to making a connection Exclusion criteria: NOT specifying making a connection with a server
Make connection with server	Description: a connection is made with a server Inclusion criteria: this code is related to statements about the process to establish a corporate VPN connection AND establishing a connection with a server. Exclusion criteria: -
Authentication	Description: the process of verifying one's identity Inclusion criteria: this code is related to statements about the process to establish a corporate VPN connection AND refers to authentication. Exclusion criteria: NOT specifying authentication by VPN server
Authentication by server	Description: the process of verifying one's identity by a VPN server Inclusion criteria: this code is related to statements about the process to establish a corporate VPN connection AND refers to authentication by a server. Exclusion criteria: -
Webtraffic is routed through server	Description: webtraffic is routed through the VPN server Inclusion criteria: this code is related to statements about the established corporate VPN connection AND refers to webtraffic being routed through the VPN server. Exclusion criteria: -
Server	Description: a computer program or a device that provides functionality for other programs or devices, called clients Inclusion criteria: statement is related to the corporate VPN connection AND names the concept server. Exclusion criteria: NOT referring to establishing a connection with a server AND NOT referring to authentication by a server AND NOT referring to an external server can function for only authentication AND not referring to the location of the server AND NOT referring to webtraffic goes through server AND NOT referring to encryption of the connection AND NOT referring to a private IP-address
Internal network	Description: the corporate network Inclusion criteria: The statement is about a corporate VPN connection AND names the concept internal network OR refers to the corporate network Exclusion criteria: NOT refer to the purpose being accessing the internal corporate network AND NOT refer to internal network segmentation AND NOT refer to impossible to directly

Internal network: uses whitelisting for access management	connect AND NOT refer to uses whitelisting for access management AND NOT refer to accessible without VPN connection AND NOT refer to the location of a VPN server Description: the internal network uses whitelisting for access management IP-addresses. Inclusion criteria: The statement is about a corporate VPN connection AND refers to the internal network using whitelisting for access management IP-addresses (i.e. the internal network uses whitelisting to determine which IP-addresses can access the internal network or the internal network uses a database containing IP-addresses to determine which IP-addresses can access the internal network). Exclusion criteria: NOT VPN filters traffic
Internet	Description: any statement which refers to Internet Inclusion criteria: statement is related to the corporate VPN connection AND names the concept Internet. Exclusion criteria: NOT referring to Internet service provider
Internet service provider	Description: an organisation that provides services for accessing, using, or participating in the Internet Inclusion criteria: statement is related to the corporate VPN connection AND names the concept Internet service provider. Exclusion criteria: NOT referring to ISP as a threat actor
IP-address	Description: a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication Inclusion criteria: statement is related to the corporate VPN connection AND names the concept IP-address. Exclusion criteria: NOT refers to the use of an IP-address as identification of endpoints NOT refers to an IP-address as private for the VPN server AND NOT refers to the private IP-address of the receiving endpoint and the VPN server as only known between the VPN server and the endpoint AND NOT referring to mask IP-address
IP-address used to identify endpoint	Description: the use of an IP-address as identification of endpoints. Inclusion criteria: statement is related to the corporate VPN connection AND refers to the use of an IP-address as identification of endpoints. Exclusion criteria: -
External server can function for only authentication	Description: In a specific situation, a server outside of the corporate environment can be used for authentication and is not used for other purposes. It implies that the server that is used for authentication does not need to be the same as the server a connection is made with. Inclusion criteria: this code is related to statements about the process to establish a corporate VPN connection AND refers to an external server can function for only authentication Exclusion criteria: -
Server: in demilitarized zone	Description: the server used for authentication or used to establish a VPN connection is located inside the demilitarized zone Inclusion criteria: this code is related to statements about the corporate VPN connection AND names the concept server when referring to the server that is used for authentication or used to establish the VPN connection AND refers to the location of the server as inside the demilitarized zone. Exclusion criteria: -
Server: inside corporate network	Description: the server used for authentication or used to establish a VPN connection is located inside the corporate network Inclusion criteria: this code is related to statements about the corporate VPN connection AND names the concept server when referring to the server that is used for authentication or used to establish the VPN connection AND refers to the location of the server as inside the corporate network. Exclusion criteria: NOT server is located in demilitarized zone
Server: outside corporate network	Description: the server used for authentication or used to establish a VPN connection is located outside the corporate network Inclusion criteria: this code is related to statements about the corporate VPN connection AND names the concept server when referring to the server that is used for authentication or used to establish the VPN connection AND refers to the location of the server as outside the corporate network. Exclusion criteria: -
Additional specifications	
VPN complete or split	Description: A distinction exists between a complete VPN, where all webtraffic goes through the VPN server when connected, and a split VPN, where not all webtraffic goes through the VPN server when connected Inclusion criteria: statement is related to the corporate VPN connection AND refers to the

	concept VPN complete or split. Exclusion criteria: -
Internal network segmentation	Description: the internal network is divided into segments Inclusion criteria: The statement is about a corporate VPN connection AND refers to internal network segmentation Exclusion criteria: -
VPN provider	Description: the party providing the VPN services Inclusion criteria: statement is related to the corporate VPN connection AND refers to the concept VPN provider. Exclusion criteria: NOT specifying who the VPN provider is (i.e. own or third party) AND NOT referring to one organization can have multiple
One organization can have multiple VPN providers	Description: one organization can have multiple VPN providers Inclusion criteria: statement is related to the corporate VPN connection AND refers to the possibility of having multiple VPN providers for one company. Exclusion criteria: -
Own VPN provider	Description: the VPN provider is the professional services firm itself Inclusion criteria: statement is related to the corporate VPN connection AND refers to the VPN provider being the professional services firm itself. Exclusion criteria: -
Third party is VPN provider	Description: the VPN provider is a third party Inclusion criteria: statement is related to the corporate VPN connection AND refers to the VPN provider being a third party. Exclusion criteria: -
Secured connection	
Secured connection	Description: a connection that is in some way secured Inclusion criteria: statement is related to a corporate VPN connection AND refer to a secured connection. Exclusion criteria: NOT refer to a secure connection as the purpose of the VPN connection
Encryption	Description: coding data in a way that it is not readable to anyone but the parties it is intended for Inclusion criteria: statement is related to the corporate VPN connection AND names the concept encryption. Exclusion criteria: NOT referring to connection is encrypted between own device and VPN server AND NOT referring to data is send to receiving point encrypted AND NOT referring to data is send to receiving point decrypted AND NOT referring to firewall can decrypt communication AND NOT referring to load balancer can decrypt communication
Protocol	Description: a set of rules Inclusion criteria: statement is related to the corporate VPN connection AND names the concept protocol. Exclusion criteria: -
Data is send to receiving point decrypted	Description: data is send to the receiving point decrypted Inclusion criteria: this code is related to statements about the established corporate VPN connection AND refers to data being send to the receiving point decrypted. Exclusion criteria: -
Data is send to receiving point encrypted	Description: data is send to the receiving point encrypted Inclusion criteria: this code is related to statements about the established corporate VPN connection AND refers to data being send to the receiving point encrypted. Exclusion criteria: NOT referring to the connection being encrypted between own device and VPN server
Is encrypted between own device and VPN server	Description: data is encrypted between the user's device and the VPN server Inclusion criteria: this code is related to statements about the established corporate VPN connection AND refers to data being encrypted between the user's device and the VPN server. Exclusion criteria: -
Firewall can decrypt communication	Description: thia firewall can decrypt communication Inclusion criteria: statement is related to the corporate VPN connection AND refering to the use of a firewall as decrypting communication. Exclusion criteria: -
Load balancer can decrypt communication	Description: a load balancer can decrypt communication Inclusion criteria: statement is related to the corporate VPN connection AND refering to the use of a load balancer as decrypting communication. Exclusion criteria: -
VPN filters traffic	Description: it is mentioned that the VPN in some way is able to scan and / or filter webtraffic, this traffic can be either inbound or outbound. Examples are that the VPN makes it impossible

	to visit certain websites (using blacklisting or whitelisting for example), the VPN includes a firewall (either in the VPN server itself or because of the VPN connection the traffic goes through a firewall), or the traffic goes through a IDS or IPS. Inclusion criteria: this code is related to statements about the established corporate VPN connection AND refers to VPN filtering traffic. Exclusion criteria: -
VPN includes antivirus	Description: VPN includes a form of antivirus Inclusion criteria: this code is related to statements about the established corporate VPN connection AND refers to VPN including an antivirus. Exclusion criteria: -
IP-address private for VPN server	Description: the VPN server has a private IP-address Inclusion criteria: statement is related to the corporate VPN connection AND refers to an IP-address as private for the VPN server. Exclusion criteria: NOT refers to the private IP-address of the receiving endpoint and the VPN server as only known between this endpoint and VPN server AND NOT referring to masking of the IP-address
IP-address private is only known by VPN server and endpoint	Description: the private IP-address of the receiving endpoint and the VPN server is only known between this endpoint and VPN server. Inclusion criteria: statement is related to the corporate VPN connection AND refers to the private IP-address of the receiving endpoint and the VPN server as only known between this endpoint and VPN server. Exclusion criteria: NOT referring to masking of the IP-address
Metaphors	
Tunnel	Description: statements referring to a tunnel (i.e. as a metaphor) Inclusion criteria: statement is related to the corporate VPN connection AND names the concept tunnel. Exclusion criteria: -

Table D.1.2: Distribution of codes in reason for use for experts

Code	1	2	3	4	5	6	7	8	9	10	11	Total	%
Virtual Private Network	1	1	2	0	0	1	0	1	0	0	1	7	54,5%
Access internal network	3	4	7	4	2	2	1	1	2	2	5	33	100%
Access from outside the network	0	4	5	0	2	0	1	1	0	0	1	14	54,5%
Not necessary when in office	1	0	3	0	0	1	1	0	0	0	2	8	45,5%
Internal network: impossible to directly connect	2	3	2	1	1	1	0	0	1	2	3	16	81,8%
Internal network: accessible without VPN connection	0	0	0	0	0	2	0	0	0	0	0	2	9,1%
Security purpose general	0	0	0	1	0	1	0	1	0	0	0	4	36,4%
Secure connection	2	2	1	2	1	1	0	2	2	1	1	15	90,9%
Secure communication	0	0	0	0	0	0	0	3	0	0	0	3	9,1%
Used when using unsecured network	1	1	2	0	1	0	0	0	1	1	0	7	54,5%
Mobile network used instead of unsecured network	1	0	1	0	1	0	1	0	0	2	0	6	45,5%
Used when using mobile network	1	0	1	0	0	0	0	0	0	3	0	5	27,3%
Not used when using mobile network	0	0	0	0	0	0	1	0	0	0	0	1	9,1%
Use unsecured network if mobile network is expensive	0	0	1	0	0	0	0	0	0	0	0	1	9,1%

Table D.1.3: Distribution of codes in reason for use for laypeople

Code	1	2	3	4	5	6	7	Total	%
Virtual Private Network	0	0	0	1	0	1	0	2	28,6%
Access internal network	3	2	1	3	2	1	2	14	100%
Access from outside the network	2	0	0	2	0	0	0	4	28,6%
Not necessary when in office	0	0	0	0	0	0	0	0	0,0%
Internal network: impossible to directly connect	2	0	0	0	2	1	3	8	57,1%
Internal network: accessible without VPN connection	0	0	0	0	0	0	0	0	0,0%
Security purpose general	1	0	0	1	0	0	0	2	28,6%
Secure connection	0	2	0	0	0	1	0	3	28,6%
Secure communication	0	0	0	0	0	3	0	3	14,3%
Used when using unsecured network	0	1	0	0	1	0	1	3	42,9%
Mobile network used instead of unsecured network	0	0	0	0	0	0	0	0	0,0%
Used when using mobile network	0	0	0	0	0	0	0	0	0,0%
Not used when using mobile network	0	0	0	0	0	0	0	0	0,0%
Use unsecured network if mobile network is expensive	0	0	0	0	0	0	0	0	0,0%

Table D.1.4: Distribution of codes in device for experts

Code	1	2	3	4	5	6	7	8	9	10	11	Total	%
Personal computer	2	1	1	1	1	1	1	1	1	1	1	12	100%
Mobile Phone	2	2	1	0	0	1	2	0	0	1	0	9	54,5%
Tablet	1	0	0	0	0	0	0	0	0	1	0	2	18,2%

Table D.1.5: Distribution of codes in device for laypeople

Code	1	2	3	4	5	6	7	Total	%
Personal computer	1	2	1	1	1	3	1	10	100%
Mobile Phone	0	1	1	1	0	0	2	5	57,1%
Tablet	0	0	0	1	0	0	0	1	14,3%

Table D.1.6: Distribution of codes in user actions for experts

Code	1	2	3	4	5	6	7	8	9	10	11	Total	%
Connect to Internet	0	1	1	1	1	0	0	0	0	2	0	6	45,5%
Launch VPN software	0	1	1	1	1	0	0	0	1	1	1	7	63,6%
Enter username	1	0	0	1	1	0	1	1	0	2	1	8	63,6%
Enter password	1	1	1	1	0	1	1	1	1	2	3	13	90,9%
Enter code access token	1	1	1	0	1	1	1	2	1	2	2	13	90,9%
Click connect to VPN	0	1	1	1	0	0	0	0	0	0	0	3	27,3%
Access token	0	2	1	0	2	4	1	1	1	0	0	12	54,5%
Access token: hardware token	3	1	2	0	3	1	1	1	1	1	1	15	90,9%
Access token: software token	3	1	3	0	4	2	2	1	1	1	1	19	90,9%

Table D.1.7: Distribution of codes in user actions for laypeople

Code	1	2	3	4	5	6	7	Total	%
Connect to Internet	1	0	0	0	0	1	0	2	28,6%
Launch VPN software	2	1	1	1	1	2	1	9	100%

Enter username	0	0	0	0	0	0	0	0	0,0%
Enter password	3	1	1	1	0	1	1	8	85,7%
Enter code access token	2	1	1	1	1	1	1	8	100%
Click connect to VPN	2	0	1	0	1	0	0	4	42,9%
Access token	0	0	0	0	0	0	0	0	0,0%
Access token: hardware token	1	1	1	1	2	1	0	7	85,7%
Access token: software token	2	1	1	2	1	2	0	9	85,7%

Table D.1.8: Distribution of codes in infrastructure for experts

Code	1	2	3	4	5	6	7	8	9	10	11	Total	%
Make connection	0	0	1	0	3	0	0	0	0	0	3	7	27,3%
Make connection with server	1	1	6	2	1	0	5	2	0	3	3	24	81,8%
Authentication	2	0	1	1	5	1	2	0	1	0	2	15	72,7%
Authentication by server	2	0	0	0	0	0	0	0	1	2	5	10	36,4%
Webtraffic is routed through server	1	0	3	7	0	0	3	0	4	3	3	24	63,6%
Server	9	0	3	7	0	0	8	6	4	8	0	45	63,6%
Internal network	3	2	7	0	5	2	1	0	3	4	8	35	81,8%
Internal network: uses whitelisting for access management	0	0	0	1	0	0	0	0	0	0	1	2	18,2%
Internet	7	5	6	3	5	0	8	4	7	5	4	54	90,9%
Internet Service Provider	1	0	1	0	2	0	0	0	0	0	0	4	27,3%
IP-address	2	0	1	4	0	0	0	1	1	1	0	10	54,5%
IP-address used to identify endpoint	5	0	0	1	0	0	0	0	1	1	1	9	45,5%
Server: in demilitarized zone	1	0	0	0	0	0	0	0	0	0	0	1	9,1%
Server: inside corporate network	1	0	0	0	0	0	1	0	0	0	4	6	27,3%
Server: outside corporate network	1	0	0	0	0	0	0	0	0	0	3	4	18,2%
external server can function for only authentication	1	0	0	0	0	0	0	0	0	0	2	3	18,2%
VPN complete or split	3	0	0	0	0	0	0	0	0	0	2	5	18,2%
Internal network segmentation	3	0	0	0	0	0	0	0	0	0	4	7	18,2%
VPN provider	3	0	0	0	0	0	0	1	0	0	0	4	18,2%
VPN provider: own provider	1	0	0	0	0	0	0	0	0	0	0	1	9,1%
VPN provider: third party	1	0	0	3	0	0	0	0	0	0	0	4	18,2%
VPN provider: one organization can have multiple	1	0	0	0	0	0	0	0	0	0	0	1	9,1%

Table D.1.9: Distribution of codes in infrastructure for laypeople

Code	1	2	3	4	5	6	7	Total	%
Make connection	2	0	2	0	2	2	1	9	71,4%
Make connection with server	0	0	0	0	0	0	1	1	14,3%
Authentication	0	0	2	0	2	1	0	5	42,9%
Authentication by server	0	0	0	0	0	0	0	0	0,0%
Webtraffic is routed through server	0	0	0	0	0	0	2	2	14,3%

Server	2	3	0	0	5	0	1	11	57,1%
Internal network	4	1	0	0	2	1	1	9	71,4%
Internal network: uses whitelisting for access management	0	0	0	0	0	0	0	0	0,0%
Internet	2	3	0	0	3	1	2	11	71,4%
Internet Service Provider	0	4	0	0	0	0	0	4	14,3%
IP-address	0	0	0	0	0	0	0	0	0,0%
IP-address used to identify endpoint	0	0	0	0	0	0	0	0	0,0%
Server: in demilitarized zone	0	0	0	0	0	0	0	0	0,0%
Server: inside corporate network	0	0	0	0	0	0	0	0	0,0%
Server: outside corporate network	0	0	0	0	0	0	0	0	0,0%
external server can function for only authentication	0	0	0	0	0	0	0	0	0,0%
VPN complete or split	0	0	0	0	0	0	0	0	0,0%
Internal network segmentation	0	0	0	0	0	0	0	0	0,0%
VPN provider	0	0	0	0	0	0	0	0	0,0%
VPN provider: own provider	0	0	0	0	0	0	0	0	0,0%
VPN provider: third party	1	0	0	0	0	0	0	1	14,3%
VPN provider: one organization can have multiple	0	0	0	0	0	0	0	0	0,0%

Table D.1.10: Distribution of codes in secured connection for experts

Code	1	2	3	4	5	6	7	8	9	10	11	Total	%
Secured connection	2	3	2	8	6	2	5	4	4	3	2	41	100%
Encryption	2	6	7	0	2	0	6	3	0	5	6	37	72,7%
Protocol	3	0	5	0	0	0	0	1	0	0	2	11	36,4%
Data is send to receiving point decrypted	2	0	0	0	0	0	1	0	0	1	2	6	36,4%
Data is send to receiving point encrypted	1	1	0	1	0	0	1	0	0	0	1	5	45,5%
Connection is encrypted between own device and VPN server	1	1	0	2	0	0	1	0	0	4	1	10	54,5%
Firewall can decrypt communication	1	0	0	0	0	0	0	0	0	0	0	1	9,1%
Load balancer can decrypt communication	2	0	0	0	0	0	0	0	0	0	0	2	9,1%
VPN filters traffic	1	0	0	4	0	0	0	0	9	3	3	20	45,5%
VPN includes antivirus	0	0	0	5	0	0	0	0	0	0	0	5	9,1%
IP-address: private for VPN server	0	0	0	4	0	0	0	0	0	0	0	4	9,1%
IP-address: private is only known by VPN server and endpoint	0	0	0	1	0	0	0	0	0	0	0	1	9,1%

Table D.1.11: Distribution of codes in secured connection for laypeople

Code	1	2	3	4	5	6	7	Total	%
Secured connection	1	1	0	0	4	0	1	7	57,1%
Encryption	0	1	0	1	0	3	4	9	57,1%
Protocol	0	0	0	0	0	0	0	0	0,0%
Data is send to receiving point decrypted	0	0	0	0	0	0	0	0	0,0%
Data is send to receiving point encrypted	0	0	0	0	0	0	3	3	14,3%
Connection is encrypted between own device and VPN server	0	0	0	0	0	0	1	1	14,3%

Firewall can decrypt communication	0	0	0	0	0	0	0	0	0	0,0%
Load balancer can decrypt communication	0	0	0	0	0	0	0	0	0	0,0%
VPN filters traffic	0	0	0	0	0	0	0	0	0	0,0%
VPN includes antivirus	0	0	0	0	0	0	0	0	0	0,0%
IP-address: private for VPN server	0	0	0	0	0	0	0	0	0	0,0%
IP-address: private is only known by VPN server and endpoint	0	0	0	0	0	0	0	0	0	0,0%

Table D.1.12: Distribution of codes in metaphors for experts

Code	1	2	3	4	5	6	7	8	9	10	11	Total	%
Tunnel	3	3	5	0	3	2	5	5	0	2	0	28	72,7%

Table D.1.13: Distribution of codes in metaphors for laypeople

Code	1	2	3	4	5	6	7	Total	%
Tunnel	0	10	0	0	0	0	0	10	14,3%

D.2: Code book perception of the current threat landscape

This section presents the code book for the perception of the current threat landscape and the frequency distribution of those codes in the interviews.

Table D.2.1: Code book perception of the current threat landscape

Threats	
Collection	Description: The adversary is trying to gather data of interest to their goal (i.e. man-in-the-middle attack, online behavior monitored) Inclusion criteria: this code is related to statements about kinds of threats in general and refers to Collection as a possible threat Exclusion criteria: NOT referring to credential access
Credential access	Description: The adversary is trying to steal account names and passwords (i.e. brute force, shoulder surfing, credentials visible when using unsecured network, logging into a fake website) Inclusion criteria: this code is related to statements about kinds of threats in general and refers to credential access as a possible threat Exclusion criteria: -
Execution	Description: The adversary is trying to run malicious code (i.e. malware, ransomware) Inclusion criteria: this code is related to statements about kinds of threats in general and refers to Execution as a possible threat Exclusion criteria: -
Exfiltration	Description: The adversary is trying to steal data Inclusion criteria: this code is related to statements about kinds of threats in general and refers to Exfiltration as a possible threat Exclusion criteria: -
Hacking	Description: statement refers to hacking as a threat, without specifying further Inclusion criteria: this code is related to statements about kinds of threats in general and refers to hacking as a possible threat Exclusion criteria: -
Impact	Description: The adversary is trying to manipulate, interrupt, or destroy your systems and data (i.e. ddos attack, manipulate endpoints) Inclusion criteria: this code is related to statements about kinds of threats in general and refers to Impact as a possible threat Exclusion criteria: -

Initial access	Description: The adversary is trying to get into your network (i.e. access to device, attacker accessing unlocked device, attacker connects to office wifi, device stolen, manipulate devices that establish Internet connection, phishing, poor access management, social engineering, being physically followed into building, receiving information through non approved channels). Inclusion criteria: this code is related to statements about kinds of threats in general and refers to Initial access as a possible threat Exclusion criteria: -
Many threats mitigated by firm	Description: statement refers to many threats being mitigated by the professional services firm Inclusion criteria: this code is related to statements about kinds of threats in general and refers to many threats are mitigated by the professional services firm Exclusion criteria: -
Privilege escalation	Description: The adversary is trying to gain higher-level permissions Inclusion criteria: this code is related to statements about kinds of threats in general and refers to Privilege escalation as a possible threat Exclusion criteria: -
There are many	Description: statement refers to the existence of many possible threats Inclusion criteria: this code is related to statements about kinds of threats in general and refers to there are many Exclusion criteria: -
Unintentional threat	Description: The action is not done by an adversary (i.e. leave device somewhere, send e-mail to wrong receiver) Inclusion criteria: this code is related to statements about kinds of threats in general and refers to an unintentional threat as a possible threat Exclusion criteria: -
Threat actor	
Clients	Description: something or someone who receives professional services from an organization Inclusion criteria: this code is related to statements about threat actors in general and refers to clients as a possible threat actor Exclusion criteria: -
Company with malicious intent	Description: a company with malicious intent is a company that has the intention to harm Inclusion criteria: this code is related to statements about threat actors in general and refers to a company with malicious intent as a possible threat actor Exclusion criteria: NOT referring to a competitor AND NOT referring to a social media company AND NOT referring to ISP
Competitor	Description: a competitor is a company that is trying to compete with another company Inclusion criteria: this code is related to statements about threat actors in general and refers to competitors as a possible threat actor Exclusion criteria: -
Cracker	Description: a cracker performs cracking, the process of breaking into a computer or a network system (i.e. a cybervandal or scriptkiddie, rejected applicant, neighbour) Inclusion criteria: this code is related to statements about threat actors in general and refers to crackers as a possible threat actor Exclusion criteria: -
Hacktivists	Description: a hacktivist is someone who gets into computer systems without permission in order to achieve political aims Inclusion criteria: this code is related to statements about threat actors in general and refers to hacktivists as a possible threat actor Exclusion criteria: -
Insider	Description: an insider is someone who works for a company and therefore has special knowledge or influence (including disgruntled ex-employee) Inclusion criteria: this code is related to statements about threat actors in general and refers to insiders as a possible threat actor Exclusion criteria: -
Internet Service Provider	Description: an organisation that provides services for accessing, using, or participating in the Internet Inclusion criteria: this code is related to statements about threat actors in general and refers to Internet Service Provider as a possible threat actor Exclusion criteria: -
Professional criminals	Description: Criminals with experience, special training or education (i.e. criminal organization) Inclusion criteria: this code is related to statements about threat actors in general and refers to professional criminals as a possible threat actor Exclusion criteria: -

Social media company	Description: a company that owns websites and computer programs that allow people to communicate and share information on the Internet Inclusion criteria: this code is related to statements about threat actors in general and refers to a social media company as a possible threat actor Exclusion criteria: -
State actor	Description: a country or its government Inclusion criteria: this code is related to statements about threat actors in general and refers to a state actor as a possible threat actor Exclusion criteria: -
State-sponsored network	Description: State-affiliated groups which are organized in networks Inclusion criteria: this code is related to statements about threat actors in general and refers to a state-sponsored network actor as a possible threat actor Exclusion criteria: -
Terrorist	Description: Threat actor who uses violent action, or threats of violent action, for political purposes Inclusion criteria: this code is related to statements about threat actors in general and refers to a state-sponsored network actor as a possible threat actor Exclusion criteria: -
There are many	Description: there are many possible threat actors Inclusion criteria: this code is related to statements about threat actors in general and refers to the existence of many possible threat actors Exclusion criteria: -
Threat actor motivation	
Coercion	Description: Forced to act illegally on behalf of another (i.e. intimidation, blackmail) Inclusion criteria: this code is related to statements about the motivation of threat actors in general and refers to coercion as a possible motivation Exclusion criteria: -
Disgruntlement	Description: a desire to avenge perceived wrongs through harm Inclusion criteria: this code is related to statements about the motivation of threat actors in general and refers to disgruntlement as a possible motivation Exclusion criteria: -
Ideology	Description: a passion to express a set of ideas, beliefs, and values that shapes and drives harmful acts (includes geopolitical motivation) Inclusion criteria: this code is related to statements about the motivation of threat actors in general and refers to ideology as a possible motivation Exclusion criteria: -
Notoriety	Description: seeking to become well known for harmful activity Inclusion criteria: this code is related to statements about the motivation of threat actors in general and refers to notoriety as a possible motivation Exclusion criteria: -
Organizational gain	Description: seeking an advantage over a competitor's organization Inclusion criteria: this code is related to statements about the motivation of threat actors in general and refers to organizational gain as a possible motivation Exclusion criteria: -
Personal financial gain	Description: Improve one's own financial status Inclusion criteria: this code is related to statements about the motivation of threat actors in general and refers to personal financial gain as a possible motivation Exclusion criteria: NOT organizational gain
Personal satisfaction	Description: Fulfilling an emotional self-interest Inclusion criteria: this code is related to statements about the motivation of threat actors in general and refers to personal satisfaction as a possible motivation Exclusion criteria: NOT notoriety
There are many	Description: there are many possible motivations Inclusion criteria: statements about motivation of threat actors in general and refers to the existence of many possible motivations Exclusion criteria: -
Coercion	Description: Forced to act illegally on behalf of another (i.e. intimidation, blackmail) Inclusion criteria: this code is related to statements about the motivation of threat actors in general and refers to coercion as a possible motivation Exclusion criteria: -
Disgruntlement	Description: a desire to avenge perceived wrongs through harm Inclusion criteria: this code is related to statements about the motivation of threat actors in

	general and refers to disgruntlement as a possible motivation Exclusion criteria: -
Ideology	Description: a passion to express a set of ideas, beliefs, and values that shapes and drives harmful acts (includes geopolitical motivation) Inclusion criteria: this code is related to statements about the motivation of threat actors in general and refers to ideology as a possible motivation Exclusion criteria: -
Notoriety	Description: seeking to become well known for harmful activity Inclusion criteria: this code is related to statements about the motivation of threat actors in general and refers to notoriety as a possible motivation Exclusion criteria: -
Organizational gain	Description: seeking an advantage over a competitor's organization Inclusion criteria: this code is related to statements about the motivation of threat actors in general and refers to organizational gain as a possible motivation Exclusion criteria: -
Personal financial gain	Description: Improve one's own financial status Inclusion criteria: this code is related to statements about the motivation of threat actors in general and refers to personal financial gain as a possible motivation Exclusion criteria: NOT organizational gain
Personal satisfaction	Description: Fulfilling an emotional self-interest Inclusion criteria: this code is related to statements about the motivation of threat actors in general and refers to personal satisfaction as a possible motivation Exclusion criteria: NOT notoriety
There are many	Description: there are many possible motivations Inclusion criteria: statements about motivation of threat actors in general and refers to the existence of many possible motivations Exclusion criteria: -
Threat actor capability	
Adept skills	Description: Expert in technology and attack methods, and can both apply existing attacks and create new ones to greatest advantage (i.e. certified hacker) Inclusion criteria: this code is related to statements about the capability of a threat actor in general and refers to adept skills Exclusion criteria: -
Minimal skills	Description: Threat actor can copy and use existing techniques (i.e. basic social engineer) Inclusion criteria: this code is related to statements about the capability of a threat actor in general and refers to minimal skills Exclusion criteria: -
No skills	Description: Threat actor has average intelligence and ability and can easily carry out random acts of disruption or destruction, but has no expertise or training in the specific methods necessary for a targeted attack. (i.e. needs social connections to an employee, access to financial resources) Inclusion criteria: this code is related to statements about the capability of a threat actor in general and refers to no skills Exclusion criteria: -
Operational skills	Description: Understands underlying technology or methods and can create new attacks within a narrow domain (i.e. hacking skills, broad technical education, experienced social engineer) Inclusion criteria: this code is related to statements about the capability of a threat actor in general and refers to operational skills Exclusion criteria: -
Threat impact	
Data manipulation	Description: Impairment of the integrity of information by means of the intentional editing of data Inclusion criteria: this code is related to statements about the impact of an attack in general and refers to information manipulation as a possible impact Exclusion criteria: -
Data theft	Description: Impairment of the confidentiality of information by means of the copying or removal of data Inclusion criteria: this code is related to statements about the impact of an attack in general and refers to information theft as a possible impact Exclusion criteria: NOT referring to a leak
Depends on access	Description: the impact depends on the access of the threat actor, including the amount of information available to the threat actor

	Inclusion criteria: this code is related to statements about the impact of an attack in general and refers to the impact depending on the access of the threat actor, including the amount of information available to the threat actor Exclusion criteria: -
Disruption	Description: Intentional temporary impairment of the accessibility of data, information systems or information services Inclusion criteria: this code is related to statements about the impact of an attack in general and refers to disruption as a possible impact Exclusion criteria: NOT sabotage (long-term disruption)
Financial loss	Description: financial loss is a possible impact (including fine) Inclusion criteria: this code is related to statements about the impact of an attack in general and refers to financial loss as a possible impact Exclusion criteria: NOT referring to a fine
Incident needs to be investigated internally	Description: the incident needs to be investigated internally Inclusion criteria: this code is related to statements about the impact of an attack in general and refers to an incident needing to be investigated internally as a possible impact Exclusion criteria: -
Inform affected persons	Description: affected persons need to be informed Inclusion criteria: this code is related to statements about the impact of an attack in general and refers to informing affected persons as a possible impact Exclusion criteria: -
Lawsuit	Description: a lawsuit can be a possible impact Inclusion criteria: this code is related to statements about the impact of an attack in general and refers to a lawsuit as a possible impact Exclusion criteria: -
Leak	Description: Impairment of confidentiality due to natural causes, technical difficulties or human error Inclusion criteria: this code is related to statements about the impact of an attack in general and refers to a leak as a possible impact Exclusion criteria: -
Notify data protection authority	Description: the data protection authority must be notified Inclusion criteria: this code is related to statements about the impact of an attack in general and refers to notifying the data protection authority as a possible impact Exclusion criteria: -
Reputation damage	Description: Damage to the opinion that people in general have about the company (including damage to the relationship between the company and a client) Inclusion criteria: this code is related to statements about the impact of an attack in general and refers to reputation damage as a possible impact Exclusion criteria: NOT referring to damage relationship with client
Sabotage	Description: Intentional and very long-lasting impairment of the accessibility of data, information systems or information services, possibly resulting in destruction Inclusion criteria: this code is related to statements about the impact of an attack in general and refers to sabotage as a possible impact Exclusion criteria: -

Table D.2.1: Distribution of codes in threats for experts

Code	1	2	3	4	5	6	7	8	9	10	11	Total	%
Initial access	2	3	5	7	5	4	3	1	1	4	2	37	100%
Execution	0	0	0	3	1	1	1	0	2	2	1	11	63,6%
Privilege escalation	0	0	2	0	0	0	0	0	0	0	0	2	9,1%
Credential access	0	1	1	0	2	0	0	0	6	0	0	10	36,4%
Collection	0	0	3	2	1	0	1	0	0	1	2	10	54,5%
Exfiltration	0	0	2	1	0	0	0	0	1	0	1	5	36,4%
Impact	1	0	0	1	1	1	0	0	1	1	1	7	63,6%
Hacking	0	1	0	3	0	0	0	0	0	1	0	5	27,3%
Unintentional threat	0	0	1	0	1	0	2	1	1	0	0	6	45,5%
There are many	0	0	2	0	0	0	0	1	1	0	1	5	36,4%

Many threats mitigated by firm	1	0	1	0	2	0	0	0	0	0	0	4	27,3%
--------------------------------	---	---	---	---	---	---	---	---	---	---	---	---	-------

Table D.2.2: Distribution of codes in threats for laypeople

Code	1	2	3	4	5	6	7	Total	%
Initial access	0	2	1	1	0	1	0	5	57,1%
Execution	1	2	0	0	1	3	0	7	57,1%
Privilege escalation	0	0	0	0	0	0	0	0	0,0%
Credential access	0	1	0	0	0	1	1	3	42,9%
Collection	0	0	0	0	0	1	0	1	14,3%
Exfiltration	0	0	0	0	0	0	0	0	0,0%
Impact	1	0	0	0	0	2	0	3	28,6%
Hacking	0	1	0	0	1	0	1	3	42,9%
Unintentional threat	1	1	1	0	1	0	0	4	57,1%
There are many	0	0	0	0	0	1	0	1	14,3%
Many threats mitigated by firm	0	0	0	0	0	0	0	0	0,0%

Table D.2.3: Distribution of codes in threat actors for experts

Code	1	2	3	4	5	6	7	8	9	10	11	Total	%
Hacktivists	0	0	0	0	0	1	1	1	1	0	2	6	45,5%
Cracker	2	1	0	0	1	1	1	1	0	4	3	14	72,7%
Terrorist	0	0	0	0	1	0	0	0	0	0	0	1	9,1%
State actor	7	0	1	3	1	0	0	0	0	3	2	17	54,5%
State-sponsored network	0	0	0	0	0	0	0	0	0	0	1	1	9,1%
Insider	0	0	5	0	0	1	2	1	2	2	0	13	54,5%
Professional criminals	2	0	0	0	0	0	0	0	0	1	1	4	27,3%
Company with malicious intent	1	0	0	0	0	0	0	0	0	0	1	2	18,2%
Competitor	1	1	2	0	0	0	0	0	0	1	1	6	45,5%
Clients	0	0	0	0	0	0	1	0	0	1	0	2	18,2%
Social media company	1	0	0	0	0	0	0	0	0	0	0	1	9,1%
There are many	0	0	1	0	0	0	0	0	0	0	0	1	9,1%

Table D.2.4: Distribution of codes in threat actors for laypeople

Code	1	2	3	4	5	6	7	Total	%
Hacktivists	0	1	0	0	0	0	0	1	14,3%
Cracker	0	1	0	0	1	1	0	3	42,9%
Terrorist	0	0	0	0	0	0	0	0	0,0%
State actor	0	2	0	0	1	0	0	3	28,6%
State-sponsored network	0	0	0	0	0	0	0	0	0,0%
Insider	0	0	0	0	0	0	1	1	14,3%
Professional criminals	2	0	0	0	0	1	1	4	42,9%
Company with malicious intent	0	0	0	0	0	0	0	0	0,0%
Competitor	0	0	0	0	0	1	1	2	28,6%
Clients	0	0	0	0	0	0	0	0	0,0%
Social media company	0	0	0	0	0	0	0	0	0,0%
Internet Service Provider	0	1	0	0	0	0	0	1	14,3%
There are many	0	0	0	0	0	0	1	1	14,3%

Table D.2.5: Distribution of codes in the motivation of a threat actor for experts

Code	1	2	3	4	5	6	7	8	9	10	11	Total	%
Coercion	0	0	0	2	1	0	0	0	0	0	0	3	18,2%
Disgruntlement	0	0	1	0	0	0	0	0	0	1	0	2	18,2%
Ideology	2	1	1	2	0	2	0	2	0	1	1	12	72,7%
Notoriety	0	0	0	2	0	0	0	0	0	0	0	2	9,1%
Organizational gain	1	1	1	1	0	0	0	0	0	1	1	6	54,5%
Personal financial gain	1	0	1	2	1	0	1	3	1	1	2	13	81,8%
Personal satisfaction	1	0	0	1	1	2	0	0	0	1	3	9	54,5%
There are many	0	0	2	0	0	0	0	0	0	0	1	3	18,2%

Table D.2.6: Distribution of codes in the motivation of a threat actor for laypeople

Code	1	2	3	4	5	6	7	Total	%
Coercion	0	0	1	0	0	0	0	1	14,3%
Disgruntlement	1	1	0	0	0	0	0	2	28,6%
Ideology	0	1	0	0	0	0	0	1	14,3%
Notoriety	0	0	0	0	0	0	0	0	0,0%
Organizational gain	0	0	0	0	0	1	2	3	28,6%
Personal financial gain	1	1	0	0	1	2	2	7	71,4%
Personal satisfaction	1	3	0	0	0	1	0	5	42,9%
there are many	0	0	0	0	1	0	0	1	14,3%

Table D.2.7: Distribution of codes in the capability of a threat actor for experts

Code	1	2	3	4	5	6	7	8	9	10	11	Total	%
No skills	0	0	2	0	0	0	0	0	1	0	0	3	18,2%
Minimal skills	0	1	1	1	0	0	0	0	0	1	0	4	36,4%
Operational skills	0	1	1	0	1	1	1	1	1	1	1	9	81,8%
Adept skills	0	0	1	1	1	0	0	0	0	1	0	4	36,4%

Table D.2.8: Distribution of codes in the capability of a threat actor for laypeople

Code	1	2	3	4	5	6	7	Total	%
No skills	0	0	0	0	0	0	1	1	14,3%
Minimal skills	0	1	1	0	0	0	0	2	28,6%
Operational skills	2	1	0	0	0	0	1	4	42,9%
Adept skills	0	0	0	0	0	0	0	0	0,0%

Table D.2.9: Distribution of codes in the impact of a possible threat for experts

Code	1	2	3	4	5	6	7	8	9	10	11	Total	%
Disruption	1	0	0	1	1	0	1	1	1	1	1	8	72,7%
Sabotage	0	0	0	1	0	0	0	0	0	0	0	1	9,1%
Data manipulation	0	0	0	0	0	0	0	1	0	0	0	1	9,1%

Data theft	1	1	2	1	4	0	1	1	1	1	1	14	90,9%
Leak	0	0	0	0	1	0	0	0	0	1	0	2	18,2%
Incident needs to be investigated internally	0	0	1	0	2	0	0	0	1	0	0	4	27,3%
Inform affected persons	0	0	1	0	0	0	0	0	1	0	0	2	18,2%
Lawsuit	0	0	1	0	0	0	0	0	0	0	0	1	9,1%
Notify data protection authority	0	0	1	0	1	0	0	0	1	0	0	3	27,3%
Reputation damage	1	2	1	1	2	1	2	0	1	1	1	13	90,9%
Financial loss	0	1	1	0	1	0	0	0	1	1	1	6	54,5%
Depends on access	0	1	1	0	0	2	0	0	0	1	0	5	36,4%

Table D.2.10: Distribution of codes in the impact of a possible threat for laypeople

Code	1	2	3	4	5	6	7	Total	%
Disruption	2	0	0	1	1	1	0	5	57,1%
Sabotage	0	0	0	0	0	0	0	0	0,0%
Data manipulation	0	0	0	1	0	0	0	1	14,3%
Data theft	2	1	1	1	1	0	1	7	85,7%
Leak	0	0	0	0	0	0	0	0	0,0%
Incident needs to be investigated internally	0	0	0	0	0	0	0	0	0,0%
Inform affected persons	0	0	0	0	0	0	0	0	0,0%
Lawsuit	0	0	0	0	0	0	0	0	0,0%
Notify data protection authority	0	0	0	0	0	0	0	0	0,0%
Reputation damage	1	1	0	0	1	1	1	5	71,4%
Financial loss	0	0	0	0	0	0	1	1	14,3%
Depends on access	0	1	0	0	0	0	0	1	14,3%

D.3: Code book perception of changes in the threat landscape when using a VPN

This section presents the code book for the perception of changes in the threat landscape when using a VPN and the frequency distribution of those codes in the interviews.

Table D.3.1: Code book perception of changes in the threat landscape when using a VPN

Threats mitigated	
Block you from accessing a website	Description: Because of filtering of traffic, done by a firewall or something unspecified, it is not possible to visit a website Inclusion criteria: this code is related to statements about threats that are mitigated due to using a VPN and refers to blocking access to a website Exclusion criteria: -
Stop malicious software	Description: Because of filtering of traffic, done by a firewall or antivirus, malicious software is stopped. Examples are 1) stop an e-mail with a malicious attachment; 2) deactivate a malicious attachment; 3) stop a virus / prevent you from downloading malicious software; 4) monitor and detect malicious software on USB stick; or 5) monitor and block an upload to the cloud Inclusion criteria: this code is related to statements about threats that are mitigated due to using a VPN and refers to stopping malicious software due to filtering of traffic as a mitigated threat Exclusion criteria: -
Does not mitigate all computer security threats	Description: A VPN does not mitigate all computer security threats Inclusion criteria: this code is related to statements about threats that are mitigated due to using a VPN and refers to VPN not mitigating all computer security threats (can be by giving an example) Exclusion criteria: -

Listening in on communication	Description: Due to the VPN connection it becomes more difficult or impossible to listen in on communication send via the connection Inclusion criteria: this code is related to statements about threats that are mitigated due to using a VPN and refers to listening in on communication as a mitigated threat Exclusion criteria: -
Masks IP-address	Description: because traffic goes through the VPN server, the receiving endpoint can only see the IP-address of the server and not the original IP-address of the sending device Inclusion criteria: this code is related to statements about threats that are mitigated due to using a VPN and refers to masks IP-address Exclusion criteria: -
More difficult for threat actor	Description: Due to the VPN connection it becomes more difficult for the threat actor to perform an attack successful. Examples are the threat actor needs more effort, knowledge, power, resources, skills, or time, or less threat actors will be successful Inclusion criteria: this code is related to statements about threats that are mitigated due to using a VPN and refers to a successful attack becoming more difficult for the threat actor Exclusion criteria: -
No access to files when access to device	Description: Due to the VPN connection files are not or less often stored locally, thus when a threat actor is able to access your device, he or she is not able to access those files Inclusion criteria: this code is related to statements about threats that are mitigated due to using a VPN and refers to no access to files when access to device Exclusion criteria: -
Single point of attack from webtraffic threats	Description: Because of the VPN connection, devices connect to the Internet via a single point, namely the VPN server, this makes it easier to monitor and filter threats coming via webtraffic Inclusion criteria: this code is related to statements about threats that are mitigated due to using a VPN and refers to single point of attack from webtraffic attacks Exclusion criteria: -
Updates pushed	Description: The VPN connection enables the possibility to push updates to connected devices Inclusion criteria: this code is related to statements about threats that are mitigated due to using a VPN and refers to updates pushed Exclusion criteria: -
New threats due to VPN	
Access to device while connected to VPN	Description: a threat actor gains physical or digital access to a device, while this device is connected to the VPN Inclusion criteria: this code is related to statements about threats that exist or are increased due to the use of a VPN connection and refers to access to device while connected to VPN as a threat Exclusion criteria: -
Authentication measures	Description: threats that arise due to the current authentication measures. Examples are someone getting access to your credentials and using them to establish a connection, static password, VPN not coupled to AD user Inclusion criteria: this code is related to statements about threats that exist or are increased due to the use of a VPN connection and refers to authentication measures as a threat Exclusion criteria: -
Hacking	Description: refers to hacking or vulnerabilities as a threat or refers to security depending on configuration or protocols used Inclusion criteria: this code is related to statements about threats that exist or are increased due to the use of a VPN connection and refers to hacking Exclusion criteria: NOT related to server is compromised
Listening in on communication	Description: refers to the threat of listening in on communication Inclusion criteria: this code is related to statements about threats that exist or are increased due to the use of a VPN connection and refers to listening in on communication Exclusion criteria: -
Malfunction	Description: threats that arise due to technical failure. Example is a power outage. Inclusion criteria: this code is related to statements about threats that exist or are increased due to the use of a VPN connection and refers to a malfunction as a threat Exclusion criteria: -
Malicious traffic can go through security layer	Description: Malicious traffic can go through the security layers, if the VPN server is placed in the internal network Inclusion criteria: this code is related to statements about threats that exist or are increased due to the use of a VPN connection and refers to malicious traffic can go through security layer as a threat Exclusion criteria: -

More suspicious for state actor	Description: using a VPN makes you more suspicious for the government Inclusion criteria: this code is related to statements about threats that exist or are increased due to the use of a VPN connection and refers to making you more suspicious for the government as a threat Exclusion criteria: -
Server is compromised	Description: The VPN server is compromised. Examples are physical access to server, hacking server, geographical location of server, or personal data is visible to server Inclusion criteria: this code is related to statements about threats that exist or are increased due to the use of a VPN connection and refers to the VPN server being compromised as a threat Exclusion criteria: -
Trace back IP-address	Description: refers to the threat of tracing back the IP-address of the original sending device Inclusion criteria: this code is related to statements about threats that exist or are increased due to the use of a VPN connection and refers to trace back IP-address Exclusion criteria: -
Use VPN when using unsecured network	Description: Using a VPN when using an unsecured network is a threat. Unsecured network can be public wifi or private wifi, can be protected with password Inclusion criteria: this code is related to statements about threats that exist or are increased due to the use of a VPN connection and refers to using a VPN when using an unsecured network as a threat Exclusion criteria: -
VPN provider	Description: the person, company or organization in charge of the VPN, the internal security measures of the VPN provider, or physical access to the VPN provider Inclusion criteria: this code is related to statements about threats that exist or are increased due to the use of a VPN connection and refers to the VPN provider as a threat Exclusion criteria: -
Change in user behavior	
Do not use VPN connection for private matters	Description: The VPN connection is not used when performing private activities Inclusion criteria: this code is related to statements about changes in user behavior due to vulnerabilities related to the VPN and refers to do not use VPN connection for private matters as a change in user behavior Exclusion criteria: -
Does not change	Description: there is no change in user behavior Inclusion criteria: this code is related to statements about changes in user behavior due to vulnerabilities related to the VPN and refers to no change in user behavior Exclusion criteria: -
Only use VPN when necessary	Description: the VPN connection is only used when necessary and not at other moments Inclusion criteria: this code is related to statements about changes in user behavior due to vulnerabilities related to the VPN and refers to only use VPN when necessary as a change in user behavior Exclusion criteria: -
Prevent access by other persons	Description: Prevent access to the device, credentials or access token by other persons than yourself Inclusion criteria: this code is related to statements about changes in user behavior due to vulnerabilities related to the VPN and refers to prevent access by other persons as a change in user behavior Exclusion criteria: -
Separate devices for work and private use	Description: having separate devices for work and private use Inclusion criteria: this code is related to statements about changes in user behavior due to vulnerabilities related to the VPN and refers to having separate devices for work and private use as a change in user behavior Exclusion criteria: -

Table D.3.1: Distribution of codes in the mitigated threats for experts

Code	1	2	3	4	5	6	7	8	9	10	11	Total	%
Block you from accessing a website	0	0	0	4	0	0	0	0	6	3	0	13	27,3%
Stop malicious software	0	0	0	7	0	0	0	0	6	0	2	15	27,3%

Listening in on communication	3	1	2	1	0	0	1	3	0	2	2	15	72,7%
Masks IP-address	3	0	0	5	2	0	0	4	5	2	1	22	63,6%
No access to files when access to device	0	0	0	0	1	1	1	0	0	0	1	4	36,4%
Single point of attack from webtraffic threats	0	0	0	0	0	0	3	0	0	1	0	4	18,2%
Updates pushed	0	1	0	0	0	0	0	0	0	0	0	1	9,1%
More difficult for threat actor	2	1	1	1	0	0	0	0	0	2	1	8	54,5%
Does not mitigate all computer security threats	2	0	3	3	0	1	0	2	3	3	1	18	72,7%

Table D.3.2: Distribution of codes in the mitigated threats for laypeople

Code	1	2	3	4	5	6	7	Total	%
Block you from accessing a website	0	0	0	0	0	0	0	0	0,0%
Stop malicious software	0	0	0	0	0	0	0	0	0,0%
Listening in on communication	0	6	0	2	0	3	1	12	57,1%
Masks IP-address	0	1	0	0	0	0	1	2	28,6%
No access to files when access to device	0	0	1	0	0	0	1	2	28,6%
Single point of attack from webtraffic threats	0	0	0	0	0	0	0	0	0,0%
Updates pushed	0	0	0	0	0	0	0	0	0,0%
More difficult for threat actor	2	2	1	0	1	0	0	6	57,1%
Does not mitigate all computer security threats	0	0	0	0	0	2	0	2	14,3%

Table D.3.3: Distribution of codes in the new threats for experts

Code	1	2	3	4	5	6	7	8	9	10	11	Total	%
Access to device while connected to VPN	0	3	3	0	0	0	0	0	0	2	0	8	27,3%
Authentication measures	0	0	0	0	3	1	1	0	0	0	0	5	27,3%
Hacking	2	0	3	1	2	0	3	0	2	2	3	18	72,7%
Listening in on communication	0	0	0	0	1	0	0	0	0	0	0	1	9,1%
Malfunction	0	0	0	0	0	0	0	1	0	0	0	1	9,1%
Malicious traffic can go through security layer	0	0	0	0	0	0	2	0	0	0	0	2	9,1%
More suspicious for state actor	0	0	2	0	0	0	0	0	0	0	0	2	9,1%
Server is compromised	1	0	1	0	0	0	0	4	0	4	1	11	45,5%
Trace back IP-address	1	0	0	0	0	0	0	0	0	0	0	1	9,1%
Use VPN when using unsecured network	0	0	0	0	2	0	0	0	0	0	0	2	9,1%
VPN provider	4	0	0	4	0	0	0	2	0	0	0	10	27,3%

Table D.3.4: Distribution of codes in the new threats for laypeople

Code	1	2	3	4	5	6	7	Total	%
Access to device while connected to VPN	0	0	0	0	0	1	1	2	28,6%
Authentication measures	1	0	0	0	2	0	0	3	28,6%
Hacking	0	3	1	0	0	1	0	5	42,9%
Listening in on communication	0	0	0	0	0	1	0	1	14,3%

Malfunction	0	0	0	0	0	0	0	0	0	0,0%
Malicious traffic can go through security layer	0	0	0	0	0	0	0	0	0	0,0%
More suspicious for state actor	0	0	0	0	0	0	0	0	0	0,0%
Server is compromised	0	0	0	0	0	0	1	1	14,3%	
Trace back IP-address	0	0	0	0	0	0	0	0	0	0,0%
Use VPN when using unsecured network	1	0	0	0	0	0	0	0	1	14,3%
VPN provider	0	1	0	0	0	0	1	2	28,6%	

Table D.3.5: Distribution of codes in the change in behavior for experts

Code	1	2	3	4	5	6	7	8	9	10	11	Total	%
Does not change	0	0	1	0	0	0	0	1	0	0	1	3	27,3%
Only use VPN when necessary	0	0	0	0	0	0	1	0	0	0	1	2	18,2%
Do not use VPN connection for private matters	1	0	0	0	0	0	0	0	0	0	0	1	18,2%
Separate devices for work and private use	1	0	0	0	0	0	0	0	0	0	1	2	18,2%
Prevent access by other persons	0	0	0	0	1	1	0	0	0	0	0	2	18,2%

Table D.3.6: Distribution of codes in the change in behavior for laypeople

Code	1	2	3	4	5	6	7	Total	%
Does not change	0	1	0	0	0	1	0	2	28,6%
Only use VPN when necessary	0	0	0	0	0	0	0	0	0,0%
Do not use VPN connection for private matters	0	0	0	0	0	0	0	0	0,0%
Separate devices for work and private use	0	0	0	0	0	0	0	0	0,0%
Prevent access by other persons	0	0	0	0	0	0	0	0	0,0%

Appendix E: Overview of ICA coefficients per semantic domain

This appendix contains an overview of the c-alpha-binary coefficients per semantic domain, presented in table E.1. The coefficients are colored coding, where green equals higher than 0.8, yellow equals between 0.667 and 0.8, and red equals below 0.667.

Table E.1: the c-alpha-binary coefficients per semantic domain

Semantic domain	C-alpha-binary before issues resolved	C-alpha binary after issues resolved
Concept	0.785	0.785
Connection	0.937	0.937
Device	0.049	0.994
Establish Connection/ S:	0.804	0.804
Establish Connection/ U:	0.791	0.791
Internal Network	0.518	0.903
IP-address	0.918	0.918
Reason for use	0.593	0.898
VPN provider	0.828	0.828
Threat actor	0.523	0.762
Threat capability	0.74	0.74
Threat general	0.634	0.767
Threat motivation	0.708	0.889
Threat impact	0.635	0.883
Threat mitigation	0.68	0.741
Threat VPN	0.505	0.924
Change in user behavior	0.745	0.874
Total	0.724	0.837