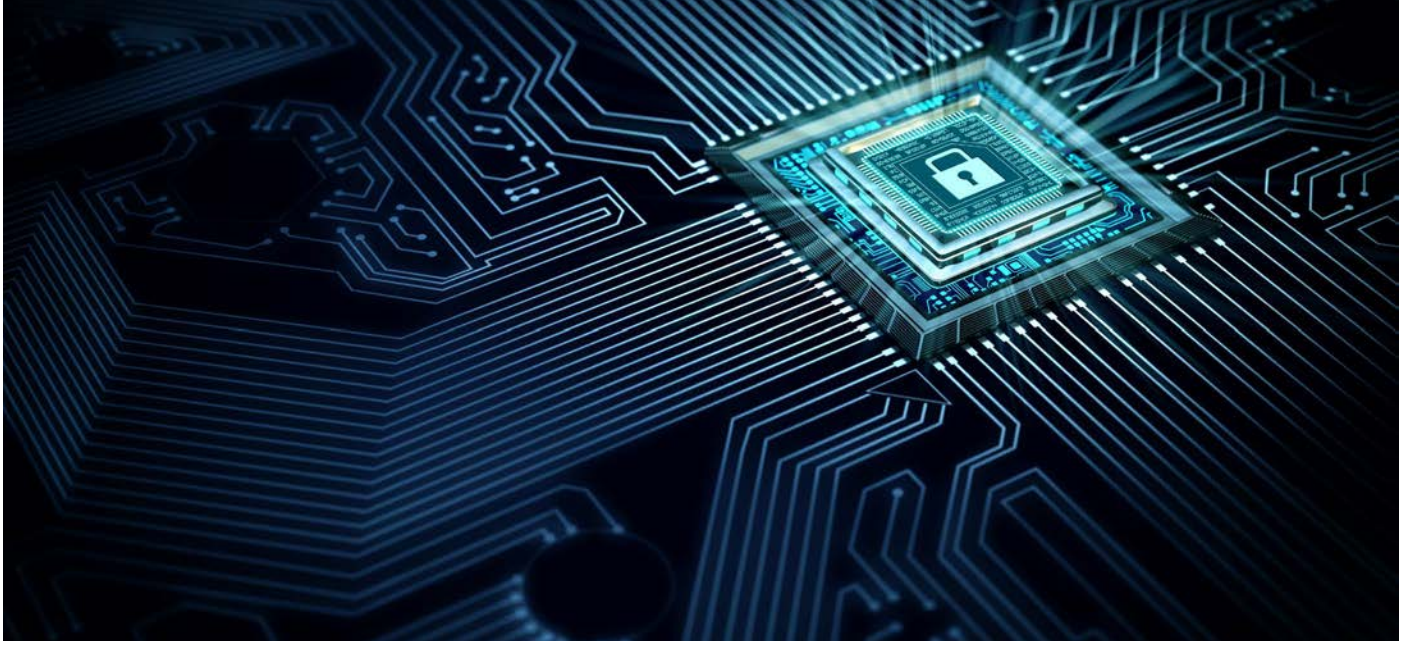
When safety meets security

Sas, Marlies; van Nunen, Karolien; Reniers, Genserik; Ponnet, Koen; Hardyns, Wim

Publication date
2019

Document Version
Final published version

Published in
Veiligheidsnieuws



WHEN SAFETY MEETS SECURITY

Op gebied van veiligheid bestaat al een lange traditie van onderzoek, maar van beveiliging staat dit nog eerder in de kinderschoenen. De aanslagen van 9/11 hebben de aandacht voor beveiliging vergroot. Ook cybercriminaliteit en de bescherming van gevoelige informatie kwam de afgelopen jaren hoger op de bedrijfsagenda te staan. Deze recente focus weerspiegelt zich in het wetenschappelijk onderzoek, waar op het vlak van beveiliging nog maar een beperkt aantal concepten en modellen werden ontwikkeld.

Marlies Sas
Doctoraatsonderzoeker beveiligingswetenschappen UAntwerpen

Karolien van Nunen
Leerstoel Vandeputte UAntwerpen

Genserik Reniers
Prof UAntwerpen/TU Delft

Koen Ponnet
Prof UGent

Wim Hardyns
Prof UGent

Verschillen en gelijkenissen tussen safety en security

De lange onderzoekstraditie op het vlak van veiligheid zorgt voor een vat vol nuttige informatie die aan de basis kan liggen bij het ontwikkelen van nieuwe beveiligingsconcepten en -modellen. In dit artikel worden de verschillen en gelijkenissen tussen veiligheid (safety) en beveiliging (security) besproken, wordt een model voor beveiligingscultuur toegelicht – naar analogie met veiligheidscultuur – en komen enkele praktische tips aan bod om bedrijfsbeveiliging te verhogen.

Verschil: niet-opzettelijk versus opzettelijk

Zowel op het vlak van veiligheid als op het gebied van beveiliging staat hetzelfde doel voorop: schade aan personen, materiaal of de omgeving voorkomen. Het belangrijkste verschil situeert zich in de manier waarop deze schade wordt veroorzaakt. Bij een veiligheidsincident is het nooit de bedoeling om schade aan te richten en ligt een niet-opzettelijke oorzaak, zoals het falen van een machine of een procesfout, aan de basis. Ook wordt een menselijke fout, waarbij de werknemer op de hoogte is dat men deze fout maakt, gezien als niet-opzettelijk – bijvoorbeeld het niet naleven van een procedure om het werk sneller af te krijgen – aangezien het niet de bedoeling is van de werknemer om schade aan te richten. Een beveiligingsincident daarentegen wordt steeds veroorzaakt door een menselijke daad waarbij het met opzet de bedoeling is om schade aan te richten. Op het vlak van beveiliging is er dus steeds een 'intelligente tegenstander' of agressor aanwezig die nadenkt over de meest efficiënte manier om schade aan te richten. Hierbij probeert de dader de bestaande beveiligingsmaatregelen te omzeilen.

> *"Zowel bij safety als security staat hetzelfde doel voorop: schade voorkomen"*

Een belangrijke consequentie van dit verschil heeft betrekking op de mate van transparantie binnen een bedrijf. Op het vlak van safety is transparantie essentieel om onder meer optimaal te leren van elkaar en van onveilige situaties. Ook is transparantie over bijvoorbeeld aanwezige gevaarlijke stoffen belangrijk om de gevolgen bij een veiligheidsincident - zoals een lek van een opslagtank - te beperken. Deze transparantie is echter niet altijd optimaal op het vlak van security. Een terroristische aanslag kan bijvoorbeeld gepland worden op basis van informatie over aanwezige gevaarlijke stoffen. De

mate van transparantie moet daarom zorgvuldig afgewogen worden om een optimaal niveau van veiligheid én van beveiliging te bekomen. Een hulpmiddel hierbij is het creëren van zogenaamde trusted communities waarbij gevoelige informatie wordt gedeeld met een beperkte groep van actoren, zoals de omliggende bedrijven en de brandweer.

> *"Veiligheidsrisico's kunnen zichtbaar gemaakt worden door risicoanalyses"*

	Veiligheid *Safety*	Beveiliging *Security*
Verschillen	✔ De oorzaak van het incident is niet-opzettelijk ✔ Afwezigheid van agressor / intelligente tegenstander ✔ Transparantie is essentieel voor hoog veiligheidsniveau ✔ Voornamelijk interne risico's	✔ De oorzaak van het incident is opzettelijk ✔ Aanwezigheid van agressor / intelligente tegenstander ✔ Transparantie levert niet altijd voordelen op ✔ Voornamelijk externe dreigingen
Gelijkenissen	✔ Nemen van preventiemaatregelen essentieel om tot aanvaardbaar niveau van veiligheid en beveiliging te komen ✔ Veiligheidsmaatregelen kunnen positief effect hebben op het vlak van beveiliging (en omgekeerd) ✔ Integrale cultuuraanpak: focus op technische, organisatorische en menselijke aspecten	

Verschil: risico's versus dreigingen
Een belangrijk onderscheid zijn de risico's op het vlak van veiligheid en de dreigingen op het gebied van beveiliging. Veiligheidsrisico's komen voornamelijk voort uit de organisatie zelf, in tegenstelling tot beveiligingsdreigingen die voornamelijk extern zijn aan het bedrijf.

MOGELIJKE DREIGINGEN VOOR EEN BEDRIJF

- Agressie
- Activisme
- Vandalisme
- Diefstal en inbraak
- Informatiebeveiligings-inbreuken
- Bedrijfsspionage
- Fraude
- Sabotage
- Terroristische aanslag
- ...

Veiligheidsrisico's kunnen zichtbaar gemaakt worden binnen het bedrijf aan de hand van risicoanalyses. Op het vlak van beveiliging is het heel wat moeilijker om alle mogelijke dreigingsscenario's in kaart te brengen omdat er verschillende externe en dus vaak onbekende factoren meespelen.

Gelijkenis: het nemen van preventiemaatregelen
Een belangrijke gelijkenis is dat preventiemaatregelen essentieel zijn om zowel safety als security op een aanvaardbaar niveau te brengen. Sommige maatregelen kunnen zelfs een dubbel effect hebben en zowel het veiligheids- als het beveiligingsniveau beïnvloeden. Zo kan een training gericht op het vergroten van het bewustzijn omtrent veiligheidsrisico's ook een invloed hebben op de alertheid voor mogelijke beveiligingsdreigingen. Ook kan een controlesysteem de toegang beperken tot een ruimte met gevaarlijke stoffen voor enerzijds werknemers zonder gepaste opleiding (safety maatregel) en anderzijds voor individuen met kwade bedoelingen (security maatregel). Het kan daarom vruchtbaar zijn om voor het invoeren van een veiligheidsmaatregel na te denken of deze maatregel – mits eventuele uitbreiding of aanpassing – ook geen voordeel kan opleveren op het vlak van beveiliging (en omgekeerd).

> *"Hou rekening met zowel de technische, organisatorische en de menselijke aspecten"*

#wistjedatje

ASIS is een internationaal platform voor security professionals. Op hun website zijn verschillende publicaties te vinden, en kan men zich lid maken om uitgenodigd te worden voor conferenties en events.

◢ n.v.d.r.

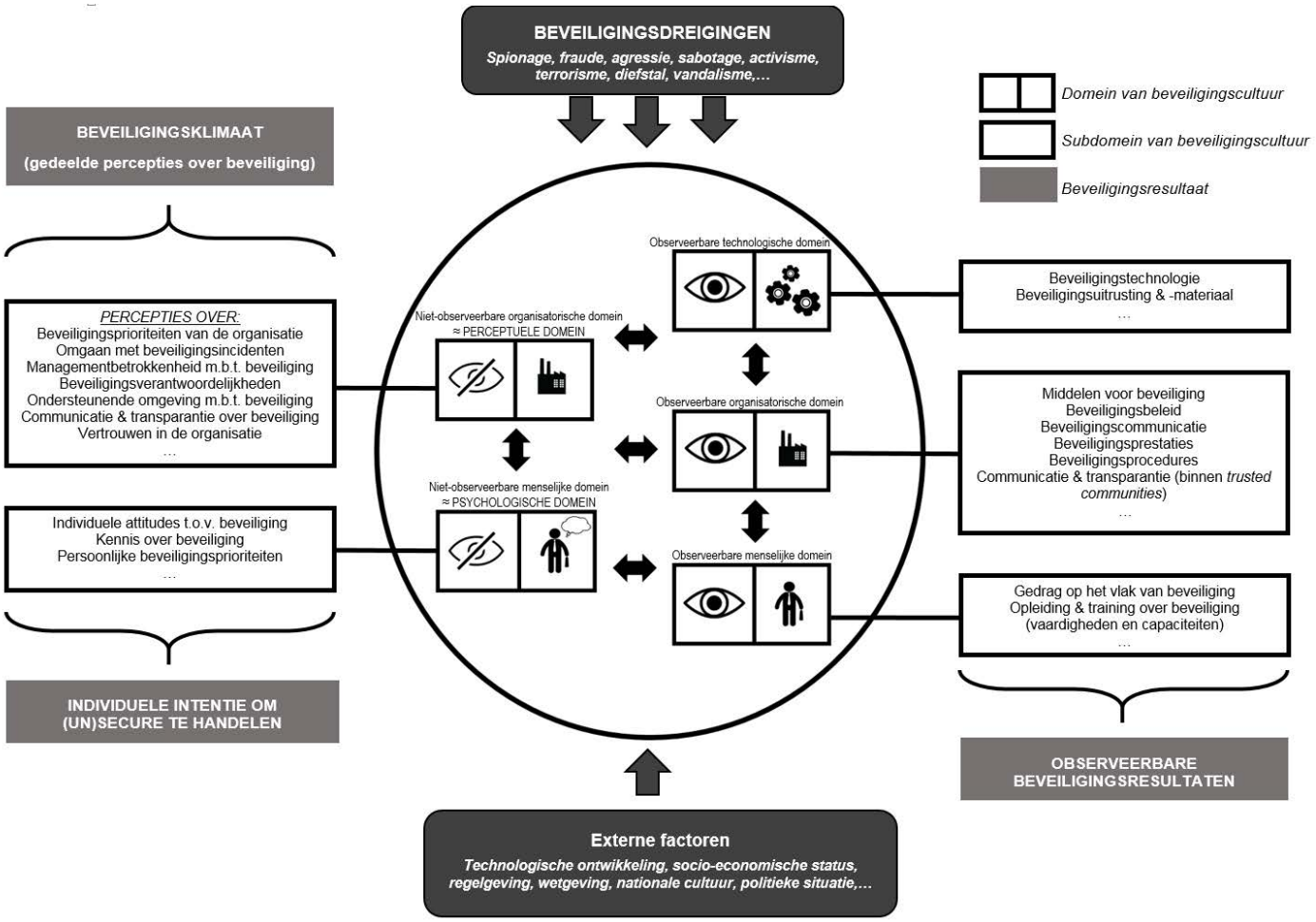
Gelijkenis: de noodzaak van een integrale aanpak
Een optimale veiligheids- en beveiligingscultuur kan men enkel bekomen als veiligheid en beveiliging op een integrale manier worden aangepakt. Dit houdt in dat er rekening moet gehouden worden met zowel de technische, de organisatorische en de menselijke aspecten.

> *"De security parameter meet hoe sterk het management bezig is met beveiliging"*

De beveiligingscultuur van een bedrijf
In wat volgt wordt een model van beveiligingscultuur toegelicht, waarbij er beroep werd gedaan op de bestaande kennis op het vlak van veiligheid en veiligheidscultuur. De figuur op de volgende pagina geeft een integraal overzicht van alle aspecten die deel uitmaken van de beveiligingscultuur van een bedrijf. Er kunnen vijf domeinen onderscheiden worden:

1. Technische observeerbare domein: technische maatregelen die een bedrijf kan nemen om de beveiliging te verhogen, zoals toegangscontrole of bewakingscamera's.

2. Organisatorische observeerbare domein: observeerbare aspecten op het niveau van de organisatie, zoals het beveiligingsbeleid en de middelen die voor beveiliging voorzien worden. ▸▸



3. Menselijke observeerbare domein: observeerbare aspecten op het niveau van het individu, zoals het gestelde gedrag (handelt men secure of unsecure) en de opleiding van werknemers over beveiliging.

Deze drie domeinen kunnen gemeten worden aan de hand van observeerbare security parameters, zoals het aantal bewakingscamera's op de plaatsen waar deze nodig zijn, de communicatie over beveiliging, of het aantal gevolgde security opleidingen. Aangezien het hier gaat om observeerbare aspecten kunnen deze in kaart gebracht worden (gemeten worden) op basis van onder meer aanwezige documenten en data in het bedrijf of op basis van observaties / rondgangen.

4. Organisatorische niet-observeerbare domein of het perceptuele domein: dit zijn de percepties die men heeft over de manier waarop het bedrijf met beveiliging omgaat, zoals het omgaan met beveiligingsincidenten of de mate waarin het management belang hecht aan beveiliging.

Dit domein kan in kaart gebracht worden door het beveiligingsklimaat van een organisatie te meten, of met andere woorden de gedeelde percepties op het vlak van beveiliging. Het afnemen van een vragenlijst is hiervoor een geschikte manier.

5. Menselijke niet-observeerbare domein of het psychologische domein: dit zijn minder tastbare aspecten, zoals de individuele attitude tegenover beveiliging, de kennis over beveiliging (schat men dreigingen adequaat in) en persoonlijke prioriteiten.

Dit domein kan in kaart gebracht worden door middel van de individuele intentie om secure of unsecure te handelen. Deze intentie kan gemeten worden aan de hand van een vragenlijst of interviews.

> *"De pijlen tonen aan dat de domeinen een invloed op elkaar uitoefenen"*

De pijlen van en naar de verschillende domeinen geven weer dat de domeinen een invloed op elkaar uitoefenen. Zo zal bijvoorbeeld de kennis van werknemers het gestelde gedrag beïnvloeden, of zal het beleid van de organisatie een effect hebben op het belang dat werknemers hechten aan beveiliging.

Ook de dreigingen zelf hebben een belangrijke impact. Afhankelijk van de sector zal een bedrijf meer of minder kwetsbaar zijn voor bepaalde soorten

#wistjedatje

De Belgische bewakingsbedrijven moeten het Vigilis-logo zichtbaar dragen op hun uitrusting. De Nederlandse veiligheidsbranche heeft diverse keurmerken om de kwaliteit te bewaken.

◢ n.v.d.r.

ENKELE ALGEMENE TIPS VOOR WERKNEMERS

- Check steeds de legitimiteit van leveranciers en bezoekers
- Spreek onbekende personen aan ("Kan ik u ergens mee helpen?")
- Geef geen sleutels of badges door
- Geef geen paswoorden door
- Let op met vreemde USB-sticks
- Registreer vooraf kentekens van laptop, gsm, auto,...
- Meld verdachte situaties en personen
- Meld kapotte sloten, deuren, ramen,...
- Laat geen pakjes, dozen, tassen,... staan op plaatsen waar deze niet thuishoren
- Hou evacuatiewegen vrij

#wistjedatje

De website Besafe is de algemene website over veiligheid en preventie van de FOD Binnenlandse zaken en de website Vigilis is de meer specifieke website over private veiligheid.

◢ n.v.d.r.

dreigingen. Een bank zal kwetsbaarder zijn voor fraude en diefstal, terwijl een chemisch of nucleair bedrijf eerder een aantrekkelijk doelwit voor terrorisme kan zijn. De kwetsbaarheid voor deze dreigingen geeft de beveiligingscultuur van de organisatie mee vorm. Tot slot zijn er externe factoren, zoals de wet- en regelgeving, die een invloed hebben op de beveiligingscultuur van een organisatie.

"Het menselijk brein is de zwakste schakel binnen het beveiligingsbeleid"

De sterkte van het menselijke domein

Een organisatie kan dus zowel op technisch, organisatorisch als op menselijk vlak maatregelen nemen om zich te beschermen tegen mogelijke dreigingen. Bij beveiligingsincidenten wordt vaak in eerste instantie gedacht aan maatregelen binnen de eerste twee domeinen, zoals camerabewaking of een nieuwe procedure. Het menselijke domein wordt vaak uit het oog verloren, terwijl dit net de zwakste schakel binnen het beveiligingsbeleid is. Technische en organisatorische maatregelen verliezen aan efficiëntie wanneer individuen zich niet bewust zijn van de mogelijke beveiligingsrisico's binnen de eigen organisatie of te weinig overtuigd zijn van het nut en de werking van de genomen maatregelen. Een toegangscontrolesysteem is bijvoorbeeld inefficiënt wanneer werknemers de deur open laten of mensen zonder badge achter zich mee binnen laten. Naar dit bewustzijn op het vlak van beveiliging wordt verwezen met de term security awareness of beveiligingsbewustzijn.

Vergroten van het beveiligingsbewustzijn

Heel wat beveiligingsincidenten, zoals diefstal of fraude, kan men vermijden door alerte werknemers. Een beveiligingsbeleid waarbij werknemers op de hoogte zijn van de mogelijke dreigingen en handelingsstrategieën draagt hiertoe bij. Het verspreiden van algemene tips kan een eerste stap zijn in de richting van meer bewuste werknemers.

"Het is bijna onmogelijk om hét profiel van de terrorist te schetsen"

Terrorisme

Sinds de recente terreuraanslagen stellen steeds meer bedrijven zich de vraag of men wel is voorbereid op dergelijke scenario's. Een organisatie kan op verschillende manieren worden getroffen door terreur. Terroristen kunnen een bedrijf uitkiezen als doelwit, bijvoorbeeld op basis van het aantal personen die getroffen kunnen worden (ziekenhuis, universiteit, luchthaven,...) of op basis van aanwezige explosieve, brandbare en toxische stoffen. Ook kan de organisatie aangewend worden als middel door bijvoorbeeld diefstal van gevaarlijke producten die kunnen ingezet worden bij een aanslag. Terreur in de buurt van het bedrijf, op belangrijke transportroutes of bij leveranciers kan eveneens een grote impact hebben op de werking van de organisatie. Tenslotte kan radicalisering onder werknemers, bezoekers, leveranciers,... in het ergste geval leiden tot een aanslag binnen het eigen bedrijf.

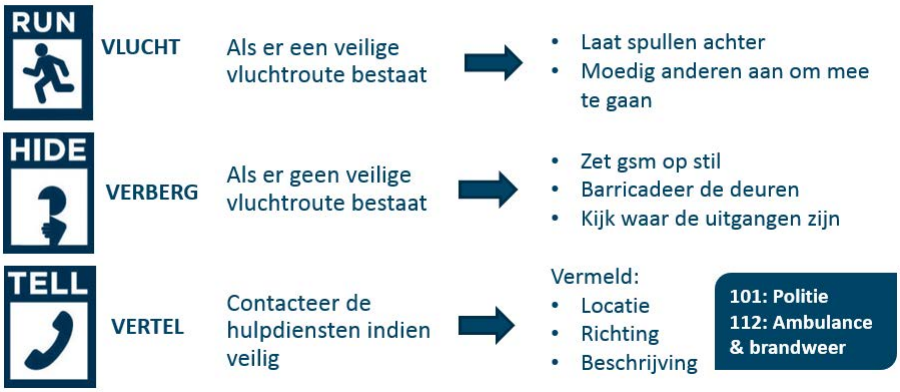
Radicalisering

Radicalisering verwijst naar het fenomeen waarbij individuen zich bepaalde extreme opinies of ideeën eigen maken wat kan leiden tot terroristische daden. Belangrijk hierbij is dat deze radicale ideeën niet per se problematisch zijn; ze monden immers niet altijd uit in gewelddadig gedrag. Daarnaast is radicalisering niet verbonden aan een bepaalde etnische, culturele of religieuze groep. Elk individu kan met andere woorden radicaliseren. Het is dus bijna onmogelijk om hét profiel van de terrorist te schetsen.

"Werknemers moeten weten hoe ze moeten reageren bij een terreurincident"

Enkel bedrijven met een hoog veiligheidsrisico mogen werknemers screenen, waardoor het van belang kan zijn om mogelijke radicaliseringssignalen tijdig op te merken (uitspraken die doen vermoeden dat het individu overtuigd is van een extreme ideologie, een verandering in uiterlijke kenmerken die wijzen op een veranderde identiteit,...). Wanneer onduidelijkheid heerst over gedetecteerde radicaliseringskenmerken is het mogelijk om contact op te nemen met met de infolijn Islam (www.infolijnislam.be). Sommige lokale politiezones hebben een apart Meldpunt Radicalisme opgericht waar elke burger terecht kan met vragen en meldingen. ▶▶

Active shooter



Bommelding

Terrorisme: hoe reageren?

Ook op het vlak van terreur speelt het beveiligingsbewustzijn een belangrijke rol. Zo werd in Groot-Brittannië na de recente terreuraanslagen de slogan 'If you see something, say something' massaal verspreid om het belang van alert te reageren en melden te benadrukken. Het is zeer belangrijk dat werknemers weten waar en hoe ze verdachte situaties kunnen melden.

> *"Het is nodig dat een brand-alarm-melding verschilt van een bomalarm-melding"*

Indien er zich een terreurincident voordoet, is het van belang dat werknemers weten op welke manier ze moeten reageren. In Groot-Brittannië hanteert men in het geval van een active shooter of 'dolle schutter' de handelingsstrategie Run, Hide, Tell. Een bommelding vraagt dan weer een andere manier van handelen, waarbij er belangrijke verschillen zijn met een evacuatie naar aanleiding van een brandalarm. Zo dient men bij een bommelding alle persoonlijke spullen mee te nemen zodat het duidelijk is dat dit geen verdachte zaken zijn. Ook is het belangrijk dat men zich niet allemaal samen verzamelt op de evacuatieplaats (perfect doelwit voor een aanslag), maar dat men zich zo ver mogelijk verwijdert van het bedrijf. Het is bijgevolg nodig dat de melding voor een brandalarm verschilt van de melding voor een bomalarm.

Onbekend is onbemind?

In een recent onderzoek van Universiteit Antwerpen (Leerstoel Vandeputte) werden 1425 veiligheidsdeskundigen uit België en Nederland bevraagd. Op het vlak van security kwam het volgende naar voor:
- Bij één op vijf zit security in het takenpakket.
- Hiervan kreeg slecht 7% een opleiding over security.
- Bij diegenen waarbij security in het takenpakket zit, zouden velen hier graag minder tijd aan besteden.

◢ n.v.d.r.

Enkele aandachtspunten

- Het is noodzakelijk dat bedrijven de specifieke dreigingen en kwetsbaarheden voor hun organisatie kennen. Dreigingsanalyses, afgestemd op het bedrijf, kunnen deze aspecten in kaart brengen. Zo kunnen beveiligingsmaatregelen worden ingevoerd die aansluiten bij het profiel van het bedrijf.
- De gelijkenissen tussen veiligheid en beveiliging zorgen ervoor dat integratie van beide domeinen op bepaalde vlakken voordelen kan opleveren. De verschillen tussen veiligheid en beveiliging leiden echter tot het omgekeerde, en kunnen leiden tot discrepanties op het vlak van te nemen preventiemaatregelen. Nieuwe beveiligingsmaatregelen worden daarom best eerst afgestemd met de bestaande maatregelen op het vlak van veiligheid en omgekeerd. Het is belangrijk dat er wordt ingezet op een integrale beveiligingscultuur, waar zowel technologische, organisatorische als menselijke aspecten deel van uitmaken.
  Binnen een efficiënt beveiligingsbeleid zijn deze aspecten geïntegreerd met elkaar. Wanneer er nieuwe maatregelen op technologisch vlak worden ingevoerd, is het noodzakelijk dat ook de organisatorische en menselijke aspecten hierop worden afgestemd.
- Binnen een beveiligingsbeleid mag de menselijke factor niet uit het oog worden verloren. Beveiligingsbewuste werknemers kunnen heel wat incidenten voorkomen en zijn cruciaal voor de efficiëntie van de bestaande beveiligingsmaatregelen.
- Het bestaande beveiligingsbeleid moet regelmatig worden geëvalueerd. Externe audits (zoals mystery visits) kunnen de zwakke plekken in het beveiligingsbeleid blootleggen, zodat nieuwe maatregelen kunnen worden ingevoerd of bestaande worden aangepast. ◆

Bronnen en externe links van dit artikel vind je terug op prebes.be/vn/204.