Delft University of Technology

Document Version
Final published version

Citation (APA)
Horst, M. V. D., Jansen, R., & Scherpenisse, W. (2025). Coordinated Vulnerability Disclosure en notificatie in het licht van NIS2. *Computerrecht*, (163). https://www.inview.nl/document/id329fcd05c1f5442ca469f5ea6d060026

Important note
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright
In case the licence states “Dutch Copyright Act (Article 25fa)”, this publication was made available Green Open Access via the TU Delft Institutional Repository pursuant to Dutch Copyright Act (Article 25fa, the Taverne amendment). This provision does not affect copyright ownership.
Unless copyright is transferred by contract or statute, it remains with the copyright holder.

Sharing and reuse
Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy
Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

This work is downloaded from Delft University of Technology.

Green Open Access added to TU Delft Institutional Repository
as part of the Taverne amendment.

More information about this copyright law amendment
can be found at https://www.openaccess.nl.

Otherwise as indicated in the copyright section:
the publisher is the copyright holder of this work and the
author uses the Dutch legislation to make this work public.

M.H. van der Horst, R.H.T. Jansen & W. Scherpenisse[1]

Coordinated Vulnerability Disclosure en notificatie in het licht van NIS2

Computerrecht 2025/163

Kwetsbaarheden in software vormen een structureel risico voor de cyberweerbaarheid. Coordinated Vulnerability Disclosure (CVD) en notificatie spelen in de praktijk een cruciale rol, maar zijn in Nederland grotendeels informeel georganiseerd. Met de komst van de NIS2-richtlijn verandert het speelveld: meldloketten worden verplicht, scanmogelijkheden uitgebreid. Deze bijdrage onderzoekt hoe de wetgever en uitvoeringsinstanties kunnen omgaan met CVD en notificatie in het licht van deze richtlijn.

1. Inleiding

Software bevat kwetsbaarheden. Dat is onvermijdelijk. Sommige daarvan zijn triviale schoonheidsfoutjes, andere – zoals de zo gevreesde *zero days* – kunnen de integriteit, vertrouwelijkheid of beschikbaarheid van gegevens en systemen ernstig aantasten. Zo'n zwakke plek in software biedt mogelijkheden voor criminelen of statelijke actoren om binnen te dringen in een geautomatiseerd werk. Om de risico's beheersbaar te houden, is het wenselijk dat kwetsbaarheden tijdig en op zorgvuldige wijze bij de leverancier worden gemeld. Het vertrouwelijk melden van een kwetsbaarheid aan de ontwikkelaar met het doel om op een gecoördineerd moment de informatie te openbaren heet *Coordinated Vulnerability Disclosure* (CVD).[2] De verantwoordelijkheid voor CVD-meldingen ligt vooralsnog voor een belangrijk deel bij de samenleving. Dat roept vragen op over de robuustheid van het huidige CVD-beleid. De inkadering van CVD is bijvoorbeeld tot dusver vooral informeel van aard: er ontbreekt een expliciete wettelijke verankering. Met de implementatie van de NIS2-richtlijn zou daar mogelijk verandering in kunnen komen. Het voornaamste doel van deze richtlijn is het bereiken van een hoog gemeenschappelijk niveau van cyberbeveiliging in de Europese Unie.[3] De richtlijn verplicht lidstaten daarom onder meer om een loket te faciliteren voor het ontvangen van kwetsbaarheidenmeldingen.[4]

CVD is in de praktijk een belangrijk instrument om kwetsbaarheden in kaart te brengen. Toch vormt het slechts een onderdeel van een bredere puzzel van cyberweerbaarheid.[5] Nadat een CVD-procedure is afgerond, is van belang dat gebruikers van kwetsbare software op de hoogte worden gebracht van de kwetsbaarheden. Voor een kwetsbaarhedennotificatie is het noodzakelijk om te weten wie de kwetsbare software gebruikt. Ter achterhaling van deze gebruikers worden kwetsbaarhedenscans ingezet. Voor deze scans geldt een soortgelijk kader als voor CVD, met een grote verantwoordelijkheid voor de samenleving zelf en zonder een eenduidige wettelijke grondslag voor overheidsorganisaties om te scannen. NIS2 biedt ook nadere juridische aanknopingspunten voor het verrichten van deze kwetsbaarhedenscans, want overheidsorganisaties zullen zulke scans mogen uitvoeren.[6]

Het CVD-proces en de bijbehorende kwetsbaarhedennotificatie krijgen in de huidige discussies over (de implementatie van) de richtlijn nog weinig aandacht, terwijl beide belangrijke onderdelen van de 'Europese' cyberweerbaarheidsstrategie vormen. In deze bijdrage staat dan ook de vraag centraal met welke aspecten van de NIS2-richtlijn de wetgever bij de implementatie met name rekening dient te houden vanuit het perspectief van CVD en kwetsbaarhedennotificatie. Gelet op het beperkte bestek van deze bijdrage, beperken wij ons tot kwetsbaarheden in software. Kwetsbaarheden in hardware komen in de praktijk ook voor, maar laten wij hier buiten beschouwing. Na een korte bespreking van het geldende CVD-beleid en de rechtspositie van melders, gaan wij ter nadere duiding in op de technische aspecten van scannen voor notificatie. Vervolgens komt de nationale implementatie van NIS2 via

1 M.H. (Max) van der Horst MSc is als promovendus verbonden aan de Technische Universiteit Delft binnen het Effective Governance for Cybersecurity and Online Safety (EGOS) project en als onderzoeker aan het Dutch Institute for Vulnerability Disclosure (DIVD). Zijn bijdrage aan deze publicatie maakt deel uit van het EGOS-project onder dossiernummer KICH1.VE05.23.001 van het onderzoeksprogramma Cybersecurity voor Digitale Weerbaarheid, dat (deels) is gefinancierd door de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) onder beursnummer https://doi.org/10.61686/GXRYB36907. Mr. drs. R.H.T. (Rowin) Jansen is als universitair docent verbonden aan het Onderzoekscentrum voor Staat en Recht (SteR) en de Interdisciplinary Hub for Digitalization and Society (iHub) van de Radboud Universiteit. Mr. W. (Wouter) Scherpenisse is als docent en promovendus verbonden aan de Erasmus School of Law (ESL) en het Erasmus Center of Law and Digitalization (ECLD) (Sectorplan SSH-breed) van de Erasmus Universiteit Rotterdam (EUR).

2 Zie J. van der Ham & F. Terra, *Ten years of Vulnerability Disclosure in the Netherlands*, 2023 (https://emagazine.one-conference.nl/2023/ten-years-of-vulnerability-disclosure-in-the-netherlands/ (laatst geraadpleegd: 25 augustus 2025)); J.J. Oerlemans, W. Van der Wagen, & M. Weulen Kranenbarg, 'Verschijningsvormen van cybercriminaliteit in enge zin', in: W. Van der Wagen, J.J. Oerlemans, & M. Weulen Kranenbarg (red.), *Basisboek Cybercriminaliteit: Een criminologisch overzicht voor studie en praktijk* (tweede druk), Den Haag: Boom 2024, p. 69-104, p. 78-79.

3 Zie artikel 1 lid 1 NIS2.

4 Artikel 12 lid 1 onder b Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (*PbEU* 2022, L 333).

5 De regering heeft onlangs het voornemen uitgesproken om ook beleid inzake 'Coordinated Accessiblity Disclosure' te ontwikkelen. Hierdoor zullen mensen die problemen ervaren met de digitale toegankelijkheid aan de hand een gestandaardiseerd proces melding kunnen doen. Een en ander is er ook op gericht om de digitale toegankelijkheid van overheidswebsites te vergroten. Zie o.a. *Kamerstukken II* 2024/25, 26 643, nr. 1360, p. 4.

6 Artikel 11 lid 3 onder h NIS2.

de Cyberbeveiligingswet (hierna: Cbw) aan bod.[7] Tot slot volgt een beknopte schets van enkele ontwikkelingen in België die in het licht van deze implementatie belangwekkend zijn. Deze bijdrage stoelt op wet- en regelgeving, parlementaire documenten, beleidskaders en wetenschappelijke literatuur.

2. Een introductie in Coordinated Vulnerability Disclosure

2.1 *De overheid kan het niet alleen*

Om de institutionele en juridische positie van CVD beter te begrijpen, zetten wij eerst uiteen hoe de huidige structuur in de praktijk functioneert.

Waar publieke instanties gebonden zijn aan specifieke mandaten en bevoegdheden, kunnen particuliere actoren zich vrijer over het internet bewegen. Zowel individuen als organisaties kunnen zonder formele toestemming bijdragen aan het opsporen en melden van kwetsbaarheden. Deze vrijwillige beveiligingsonderzoekers – de 'melders' of 'ethisch hackers' – vormen de kern van het huidige, grotendeels informele CVD-landschap in Nederland. Als zij op kwetsbaarheden stuiten, staat het hen in principe vrij om deze te melden aan de verantwoordelijke partij: de leveranciers van de softwareproducten. Deze leveranciers kunnen vervolgens maatregelen nemen om te voorkomen dat derden actief misbruik maken van de kwetsbaarheden.

De motivatie van melders om deel te nemen aan een CVD-proces varieert: veel beveiligingsonderzoekers zijn maatschappelijk gemotiveerd, sommigen handelen uit professioneel belang, anderen rekenen op een (symbolische of financiële) beloning.[8] Denk bij dat laatste aan een vermelding op een '*hall of fame*' of aan een zogeheten '*bug bounty*' in de vorm van t-shirts of geldbedragen.[9]

Het werk van vrijwillige beveiligingsonderzoekers kent naast praktische ook juridische risico's, omdat het zoeken naar 'bugs', datalekken of een ander type kwetsbaarheid in ICT-systemen, behoudens toestemming van de eigenaar, in principe niet is toegestaan. Tegelijkertijd is de hulp van vrijwillige beveiligingsonderzoekers vaak essentieel om organisaties te stimuleren om kwetsbaarheden te verhelpen. In de praktijk wordt deze hulp echter bemoeilijkt doordat onduidelijk is bij wie de kwetsbaarheid kan worden gemeld. Sinds de invoering van de Algemene Verordening Gegevensbescherming (AVG) is de kwaliteit van deze contactinformatie verminderd. Veel informatie in WHOIS-en RDAP-databanken is verouderd, waardoor het lastiger is om contactinformatie aan IP-adressen te koppelen. Van der Horst stelt dat in 2023 naar schatting 41% van de meldingen van het Dutch Institute for Vulnerability Disclosure (hierna: DIVD), een non-profit organisatie bestaande uit vrijwilligers die zoeken naar kwetsbaarheden, voor bepaalde onderzoeken niet bij de bedoelde ontvanger terechtkwam.[10]

Overheidsloketten, zoals dat van het Nationaal Cyber Security Centrum (NCSC), bieden inmiddels wel een vangnet voor melders die geen respons krijgen of geen contactpunt kunnen vinden bij een organisatie. Toch is de inhoudelijke terugkoppeling vanuit deze loketten niet gegarandeerd. Onder onderzoekers leidt dat soms tot frustratie en mogelijk ook tot terughoudendheid om meldingen via officiële kanalen te doen.[11] Daar komt bij dat er vooralsnog gescheiden regimes zijn: het NCSC richt zich uitsluitend op de rijksoverheid en vitale sectoren, terwijl het Digital Trust Center (DTC) zich richt op het niet-vitale bedrijfsleven. Het NCSC deelt informatie enkel met daartoe aangewezen vitale aanbieders en OKTT-organisaties (OKTT staat voor 'objectief kenbaar tot taak').[12] Veel organisaties vallen daar niet onder. Dat dit een problematische situatie kan opleveren, bleek tijdens de Citrix-crisis. Het NCSC mocht toen niet alle getroffen partijen waarschuwen. Het DIVD pakte die taak wel op.[13] Op de samenvoeging van NCSC en DTC, die ophanden is, komen wij zo terug.[14]

2.2 *(In)formele afspraken*

CVD is, als gezegd, te definiëren als het vertrouwelijk melden van een kwetsbaarheid aan de ontwikkelaar met het doel om op een gecoördineerd moment de informatie te openbaren. De ontwikkelaar wordt met de melding in staat gesteld om de kwetsbaarheid in de software te verhelpen. De meerwaarde van CVD is daarmee gelegen in het verbeteren van de algemene cyberveiligheid van systemen. De verkregen inzichten worden idealiter breder verspreid en geopenbaard, zodat een bredere groep dan de betreffende melder en de betrokken organisatie op de hoogte zijn van de kwetsbaarheid en de (mogelijke) remedie. Dit onderdeel van CVD wordt vaak aangeduid als '*public disclosure*'.[15]

Het fundament van CVD is gelegd in 2013. In dat jaar kwam de *Leidraad om te komen tot een praktijk van Responsible Disclosure* tot stand.[16] Nederland ontwikkelde zich daarmee tot koploper op het gebied van CVD. Een

7 *Kamerstukken II* 2024/25, 36764, nr. 2.

8 L.Y.C. Chang e.a., 'Citizen co-production of cyber security: Self-help, vigilantes, and cybercrime', *Regulation & Governance* 2018/12, afl. 1, p. 101-114, p. 103.

9 M. Weulen Kranenbarg, T.J. Holt & J. van der Ham, 'Don't shoot the messenger! A criminological and computer science perspective on coordinated vulnerability disclosure', *Crime Science* 2018/16, afl. 7, p. 3.

10 M. van der Horst, *Global Vulnerability Vigilance: Timely Disaster Notification using Internet-Scale Coordinated Vulnerability Disclosure,* (masterscriptie Universiteit van Amsterdam 2023), (beschikbaar via www.scripties.uba.uva.nl/search?id=record_54279).

11 C. van 't Hof, *Cyberellende was nog nooit zo leuk,* Rotterdam: Tek Tok 2021, p. 241.

12 Zie artikel 3 lid 2 en 20 lid 2 Wbni.

13 Onderzoeksraad voor Veiligheid, *Kwetsbaar door software. Lessen naar aanleiding van beveiligingslekken door software van Citrix,* december 2021, p. 42; 'DIVD-2023-00007 – Global VMware ESXi Ransomware Attack', www.csirt.divd.nl (laatst geraadpleegd: 25 augustus 2025); 'DIVD-2024-00008 – Authentication Bypass and Remote Code Execution in ConnectWise ScreenConnect', www. csirt.divd.nl (laatst geraadpleegd: 25 augustus 2025).

14 *Kamerstukken II* 2024/25,26643, nr. 1277, p. 7.

15 ENISA, *Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations*, November 2015, p. 24.

16 NCSC, *Leidraad om te komen tot een praktijk van Responsible Disclosure,* januari 2013; *Kamerstukken II* 2012/13, 26643, nr. 264.

aantal organisaties begon in 2013 met het publiceren van beleid waarmee het voor melders duidelijk werd op welke wijze meldingen omtrent kwetsbaarheden in de systemen van deze organisaties gedaan konden worden. Met dit beleid geven bedrijven aan open te staan voor meldingen van kwetsbaarheden van buitenaf, beschrijven ze de randvoorwaarden en doen zij beloften over onder meer de terugkoppeling van informatie aan de melder en het afzien van een aangifte.[17] In 2018 volgde een nieuwe versie, getiteld *Coordinated Vulnerability Disclosure: de Leidraad.* Inmiddels is het daarin uiteengezette beleid breed onder bedrijven en overheidsinstanties gecommuniceerd.[18]

Het CVD-beleid tracht een balans te vinden 'tussen het belang om kwetsbaarheden zo snel mogelijk [publiekelijk] bekend te maken, zodat men maatregelen kan treffen, en het belang van ontwikkelaars en leveranciers om voldoende tijd te hebben de kwetsbaarheid te verhelpen'.[19] Maatwerk is mogelijk door het flexibele karakter van het beleid. De CVD-Leidraad biedt namelijk handvatten aan organisaties om hun eigen randvoorwaarden te schetsen voor potentiële melders.[20] De CVD-Leidraad onderkent ook uitdrukkelijk het grote belang van CVD-meldingen voor publieke en private actoren. Specifiek wordt omschreven dat dit belang kan worden gevonden in de verbeterde veiligheid en continuïteit van systemen en de bijdrage aan het algemene ICT-veiligheidsbewustzijn bij bedrijven in Nederland.[21] Het verbeteren van de cyberveiligheid door middel van CVD wordt, zo beschrijft Van der Horst, bereikt via het stimuleren van samenwerking, verminderen van het risico op uitbuiting van kwetsbaarheden en het faciliteren van tijdige beveiligingsverbeteringen.[22]

CVD gaat uit van een melding bij een leverancier van een kwetsbaar product, waarna op een later, gecoördineerd moment de relevante informatie met het publiek wordt gedeeld. Normaliter wordt deze informatie gedeeld met het publiek vanuit de leverancier. In uitzonderlijke situaties kan die informatie ook worden gedeeld vanuit de melder of bijvoorbeeld het NCSC. Het is voorstelbaar dat sommige organisaties zich terughoudend opstellen met betrekking tot deze informatiedeling, bijvoorbeeld vanwege het risico op imagoschade. 'Openbaarmaking van kennis en kwetsbaarheden na het verhelpen' is niettemin het uitgangspunt van het CVD-beleid.[23] Het is dan ook belangrijk om duidelijke afspraken te maken tussen melder en organisatie over de termijn die organisaties kunnen gebruiken om de kwetsbaarheid zoveel als mogelijk op te lossen, voordat de informatie breder wordt gedeeld.

Inmiddels zijn er duidelijke kaders voor CVD-meldingen voorhanden. Er staan voor burgers, bedrijven en overheden nu eenmaal grote belangen op het spel. Situaties waarin melders misbruik maken van hun kennispositie – bijvoorbeeld door geld te eisen voor het leveren van ongevraagde hulp aan organisaties – dienen bovendien te worden voorkomen.[24] De CVD-Leidraad noemt daarom expliciet de verantwoordelijkheid van melders voor het op de hoogte zijn van en het handelen binnen de randvoorwaarden van organisaties met een CVD-beleid.[25] Alleen als melders aan deze randvoorwaarden voldoen, zal de organisatie afzien van een eventuele aangifte wegens computervredebreuk of civielrechtelijke procedures ten aanzien van de mogelijk ontstane schade door de melder of de (reputatie)schade die ontstaat na de openbaring van de kwetsbaarheid.[26] Het is echter denkbaar dat de organisatie, na een melding die zich keurig binnen de randvoorwaarden heeft afgespeeld, toch aangifte doet, bijvoorbeeld omdat een organisatie reputatieschade wil voorkomen of geen mogelijkheid ziet om de kwetsbaarheid binnen een redelijk termijn te verhelpen. In dat geval zullen de politie en het Openbaar Ministerie (OM) 'in principe' geen strafrechtelijk onderzoek starten, aldus de CVD-Leidraad.[27]

2.3 *Strafvervolging?*

Het OM stimuleert organisaties om beleid over het melden van kwetsbaarheden in hun ICT-systemen vast te stellen in eigen CVD-beleid.[28] Het heeft in een beleidsbrief uiteengezet hoe het omgaat met CVD-zaken en onder meer de eventuele vervolging van computervredebreuk.[29] In de betreffende brief uit 2020 benadrukt het OM dat tot dan toe geen strafvervolging was ingesteld naar melders die binnen de randvoorwaarden van het CVD-beleid van organisaties opereerden.[30] Om te kunnen beoordelen of een melder binnen de randvoorwaarden van het CVD-be-

17 NCSC, *Coordinated Vulnerability Disclosure: de Leidraad,* oktober 2018, p. 5.
18 Zo stelt de regering althans in o.a. *Aanhangsel Kamerstukken II* 2023/24, 2524, p. 4-5.
19 CVD-Leidraad, p. 15.
20 Het is overigens ook mogelijk dat melders hun melding doen bij publieke actoren zoals het NCSC, in plaats van bij de leverancier. Het kan namelijk voorkomen dat er in de communicatie tussen melder en leverancier iets misgaat of kan de melder zich niet veilig genoeg voelen om een melding direct bij een organisatie te doen (CVD-Leidraad, p. 14).
21 CVD-Leidraad, p. 5.
22 M. van der Horst, *Global Vulnerability Vigilance: Timely Disaster Notification using Internet-Scale Coordinated Vulnerability Disclosure,* (masterscriptie Universiteit van Amsterdam 2023), p. 3, (beschikbaar via www.scripties.uba.uva.nl/search?id=record_54279).
23 CVD-Leidraad, p. 7.
24 Rb. Den Haag 11 juni 2020, ECLI:NL:RBDHA:2020:5654.
25 CVD-Leidraad, p. 9.
26 Het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd werk of in een deel daarvan kan op verschillende manieren gebeuren. Artikel 138ab Sr geeft zelf al een niet-limitatieve lijst: 'a. door het doorbreken van een beveiliging, b. door een technische ingreep, c. met behulp van valse signalen of een valse sleutel, of d. door het aannemen van een valse hoedanigheid'.
27 CVD-Leidraad, p. 9. Belangrijke bepalingen hierbij zijn artikel 138ab Sr voor computervredebreuk, artikel 139g Sr voor het verwerven, voorhanden hebben of delen van niet-openbare gegevens en artikel 273 Sr voor het openbaren van zulke gegevens. Gelet op het beperkte bestek van deze bijdrage blijft een nadere analyse van dit afwegingskader en de daadwerkelijke toepassing daarvan hier achterwege.
28 'Coordinated Vulnerability Disclosure / ethisch hacken', www.om.nl (laatst geraadpleegd: 25 augustus 2025).
29 OM-beleidsbrief Coordinated Vulnerability Disclosure van 14 december 2020 (kenmerk PaG/B&S/18501).
30 Het OM verwijst hieromtrent naar een brief van de Minister van J&V, welke slechts betrekking heeft op de jaren 2013 en 2014 (OM-beleidsbrief Coordinated Vulnerability Disclosure van 14 december 2020 (kenmerk PaG/B&S/18501), p. 2; *Kamerstukken II* 2014/15, 26643, nr. 342, p. 2.

leid is gebleven, stelt de officier van justitie ten minste de volgende drie vragen:

1. *Is er gehandeld in het kader van een wezenlijk maatschappelijk belang?*
2. *Is er sprake van proportioneel handelen (oftewel: ging de verdachte niet verder dan noodzakelijk was om zijn doel te bereiken)?*
3. *Is er voldaan aan het subsidiariteitsvereiste (oftewel: was/waren er geen minder vergaande manier(en) om het door de verdachte beoogde doel te bereiken)?*

Het genoemde afwegingskader is gebaseerd op jurisprudentie waarin verschillende aspecten van de proportionaliteits- en subsidiariteitsafwegingen worden behandeld.[31] Daarbij geldt dat met name de proportionaliteitseis op verschillende manieren kan worden ingekleurd. In zoverre is, vanuit het perspectief van ethisch hackers bezien, sprake van een zekere mate van onvoorspelbaarheid. Waar de meeste vrijwillige beveiligingsonderzoekers handelen vanuit een maatschappelijk verantwoord motief, is de invulling van 'ethisch handelen' niet altijd eenduidig. Daardoor kan een (onervaren) onderzoeker denken correct te handelen, terwijl dit in de praktijk niet strookt met wat het Openbaar Ministerie verwacht.[32] Sterk casuïstische proportionaliteitsoordelen kunnen afdoen aan de rechtszekerheid voor de betrokken onderzoekers, waardoor de bescherming van ethisch hacken wordt beperkt.

Lang niet alle organisaties hebben eigen CVD-beleid vastgesteld. Een organisatie die daar niet of onvoldoende over heeft nagedacht, kan schrikken van een melding en menen dat deze melding uit kwade bedoelingen voortkomt.[33] Dat laatste is lang niet altijd het geval. In de beleidsbrief benadrukt het OM dan ook dat de melder niet per definitie strafrechtelijk vervolgd dient te worden na een mogelijke aangifte van de organisatie. In dat geval ligt het in de rede om eerst aan de hand van feitenonderzoek vast te stellen of er binnen genoemde uitgangspunten is gehandeld en of er sprake is van 'ethisch hacken' of CVD. Ten slotte is opgemerkt dat 'de bijdrage die CVD levert aan een veilige digitale wereld' zwaar zal wegen in de beoordeling om de melder strafrechtelijk te vervolgen.[34] Toch kan onduidelijkheid over of gebrek aan inzicht in deze dynamiek het gevolg hebben dat onderzoekers ervoor kiezen hun bevinding niet te melden, omdat voor hen de mogelijke consequenties niet goed te overzien zijn. De bereidheid tot het doen van meldingen houdt mede verband met het idee dat onderzoekers zich serieus genomen voelen.[35]

3. Scannen ten behoeve van notificatie

3.1 *Na disclosure: hoe de eindgebruikers te beschermen?*

De CVD-procedure vormt een essentieel kader om kwetsbaarheden op een gecontroleerde en verantwoordelijke wijze bekend te maken, waarbij onderzoekers en leveranciers samenwerken om schade te beperken en tijdig patches beschikbaar te stellen. Daarmee is de kwetsbaarheid echter niet uit de systemen verdwenen. Eindgebruikers van de kwetsbare software hebben vaak geen idee van de kwetsbaarheid en hoe deze kan worden verholpen. Hun systemen kunnen dan onbeschermd blijven. Om de eindgebruikers in kaart te brengen, is het nodig om kwetsbaarhedenscans te verrichten (zie hierna). Net als bij CVD is daarbij een grote verantwoordelijkheid weggelegd voor de betrokken bedrijven, de instellingen en de maatschappij in bredere zin. Op dit moment zijn overheidsorganisaties zoals het NCSC immers niet juridisch uitgerust om zulke scans uit te voeren. De vrijwillige beveiligingsonderzoekers zijn zodoende weer aan zet. Deze vrijwilligers scannen en notificeren in individueel en georganiseerd verband. Voorbeelden van organisaties zijn, naast het al genoemde DIVD,[36] The ShadowServer Foundation,[37] Team Cymru, en Volexity.[38]

Inzet door de genoemde organisaties ontstaat vaak vanuit de wens om structurele tekortkomingen in het informatieproces tussen leveranciers en eindgebruikers te kunnen overbruggen. Dit is vooral belangrijk bij grote incidenten waarbij directe communicatie ontbreekt of niet goed functioneert. In dit opzicht vullen de georganiseerde melders een lacune in het digitale veiligheidsstelsel. Dit type organisaties voeren op grote schaal internetscans uit en informeren (lees: melden) vervolgens de verantwoordelijke partijen over hun kwetsbaarheden.[39] Deze meldingen vinden geregeld plaats in samenwerking met leveranciers of via partners binnen het Landelijk Dekkend Stelsel, kort-

31 Zie Rb. Oost-Brabant 15 februari 2013, ECLI:NL:RBOBR:2013:BZ1163; Rb. Den Haag 17 december 2014, ECLI:NL:RBDHA:2014:15611; Rb. Den Haag 30 augustus 2018, ECLI:NL:RBDHA:2018:10451.

32 Een bekend voorbeeld is de strafzaak tegen politicus Henk Krol. Zie Rb. Oost-Brabant 15 februari 2013, ECLI:NL:RBOBR:2013:BZ1163.

33 M. Weulen Kranenbarg, T.J. Holt & J. van der Ham, 'Don't shoot the messenger! A criminological and computer science perspective on coordinated vulnerability disclosure', *Crime Science* 2018/16, afl. 7, p. 3.

34 OM-beleidsbrief Coordinated Vulnerability Disclosure van 14 december 2020 (kenmerk PaG/B&S/18501), p. 3-4. Vgl. Kranenbarg, Holt & Van der Ham 2018, p. 4.

35 F. Spronk, & M. Weulen Kranenbarg, 'Hacked it! What's next? Een kwalitatief onderzoek naar de afweging van jonge hackers omtrent het maken van meldingen van kwetsbaarheden onder Responsible Disclosure beleid', *Cahiers Politiestudies* 2020/3, afl. 56, p. 177-202, p. 193.

36 www.divd.nl (laatst geraadpleegd: 25 augustus 2025).

37 www.shadowserver.org (laatst geraadpleegd: 25 augustus 2025); zie Operation Endgame ('Partners', www.operation-endgame.com) (laatst geraadpleegd 25 augustus 2025).

38 www.team-cymru.com (laatst geraadpleegd: 25 augustus 2025); zie voor Team Cymru Operation Endgame ('Partners', www.operation-endgame.com (laatst geraadpleegd 25 augustus 2025); www.volexity.com (laatst geraadpleegd: 25 augustus 2025).

39 Onderzoeksraad voor Veiligheid, *Kwetsbaar door software. Lessen naar aanleiding van beveiligingslekken door software van Citrix,* december 2021, p. 42; DIVD-2023-00007 – Global VMware ESXi Ransomware Attack', www.csirt.divd.nl (laatst geraadpleegd: 25 augustus 2025); 'DIVD-2024-00008 – Authentication Bypass and Remote Code Execution in ConnectWise ScreenConnect', www.csirt.divd.nl (laatst geraadpleegd: 25 augustus 2025).

weg LDS.[40] Het LDS is niet één instantie die digitale dreigingsinformatie verzamelt, analyseert en deelt met relevante partijen, maar een omvangrijk netwerk van private en publieke partijen.[41]
Het DIVD beperkt zich met meldingen niet tot vitale sectoren, maar richt zich op alle getroffen organisaties en vervult daarmee een unieke publieke rol. De afhankelijkheid van de hierbij aangesloten vrijwilligers is meer dan eens onderwerp geweest van parlementair debat.[42] Zo wordt bijvoorbeeld de onwenselijkheid van het kwetsbare karakter van de vrijwillige inzet benoemd en is het belang van structurele en duurzame financiering – waar het nu aan schort – onderstreept.[43]

3.2 *Technische duiding van scannen*

Kwetsbaarheden in software kunnen worden gelokaliseerd door software te 'scannen'. Dat begrip behoeft enige technische uitleg. Scannen houdt in dat er wordt gezocht naar tekens dat een systeem fouten bevat die het voor een aanvaller mogelijk maken om de vertrouwelijkheid, integriteit en/of de beschikbaarheid van de informatie op dat systeem aan te tasten. Scannen gebeurt vaak automatisch. Concreet geschiedt het meestal door aanvallen te simuleren en te onderzoeken hoe een systeem daarop reageert. Kwetsbaarheden kunnen echter ook worden afgeleid van bijvoorbeeld de softwareversie van een systeem.
Een specifieke tactiek om kwetsbaarheden te herkennen heet ook wel een 'fingerprint'. Fingerprints worden ingezet om enkele (of een serie van) kwetsbaarheden op een (computer)systeem te bevestigen. Zo kan er bij beveiligingsaudits bijvoorbeeld voor worden gekozen om een softwareproduct te onderwerpen aan een groot aantal fingerprints. De meeste fingerprints zullen niets uithalen. Desalniettemin is dit een effectieve manier om op een snelle manier te testen op de meest voorkomende beveiligingsproblemen. Deze scanmethodiek kent grofweg twee vormen: (1) scannen van één systeem op veel kwetsbaarheden, zoals bij een beveiligingsaudit; (2) scannen van veel systemen op één specifieke kwetsbaarheid, vaak publiek verbonden via het internet. Vooral de tweede methodiek kan vaak gebruikt worden om op een hoog tempo in te schatten wat de publieke blootstelling is voor een nieuwe kwetsbaarheid, zoals bijvoorbeeld in tijden van crisis. In deze vorm ontstaat ook het fenomeen van grootschalige doelwitnotificatie: het op brede schaal detecteren en waarschuwen van kwetsbare systemen nadat de kwetsbaarheid publiek is geworden. In die gevallen betreedt men al snel het domein van ethiek: de voordelen van een fingerprint zullen moeten opwegen tegen de mogelijke consequenties, en dat is zoals benoemd geen strikt juridische afweging. Er moet – en dat is ook juridisch relevant – te allen tijde worden voorkomen dat er grootschalige schade wordt aangebracht aan andermans systemen.
Niet alle kwetsbaarheden reageren exact hetzelfde wanneer deze worden gescand. Dat maakt het belangrijk dat de mogelijke effecten van een fingerprint goed zijn afgewogen en dat bij het scannen de beginselen van proportionaliteit en subsidiariteit in acht worden genomen. De 'intrusiviteit' van een scan dient dus zo beperkt mogelijk te zijn. Met name dat laatste zorgt soms voor wrijving: als de intrusiviteit niet wordt meegenomen in de overweging bij het testen voor kwetsbaarheden, ontstaat de mogelijkheid tot al te vergaande toegang tot systemen of zelfs het aanbrengen van (onnodige) schade.

4. NIS2 en Cbw

Wij verleggen nu de aandacht naar NIS2 en de Cbw. Eind 2022 is de NIS2-richtlijn aangenomen; twee jaar later trad deze in werking. Sindsdien loopt in Nederland op nationaal niveau het traject om deze richtlijn te implementeren in de Cbw. De Cbw had eigenlijk al van kracht moeten zijn, maar dat is vooralsnog niet het geval.[44] Over deze vertraging is elders in dit blad al het nodige opgemerkt.[45] Tot nu toe is er enkel een conceptversie van het wetsvoorstel beschikbaar die de regering voor de advisering heeft voorgelegd aan de Afdeling Advisering van Raad van State.[46] Vanuit het perspectief van NIS2 en dat conceptvoorstel voor de Cbw bezien, vallen een aantal zaken op.
Met betrekking tot kwetsbaarhedenscans merken wij het volgende op. Onder de Wbni ontbreekt een bevoegdheid voor het NCSC en sectorale CSIRT's om gericht te scannen naar kwetsbaarheden in systemen van de entiteiten die vallen onder de reikwijdte van de Wbni. Dat lijkt te veranderen. In het voorstel krijgt het NCSC als de aangewezen CSIRT de bevoegdheid om niet-intrusieve scans uit te voeren op partijen die aangemerkt staan als belangrijke of essentiële entiteit.[47]
Voor 2026 staat echter – wij hintten daar al op – een fusie van verschillende overheidsinstanties gepland.[48] Het DTC en het nationale Computer Security Incident Response Team voor Digitale Serviceproviders (CSIRT-DSP) zullen in aanloop naar 2026 steeds verder met het NCSC integreren.[49] Op 11 februari 2025 informeerde minister van Economische Zaken Beljaarts de Kamer dat de doelgroep van het CSIRT-DSP sinds 1 januari 2025 bediend wordt door

40 Brief van de Minister van Volksgezondheid, Welzijn en Sport van 12 maart 2025, 4061934-1079008-DICIO.
41 Zie uitgebreid R. Brennenraedst e.a., *Informatie-uitwisseling landelijk dekkend stelsel cybersecurity*, Den Haag: WODC 2020.
42 Zie bijvoorbeeld *Kamerstukken II* 2022/23, 36084, nr. 9.
43 *Kamerstukken II* 2022/23, 36200 VII, nr. 116, p. 24.
44 Artikel 42 NIS2.
45 G. van Til & L. Viergever, 'NIS2 en de complexe bedrijfsstructuren van multinationals: tussen theorie en praktijk', *Computerrecht* 2025/88, afl. 3, p. 182-187, aldaar p. 182-183. Zie meer in algemene zin ook L. Viergever & G. van Til, 'NIS2 en de AVG: werk aan de winkel?', *Computerrecht* 2023/166, afl. 4, p. 290-300; N.M. Brouwer & J.J.H. van Mil, 'Cybersecurity in Europa. De herziene Netwerk- en Informatiebeveiligingsrichtlijn (NIS2)', *NJB* 2023/674, afl. 10, p. 748-757.
46 *Kamerstukken II* 2024/25, 36764, nr. 2; *Kamerstukken II* 2024/25, 36764, nr. 4.
47 Artikel 11 lid 3 onder h NIS2 jo. artikel 16 lid 4 Cbw.
48 *Kamerstukken II* 2022/23, 26643, nr. 1058; *Kamerstukken II* 2023/24, 26643, nr. 1143.
49 *Kamerstukken II* 2024/25, 26643, nr. 1277, p. 7.

het NCSC, en dat er wordt gestreefd naar het bedienen van de DTC-doelgroep vanaf het derde kwartaal van 2025.[50] Wij vragen ons daarom af of deze fusie noopt tot een uitbreiding van de doelgroep ten aanzien van de scanbevoegdheid ex artikel 16 lid 4 Cbw. De huidige DTC-entiteiten die straks onder deze nieuwe cyberautoriteit vallen kunnen namelijk eveneens baat hebben bij zulke scans.

De wijze waarop de doelgroep wordt afgebakend kan ook leiden tot problemen voor NIS2-entiteiten. Volgens de Kamerbrief van 11 februari 2025 wordt het aantal entiteiten dat alleen al onder de Cbw valt geschat op 10.000.[51] Ter afbakening van deze entiteiten komt er, op basis van artikel 26 lid 1 van de NIS2, een registratieplicht bij het NCSC. Het registratieregister met de opgenomen entiteiten dat daaruit volgt, bepaalt in zekere zin de reikwijdte van de uitoefening van de verantwoordelijkheden van het NCSC. Daarin moet ten minste de naam van een rechtspersoon, het adres, de sector, subsector en contactinformatie staan. De Cbw breidt deze verplichting uit met IP-reeksen.[52] Volgens een analyse van de Informatiebeveiligingsdienst (IBD) uit april 2025 is deze registratie echter foutgevoelig. Er ontstaat door deze foutgevoeligheid een grote kans op een mismatch tussen de geregistreerde systemen van een belangrijke of essentiële entiteit en hun daadwerkelijke infrastructuur.[53] De IBD geeft aan dat dit alleen handmatig kan worden opgelost, wat voor dit aantal partijen geen schaalbare situatie lijkt. Als men wil voorkomen dat NIS2-entiteiten niet per abuis uit het oog worden verloren, kan het werken zonder afgekaderd registratieregister een oplossing zijn.

Van belang is ook dat het melden van kwetsbaarheden gedeeltelijk zal worden gecodificeerd.[54] Artikel 12 lid 1 onder b NIS2 jo. voorgesteld artikel 34 Cbw biedt namelijk een grondslag voor vrijwillige meldingen aan coördinatoren ('CSIRT's') door rechtspersonen, maar ook door natuurlijke personen. Dat is een uitbreiding ten opzichte van het huidige artikel 16 Wbni. Uit de memorie van toelichting van de Wbni blijkt namelijk dat de potentiële melder – 'de betrokken dienstverlener' – zich beperkt tot rechtspersonen en commerciële dienstverleners zonder rechtspersoonlijkheid.[55] En, als gezegd: juist natuurlijke personen vormen een belangrijke schakel in het CVD-landschap. Ondanks de genoemde uitbreiding zal een essentieel onderdeel van CVD buiten de reikwijdte van het wetsvoorstel vallen. Op de verhouding melder-organisatie gaat het voorstel voor de Cbw namelijk niet in, laat staan het daadwerkelijk opsporen en openbaren van kwetsbaarheden. Dat is in zoverre begrijpelijk, omdat NIS2 zich richt op de cyberweerbaarheid van specifieke entiteiten en niet op de wisselwerking tussen vrijwillige beveiligingsonderzoekers en deze entiteiten. Niettemin lijkt het mogelijk om zonder al te veel juridische complexiteit de nodige ruimte te bieden aan CVD, door de publicatie van een (standaard) CVD-beleid op de website van de NIS2-entiteiten in het wetsvoorstel op te nemen als verplichte beveiligingsmaatregel.[56] Onderzoek laat namelijk zien dat de meldingsbereidheid toeneemt als er een (ondubbelzinnig) CVD-beleid door een organisatie online is geplaatst.[57] Op die manier wordt bewustwording over CVD gestimuleerd en weten melders (beter) onder welke spelregels ze kunnen opereren. Uiteraard biedt dergelijk CVD-beleid geen garantie voor de hogere meldingsbereidheid: als organisaties meldingen niet serieus opvolgen of melders alsnog juridische risico's lopen, kan dit onderzoekers juist afschrikken. Desondanks is het publiceren van CVD-beleid een simpele maatregel die gebaseerd kan worden op bestaande templates,[58] wat het een gunstige kosten-batenafweging maakt.

Het (deels) formaliseren van de relatie tussen vrijwillige beveiligingsorganisaties en het NCSC heeft overigens in het verleden al eens op de politieke agenda gestaan.[59] De toenmalige minister van Justitie en Veiligheid Yeşilgöz-Zegerius steunde bijvoorbeeld de oproep om te onderzoeken hoe het functioneren van het DIVD beter zou kunnen worden geborgd.[60] Bij de totstandkoming van de Wet Computercriminaliteit III is eveneens een oproep gedaan om *responsible disclosure* te bevorderen,[61] en ook in de latere parlementaire behandeling is aandacht gevraagd voor vrijwillige beveiligingsonderzoekers.[62] Het lopende wetgevingstraject biedt dan ook een kans om deze oproep (alsnog) naar concrete wetgeving te vertalen.

5. Ontwikkelingen in België

Nederland vervulde lange tijd een voortrekkersrol op het gebied van CVD, zo stelden wij hiervoor al vast. Inmiddels maakt België een inhaalslag. In tegenstelling tot het Nederlandse CVD-beleid is het Belgische CVD-beleid, en daarmee ook de positie van melders, wettelijk verankerd.[63] België heeft CVD uitdrukkelijk gecodificeerd in de NIS2-imple-

50 *Kamerstukken II* 2024/25, 26643, nr. 1277.
51 *Kamerstukken II* 2024/25, 26643, nr. 1277, p. 4.
52 Artikel 44 lid 1 onder b Cbw (nationale register).
53 'Registratieplicht Cyberbeveiligingswet: 3 stappen in de voorbereiding', www.informatiebeveiligingsdienst.nl (laatst geraadpleegd: 25 augustus 2025).
54 W. Scherpenisse & S. van Schendel (Erasmus Center of Law and Digitalization), *Reactie op de Cyberbeveiligingswet (Cbw)*, juni 2024, p. 4 (te raadplegen via: www.internetconsultatie.nl/cyberbeveiligingswet/reactie/09c82020-88d5-4c2a-b26c-16cf34eb2d66).
55 *Kamerstukken II* 2017/18, 34 883, nr. 3, p. 44.
56 Zie artikel 21 NIS2.
57 F. Spronk, & M. Weulen Kranenbarg, 'Hacked it! What's next? Een kwalitatief onderzoek naar de afweging van jonge hackers omtrent het maken van meldingen van kwetsbaarheden onder Responsible Disclosure beleid', *Cahiers Politiestudies* 2020/3, afl. 56, p. 177-202, p. 185-186.
58 'Example CVD policy', www.coordinatedvulnerabilitydisclosure.org (laatst geraadpleegd: 25 augustus 2025).
59 *Kamerstukken II* 2022/23, 36 084, nr. 11, p. 24.
60 *Kamerstukken II* 2022/23, 36 084, nr. 11, p. 30.
61 *Kamerstukken II* 2016/17, 34 372, nr. 23.
62 *Kamerstukken II* 2022/23, 26 643, nr. 1015, p. 8.
63 C. Somers, 'Ethisch hacken uit de illegaliteit in België', *Computerrecht* 2023/111, afl. 2, p. 111; vgl. het Duitse codificatievoorstel: Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Modernisierung des Computerstrafrechts, 4 november 2024 (te raadplegen via: www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/2024_ComputerStrafR.html?nn=110490 (laatst geraadpleegd: 25 augustus 2025)).

mentatiewet (hierna: NIS2-wet).[64] Het Centrum voor Cybersecurity België (CCB) is daarin – overeenkomstig artikel 12 lid 1 onder b NIS2 – aangewezen als nationaal meldpunt, met vastgelegde rollen, verantwoordelijkheden en doorlooptijden.[65] Dat biedt enerzijds uniformiteit in het meldingsproces en rechtszekerheid. Anderzijds leidt dat ook tot problemen ten aanzien van een kernprincipe van CVD: de openbaarmaking van kwetsbaarheden.

De crux is dat de Belgische NIS2-wet strikte geheimhouding verbindt aan de CVD-procedure. Artikel 23 lid 1 onder 5 bepaalt dat melders toestemming nodig hebben van het CCB om informatie over de kwetsbaarheden te openbaren. Publicatie zonder toestemming van het CCB is niet toegestaan, zelfs niet bij een trage afhandeling of ontbrekend zicht op mitigatie. *Public disclosures* zijn daarmee niet langer het uitgangspunt. In combinatie met de centrale positie van het CCB ontstaat zo een juridische lock-in die onderzoekers ontmoedigt om te melden. Terra[66] en De Vaere[67] wijzen erop dat het principe van tijdelijke terughoudendheid verschuift naar onbeperkte stilzwijgplicht, omdat artikel 23 melders verplicht het door de ontvangende organisatie of het CCB opgelegde proces volledig te volgen, ook als dit disproportioneel is. Zoals De Vaere uitlegt:

> "under the current Belgian framework, public disclosure is de facto prohibited. The CCB seems to rarely grant permission to disclose, and reporters are expected to remain silent indefinitely, even when a vulnerability remains unaddressed. This undermines transparency and reduces pressure on organizations to fix serious issues".[68]

De vraag is zodoende of de potentiële, gewenste voordelen in het kader van rechtszekerheid in het Belgische model opwegen tegen de beperkte ruimte voor openbaarheid. Nu openbaarheid als uitgangspunt geldt van het CVD-beleid in Nederland, lijkt ons dat niet waarschijnlijk.[69] Daarnaast: als het gevolg van het Belgische beleid is dat de meldingsbereidheid van vrijwillige beveiligingsonderzoekers afneemt of zelfs staakt, dan ontmoedigt het beleid juist CVD-meldingen, in plaats van deze te faciliteren. Het decentrale karakter van het Nederlandse CVD-beleid biedt meer ruimte voor alternatieve meldroutes, waaronder een directe melding bij de leveranciers of via onafhankelijke intermediairs. De keerzijde is dat de CVD-praktijk in juridisch opzicht minder voorspelbaar is, met name op het punt van de bescherming voor melders. De bescherming tegen civiele of strafrechtelijke claims blijft afhankelijk van afwegingen op basis van jurisprudentie en casuïstiek.

6. Slot

In Nederland lijken CVD en de bijbehorende notificatie zich op een kruispunt te bevinden. Waar de maatschappelijke waarde ervan onmiskenbaar is, blijft de institutionele inbedding versnipperd en zijn de kaders vooralsnog grotendeels beleidsmatig van aard. Vrijwillige beveiligingsonderzoekers, zoals het DIVD, vervullen een publiek relevante functie. Zij opereren echter in een juridisch schemergebied, waarin de toepassing en de uitwerking van het OM-afwegingskader niet in alle gevallen duidelijk voorspelbaar zijn. Het wettelijk beschermen van vrijwillig beveiligingsonderzoekers lijkt echter niet per definitie bij te dragen aan een robuuster systeem, zo doen althans de ontwikkelingen in België vermoeden. Het centraliseren van meldingen en het verbinden van voorwaarden aan het openbaren van informatie over kwetsbaarheden kan leiden tot terughoudendheid aan de zijde van potentiële melders en doet de meldingsbereidheid mogelijk afnemen. Tegelijkertijd biedt de implementatie van NIS2 een kans om de samenwerking tussen overheid – die zelf nieuwe scanmogelijkheden krijgt – en samenleving te versterken. Het verplicht stellen van CVD-beleid bij NIS2-entiteiten, en het onderkennen van de belangrijke rol van vrijwillige beveiligingsonderzoekers, zou de meldingsbereidheid kunnen vergroten en kunnen bijdragen aan de cyberweerbaarheid. De uitdaging ligt, kortom, in het vinden van een balans die voldoende voorspelbaarheid biedt, zonder de meldingsbereidheid te ondermijnen.

64 Wet van 26 april 2024, tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare, B.S. 17 mei 2024, p. 63179.

65 Zie artikel 3 lid 1 van het Koninklijk besluit tot uitvoering van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, B.S. 2024 juni 2024, p. 78183.

66 'Belgium is unsafe for CVD', www.floort.net (laatst geraadpleegd: 25 augustus 2025).

67 'Belgian CVD is deeply broken', www.devae.re (laatst geraadpleegd: 25 augustus 2025).

68 'Belgian CVD is deeply broken', www.devae.re (laatst geraadpleegd: 25 augustus 2025).

69 CVD-Leidraad, p. 7.