CENTRE FOR
CYBER SECURITY
BELGIUM

UNDER THE AUTHORITY OF
THE PRIME MINISTER

BELEID VOOR DE GECOÖRDINEERDE BEKENDMAKING VAN KWETSBAARHEDEN

COORDINATED VULNERABILITY DISCLOSURE POLICY

Beleid voor de gecoördineerde bekendmaking van kwetsbaarheden *(Coordinated Vulnerability Disclosure Policy – "CVDP")*

Ieder informaticasysteem of netwerk kan kwetsbaarheden bevatten. Zowel mensen met goede als mensen met slechte bedoelingen kunnen deze kwetsbaarheden opsporen. De angst om gerechtelijk vervolgd te worden, belet mensen met goede bedoelingen ("ethische hackers") echter vaak om kwetsbaarheden te melden.

Het ongeoorloofd binnendringen in een informaticasysteem of de poging hiertoe is strafbaar, zelfs als het informaticasysteem niet beveiligd is en de persoon met goede bedoelingen handelt. Wanneer de persoon over een toegangsmachtiging tot het informaticasysteem beschikt, zijn de rechtsregels echter anders.

Een organisatie die een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden voert of een beloningsprogramma voor het opsporen van kwetsbaarheden toepast, verleent minstens een gedeeltelijke toegangsmachtiging tot het betrokken informaticasysteem.

De organisatie kan immers een beroep doen op een onderneming om de beveiliging van haar informatiesystemen na te gaan (bijvoorbeeld door middel van een veiligheidsaudit) of op "ethische hackers" (via een CVDP of *bug bounty*-programma).

Een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden[1] *(**Coordinated Vulnerability Disclosure Policy – "CVDP"**) is een geheel van regels die vooraf zijn bepaald door een organisatie die verantwoordelijk is voor informatiesystemen waardoor deelnemers*[2] *met goede bedoelingen (of "ethische hackers") mogelijke kwetsbaarheden*

1 *Ook "beleid voor verantwoorde bekendmaking" genoemd: wij verkiezen de term "gecoördineerde" in plaats van "verantwoorde" aangezien die elke verwarring met de wettelijke aansprakelijkheidsbegrippen vermijdt en de nadruk legt op het wederzijdse karakter van het proces.*

2 *Dit kunnen bijvoorbeeld cybersecurity-onderzoekers of gebruikers zijn. Deelnemers kunnen eventueel onderworpen worden aan een selectie door een derde vertrouwenspersoon ("coördinator").*

in haar systemen kunnen opsporen, of haar alle relevante informatie hierover kunnen bezorgen. Deze regels, doorgaans openbaar gemaakt op een website, maken het mogelijk een juridisch kader te bepalen voor de samenwerking tussen de verantwoordelijke organisatie en de beleidsdeelnemers. Deze regels moeten onder meer de vertrouwelijkheid van de uitgewisselde informatie garanderen en een eventuele bekendmaking van ontdekte kwetsbaarheden op een verantwoorde en gecoördineerde manier omkaderen.

Een beloningsprogramma voor het opsporen van kwetsbaarheden *(bug bounty-programma)[3] heeft betrekking op alle regels die een verantwoordelijke organisatie heeft bepaald om beloningen toe te kennen aan deelnemers die kwetsbaarheden identificeren in de door haar gebruikte technologieën. Deze beloning kan een geldsom zijn, maar ook een geschenk of een gewone publieke erkenning (rangschikking onder de beste deelnemers, publicatie, conferentie, enz.). Het betreft een beleidsvorm voor de gecoördineerde bekendmaking van kwetsbaarheden die voorziet in de toekenning van een beloning aan de deelnemer naargelang de hoeveelheid, het belang of de kwaliteit van de bezorgde informatie. Deze beleidsvorm is aantrekkelijker voor eventuele deelnemers en leidt vaak tot betere resultaten voor de organisatie. De organisatie kan met name een beroep doen op een bug bounty-platform dat technische en administratieve bijstand biedt voor het beheer van haar beloningsprogramma voor het opsporen van kwetsbaarheden (rol van coördinator)[4].*

Momenteel beschikken tal van organisaties al over een CVDP, al dan niet samen met een bug bounty-programma.

Om organisaties te helpen bij het uitvoeren van een CVDP, heeft het Centrum voor Cybersecurity België (CCB) deze brochure en een (tweedelige) gids[5] opgesteld en biedt het een model van CVDP aan. Deze documenten zijn beschikbaar op de website van het CCB.

Het CCB heeft overigens zelf een CVDP ingevoerd en gepubliceerd op zijn website (*www.ccb.belgium.be/nl/vulnerability-policy*).

---

3 In het Engels "vulnerability rewards program" of "bug bounty program".

4 Zie bijvoorbeeld: www.intigriti.com (België); www.yeswehack.com, www.yogosha.com (Frankrijk); www.zerocopter.com (Nederland); www.hackerone.com, www.bugcrowd.com (VS).

5 Gids over het beleid voor de gecoördineerde bekendmaking van kwetsbaarheden, Deel I: Goede praktijken en Deel II: Wettelijke aspecten, Centrum voor Cybersecurity België (CCB), 2020 (www.ccb.belgium.be).

In deze brochure vindt u een samenvatting van de begrippen, doelstellingen, juridische vraagstukken en goede praktijken rond de invoering van een CVDP in de huidige stand van de Belgische wetgeving – voor meer informatie verwijzen we naar de Gids CVDP (Delen I en II) en naar het voorbeeld van een CVDP.

We wijzen erop dat de door het CCB opgestelde documenten geenszins de bestaande wettelijke regels wijzigen. Het ongeoorloofd binnendringen in het informaticasysteem van een derde, zelfs met goede bedoelingen, is een strafrechtelijk misdrijf.

De deelnemer aan een CVDP moet zich ervan bewust zijn dat hij zich niet kan beroepen op een algemene uitsluiting van aansprakelijkheid wanneer hij deelneemt aan dat beleid: hij moet omzichtig te werk gaan en alle voorwaarden van het beleid, alsook de toepasselijke wettelijke bepalingen nauwgezet naleven.

Voor organisaties:

Welke voordelen biedt de invoering van een CVDP voor uw organisatie?
De uitvoering van een CVDP:

a) biedt een juridisch kader voor een nuttige, eerlijke, doeltreffende, wettelijke en budgetvriendelijke samenwerking.

Het beleid voor de gecoördineerde bekendmaking van kwetsbaarheden is een vorm van toetredingsovereenkomst waarin alle contractuele bepalingen worden vastgelegd door de verantwoordelijke organisatie en vervolgens worden aanvaard door de deelnemer wanneer deze vrij beslist om deel te nemen aan het uitgewerkte programma. De invoering van een dergelijk beleid verduidelijkt de juridische situatie van de deelnemers. Ze kunnen immers aantonen dat ze over een voorafgaande toegangsmachtiging tot de betrokken informaticasystemen beschikken en dus niet ongeoorloofd binnendringen in

die systemen, mits de in het beleid vermelde voorwaarden worden nageleefd (zie Gids Deel II: Wettelijke aspecten).

Het beleid voor de gecoördineerde bekendmaking van kwetsbaarheden biedt de mogelijkheid om de beveiliging van systemen of uitrusting voortdurend en doeltreffend na te gaan. Vanzelfsprekend is het beleid aantrekkelijker en doeltreffender wanneer de verantwoordelijke organisatie beslist om de deelnemers beloningen toe te kennen naargelang het belang en de kwaliteit van de verstrekte informatie (in het kader van een beloningsprogramma voor het opsporen van kwetsbaarheden of bug bounty-programma). Zelfs wanneer de organisatie beloningen toekent en een beroep doet op een externe coördinator (platform voor ethische hacking), is de invoering van een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden doorgaans budgetvriendelijker dan de uitvoering van audits door externe bedrijven.

b) zorgt voor een betere beveiliging van informatiesystemen en moedigt onderzoek aan.

Naast andere technische en organisatorische maatregelen kan het opzetten van deze samenwerking een passende maatregel zijn om incidenten te voorkomen die de beveiliging van de netwerk- en informatiesystemen van de organisatie in het gedrang zouden brengen. Ze biedt het onmiskenbare voordeel dat kwetsbaarheden worden geïdentificeerd en verholpen voordat zich een beveiligingsincident voordoet. Dit beleid kan niet alleen zorgen voor een betere beveiliging maar ook voor een betere kennis inzake cybersecurity en het onderzoek in dit domein aanmoedigen.

c) zorgt ervoor dat gebruikers vertrouwen hebben in informatietechnologieën.

De uitvoering van een CVDP toont het publiek en de gebruikers dat de verantwoordelijke organisatie veel waarde hecht aan de veiligheid van haar informatietechnologieën. Deze aanpak houdt immers in dat de organisatie zich ertoe verbindt de door de deelnemers verstrekte informatie te verwerken en te proberen de geïdentificeer-

de kwetsbaarheden te verhelpen, of minstens de gebruikers op de hoogte te brengen van de risico's. Deze verbintenis kan ook een marketingargument zijn. De organisatie kan erop wijzen in haar communicatie. Vertrouwen in informatiesystemen is zeker een belangrijk element voor gebruikers of consumenten.

d) garandeert de vertrouwelijkheid.

De volledige bekendmaking van een kwetsbaarheid, terwijl die nog altijd bij tal van gebruikers bestaat, vormt een groot veiligheidsrisico inzake informatietechnologieën. Derden met slechte bedoelingen kunnen immers specifieke tools ontwikkelen en verspreiden om deze kwetsbaarheid uit te buiten. De openbaarmaking van beveiligingsproblemen kan ook de reputatie van de verantwoordelijke organisatie schaden en het vertrouwen van de gebruikers in de betrokken technologieën aantasten. Het belang van een CVDP bestaat er dus in een juridisch kader vast te leggen dat de vertrouwelijkheid bevordert en een eventuele openbare bekendmaking zo goed mogelijk regelt.

e) zorgt voor een betere naleving van de wettelijke verplichtingen op het vlak van de beveiliging van informatietechnologieën.

Een organisatie die een beleid voor gecoördineerde bekendmaking voert, kan aantonen dat zij zich inspant om haar wettelijke verplichtingen voor de beveiliging van haar netwerk- en informatiesystemen na te leven: Algemene Verordening Gegevensbescherming EU nr. 2016/679 ("AVG"), wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid ("NIS-wet"), regelgeving burgerlijke aansprakelijkheid, Wetboek van economisch recht, enz. (zie Gids Deel I: Goede praktijken).

Elke organisatie kan de nadere regels van een CVDP bepalen, op voorwaarde dat ze bepaalde elementen opneemt zodat het beleid ten volle juridische uitwerking kan hebben. We raden dus aan de volgende maatregelen te nemen:

- **Gemachtigde personen**: laat het beleid goedkeuren door iemand die uw organisatie rechtsgeldig kan vertegenwoordigen (bijvoorbeeld de directeur).
- **Openbaarheid**: de inhoud van uw CVDP moet beschikbaar en toegankelijk zijn voor de deelnemer: op uw website, op de website van een coördinator (bijvoorbeeld een *bug bounty*-platform). Indien mogelijk moet het CVDP in de verschillende talen van uw website zijn opgesteld. We raden aan een beknopte en duidelijke, maar volledige tekst op te stellen.
- **Contactpunt**: vermeld duidelijk een contactpunt of gebruik een onlineformulier. Communiceer vervolgens zoveel en zo efficiënt mogelijk met de deelnemers. Zij kunnen u helpen nagaan of uw technische oplossing werkt.
- **Coördinator**: het aanstellen van een coördinator kan u veel efficiënter doen werken. Zo kan het gebruik van een platform voor beloningsprogramma's voor het opsporen van kwetsbaarheden (*bug bounty*-platform) ervoor zorgen dat een groter aantal kwetsbaarheden worden gemeld. Indien de deelnemers aan het beleid of de aangestelde coördinator niet reageren, kan u standaard een beroep doen op het CCB (vulnerabilityreport@cert.be) als coördinator.
- **Beveiliging en vertrouwelijkheid van de communicatie:** beveilig uw communicatie en zorg ervoor dat de vertrouwelijkheid gewaarborgd wordt.
- **Toepassingsgebied**: vermeld duidelijk op welke sites, producten, toestellen, diensten, systemen en netwerken uw CVDP van toepassing is. Ga bedachtzaam te werk bij de keuze van het toe-

passingsgebied van uw beleid, op basis van de elementen van uw systeem die u technisch kan controleren. Alle systemen die afhankelijk zijn van derden die niet uitdrukkelijk zouden hebben ingestemd met de regels van uw CVDP, dient u uit te sluiten. Als u voor bepaalde onderdelen van uw systeem niet kan nagaan of het CVDP gevolgd werd, neemt u deze best niet op in het toepassingsgebied van uw CVDP. Wat niet uitdrukkelijk in het toepassingsgebied is vermeld, valt in principe niet onder het toepassingsgebied van het beleid.

- **Voorwaarden**: vermeld duidelijk wat de deelnemer wel en niet mag doen om het bestaan van een vermoedelijke kwetsbaarheid aan te tonen. Eventuele wijzigingen van gegevens in het informaticasysteem mogen slechts minimaal zijn (bijvoorbeeld de aanwezigheid van *visit logs*). Verbied uitdrukkelijk de installatie van malware of virussen, het stelen van paswoorden, het verwijderen of wijzigen van parameters van het systeem, "Distributed Denial of Service (DDoS)"-aanvallen, "social engineering"-aanvallen, phishing, het massaal versturen van ongewenste e-mails (spamming), enz. U dient het gebruik, het bezit, het onthullen of het bekendmaken uit te sluiten van de inhoud van niet voor het publiek toegankelijke communicatie of van gegevens van een informaticasysteem waarvan de deelnemer redelijkerwijs moet weten dat deze illegaal verkregen zijn (zoals gestolen paswoorden die op het internet zijn gevonden).
- **Melding**: vermeld duidelijk welke informatie best wordt verstrekt bij het melden van een incident (beschrijving van de kwetsbaarheid, configuratiedetails, verrichte handelingen, gebruikte tools, data van de tests, bewijzen, IP-adres of URL van het aangetaste systeem, screenshot, contactgegevens, enz.). Bepaal op voorhand de antwoordtermijnen voor het versturen van informatie over een kwetsbaarheid en voor de andere fasen van de procedure. Vermeld deze termijnen ook bij elk contact. Behoud het recht op flexibiliteit naargelang de complexiteit, dringendheid en omvang van de kwetsbaarheid.
- **Evenredigheid**: laat de gebruikers zich ertoe verbinden niet verder te gaan dan redelijk is om de kwetsbaarheid aan te tonen. Dit impliceert ook dat de beschikbaarheid van de diensten van de verantwoordelijke organisatie niet mag worden verstoord door het onderzoek.
- **Vertrouwelijkheid**: eis dat de in het kader van het beleid uitgewisselde informatie vertrouwelijk wordt behandeld.

- **Uitvoering te goeder trouw**: verbind u ertoe de inhoud van uw beleid na te leven en de deelnemer die de voorwaarden ervan naleeft noch burgerrechtelijk noch strafrechtelijk te vervolgen.
- **Verwerking van persoonsgegevens**: vermeld duidelijk welke verplichtingen de partijen moeten nakomen inzake de verwerking van persoonsgegevens.
- **Ontwikkel een oplossing en pas deze toe** binnen een redelijke termijn indien dit mogelijk is. Breng de deelnemers hiervan ook op de hoogte.
- **Bedank de deelnemers**, ook al wijzen ze u op kwetsbaarheden. Ze hebben uw dienst per slot van rekening veiliger proberen te maken. Dit kan u best doen via een beloningsprogramma voor het opsporen van kwetsbaarheden (*bug bounty*-programma), waarbij de beloning afhangt van het belang van de kwetsbaarheid. Zo'n beleid is aantrekkelijker voor eventuele deelnemers en vaak doeltreffender voor uw organisatie. De beloning kan verschillende vormen aannemen: een geldsom, een geschenk of eenvoudigweg een openbaar deelnemersklassement (*Leaderboard*).
- **Bied deelnemers de mogelijkheid om te publiceren** over de kwetsbaarheid. Dit is vaak een grote drijfveer voor hun onderzoek. Publicaties over de kwetsbaarheid (bijvoorbeeld zonder vermelding van uw organisatie) dragen bij tot veiligere informatiesystemen.
- **Informeer het CCB** (vulnerabilityreport@cert.be) en derden (of hun representatieve organisaties) die waarschijnlijk ook zijn getroffen door de kwetsbaarheid.

Voor deelnemers

Een CVDP biedt de mogelijkheid om op een legale manier kwetsbaarheden op te sporen en te melden. Deze opportuniteit steunt op een machtiging, onder bepaalde voorwaarden, en draait om wederzijds vertrouwen.

Het is dus belangrijk dat u de inhoud van het CVDP aandachtig doorleest voordat u actie onderneemt:

- **Respecteer de voorwaarden van het CVDP**: respecteer het toepassingsgebied en de voorwaarden van het CVDP.

- **Evenredigheid**: ga niet verder dan redelijk is om de kwetsbaarheid aan te tonen. Dit is de rode draad in al uw acties.
  - Als de kwetsbaarheid op kleine schaal kan worden aangetoond, hoeft u niet verder te gaan.
  - Verzamel enkel de nodige bewijzen (downloads of screenshots), bij voorkeur zonder persoonsgegevens.
  - Verstoor de beschikbaarheid van het systeem niet, en gebruik de kwetsbaarheid enkel voor zover nodig is om deze aan te tonen en te documenteren.
- **Vertrouwelijkheid en beveiliging van de resultaten van uw onderzoek**: deel geen informatie over ontdekte kwetsbaarheden met derden en verspreid deze informatie niet onder derden, behoudens uitdrukkelijke toestemming van de betrokken organisatie. Respecteer ook de aanbevolen beveiligde communicatiemiddelen.
- **Wees zo volledig mogelijk** in uw rapportering. Gebruik ook *timestamps* om aan te tonen dat u zo snel mogelijk na de ontdekking van de kwetsbaarheid hebt gehandeld: zo neemt u elke twijfel over uw intenties weg. Probeer vooraf controles uit te voeren om het bestaan van de kwetsbaarheid te bevestigen, en eventuele risico's te identificeren.
- **Regelmatige communicatie**: wees geduldig en vriendelijk in uw communicatie: misschien weet de organisatie niet zo goed hoe gepast om te gaan met deze kwetsbaarheid. Het is ook mogelijk dat een bepaalde kwetsbaarheid al vaker gemeld werd en geen risico leek te vormen.
- **Uitvoering te goeder trouw**: uw acties moeten aantonen dat geen sprake is van bedrieglijk opzet, het oogmerk om te schaden, of de wil om gebruik te maken van of schade te veroorzaken aan het bezochte systeem of aan de gegevens ervan.
- **Eventuele openbare bekendmaking**: vraag steeds de toestemming van de verantwoordelijke organisatie vóór elke openbare bekendmaking over de kwetsbaarheid. Wacht ook een redelijke tijd (in overleg met de organisatie) zodat een oplossing kan worden ontwikkeld en toegepast. Een organisatie kan er steeds voor kiezen geen oplossing te ontwikkelen en toe te passen, behalve indien ze daar wettelijk of contractueel toe verplicht is. Als u toch vindt dat een oplossing moet worden ontwikkeld, onderneem geen stappen die het CVDP kunnen schenden, en contacteer het CCB (vulnerabilityreport@cert.be) als coördinator.

- **Verwerking van persoonsgegevens**: een CVDP heeft niet tot doel om intentioneel persoonsgegevens te verwerken. Het is echter wel mogelijk dat de deelnemer persoonsgegevens moet verwerken in het kader van zijn onderzoek naar kwetsbaarheden. Respecteer in dat geval uw verplichtingen inzake de bescherming van persoonsgegevens.
- **Vraag geen beloning** als de verantwoordelijke organisatie dit niet vooraf duidelijk heeft vermeld in haar CVDP/*bug bounty*-programma. Elk verzoek om een beloning buiten de door het CVDP bepaalde voorwaarden kan dan worden gelijkgesteld met een illegale poging tot afpersing.

Als u per toeval een kwetsbaarheid ontdekt bij een organisatie zonder CVDP, onderneem dan geen verdere stappen. Als de kwetsbaarheid kritiek is, neemt u best contact op met een derde coördinator zoals een bug bounty-platform of, bij gebrek hieraan, met het CCB (vulnerabilityreport@cert.be). Opzettelijk en ongeoorloofd binnendringen in een informaticasysteem blijft strafbaar zonder CVDP.

Referenties

Gids over het beleid voor de gecoördineerde bekendmaking van kwetsbaarheden: deel I (Goede praktijken), Centrum voor Cybersecurity België (CCB), 2020 (www.ccb.belgium.be).

Gids over het beleid voor de gecoördineerde bekendmaking van kwetsbaarheden: deel II (Wettelijke aspecten), Centrum voor Cybersecurity België (CCB), 2020 (www.ccb.belgium.be).

European union Agency for Network and Information security (ENISA), *Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations*, 2015, www.enisa.europa.eu/publications/vulnerability-disclosure en *Economics of Vulnerability Disclosure*, 2018, www.enisa.europa.eu/publications/economics-of-vulnerability-disclosure

Software Engineering Institute, *The CERT Guide to Coordinated Vulnerability Disclosure, 2013 (updated in 2019)* https://vuls.cert.org/confluence/display/CVD

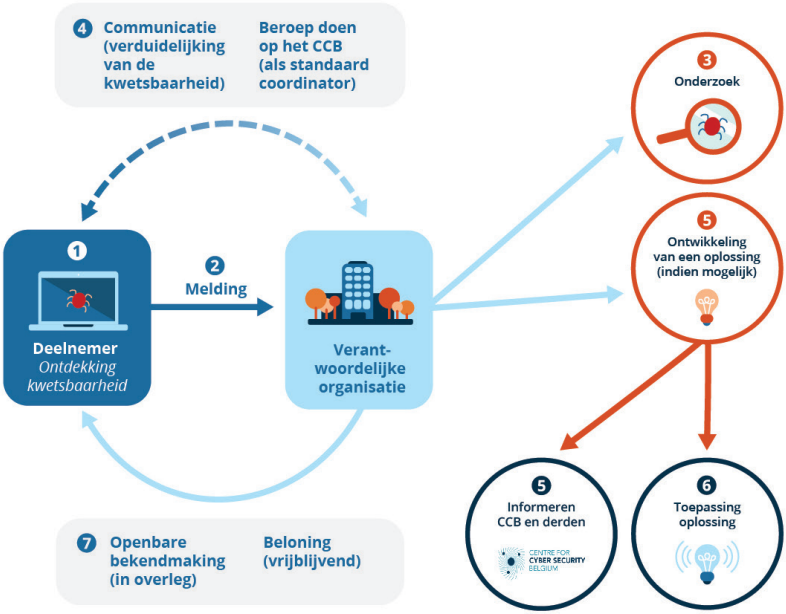
National Cyber Security Centre (NL), *Leidraad Coordinated Vulnerability Disclosure (Coordinated Vulnerability Disclosure: the Guideline)*, 2019, //english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline en *Policy for arriving at a practice for Responsible Disclosure*, 2013

CIO Platform Nederland - CEG Information Security, *Coordinated Vulnerability Disclosure. Model Policy and Procedure*, 2016, www.cio-platform.nl/en/publications en *Coordinated Vulnerability Disclosure 1.4. Implementation guide*, 2016, www.cio-platform.nl/en/publications

ISO/IEC 29147:2018 Information technology — Security techniques — Vulnerability disclosure
(https://www.iso.org/standard/72311.html).

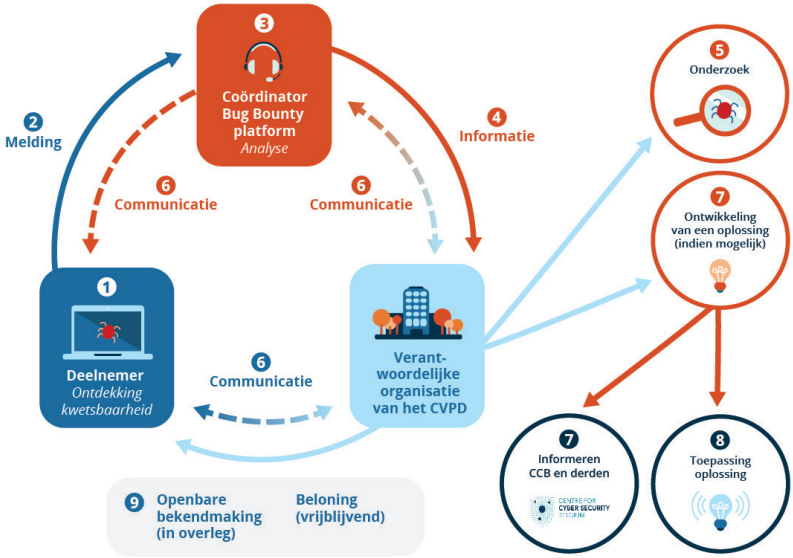
ISO/IEC 30111:2019 Information technology — Security techniques — Vulnerability handling processes (https://www.iso.org/standard/53231.html).

CVDP zonder coördinator



1. De deelnemer vindt een kwetsbaarheid binnen de context van het beleid voor de gecoördineerde bekendmaking van kwetsbaarheden (CVDP)
2. De deelnemer rapporteert de kwetsbaarheid aan de verantwoordelijke organisatie op basis van de CVDP voorwaarden.
3. De verantwoordelijke organisatie onderzoekt de kwetsbaarheid.
4. Er is regelmatige communicatie tussen de deelnemer en de verantwoordelijke organisatie om de kwetsbaarheid te verduidelijken. De organisatie kan beroep doen op het CCB (als standaard coördinator) bij gebrek aan communicatie in dit proces.
5. Indien mogelijk wordt een oplossing ontwikkeld. In het geval dat de kwetsbaarheid ook andere organisaties zou kunnen treffen, informeert de verantwoordelijke organisatie het CCB hierover.
6. De verantwoordelijke organisatie past de oplossing toe voor gebruikers of klanten.
7. De mogelijkheid tot openbare publicatie van de kwestsbaarheid kan onderling overlegd worden en een beloning uitreiken kan op basis van de CVDP-voorwaarden.

CVDP met coördinator



1. De deelnemer vindt een kwetsbaarheid binnen de context van het beleid voor de gecoördineerde bekendmaking van kwetsbaarheden (CVDP)
2. De deelnemer rapporteert de kwetsbaarheid aan de coördinator (zoals een bug bounty platform) op basis van de CVDP voorwaarden.
3. De coördinator analyseert de kwetsbaarheid.
4. Na validatie informeert de coördinator de verantwoordelijke organisatie.
5. De verantwoordelijke organisatie onderzoekt de kwetsbaarheid.
6. Er is regelmatige communicatie tussen de deelnemer en de verantwoordelijke organisatie om de kwetsbaarheid te verduidelijken. Indien wenselijk kan de organisatie daarvoor beroep doen op de coördinator.
7. Indien mogelijk wordt een oplossing ontwikkeld. In het geval dat de kwetsbaarheid ook andere organisaties zou kunnen treffen, informeert de verantwoordelijke organisatie het CCB hierover.
8. De verantwoordelijke organisatie past de oplossing toe voor gebruikers of klanten.
9. De mogelijkheid tot openbare publicatie van de kwestsbaarheid kan onderling overlegd worden en een beloning uitreiken kan op basis van de CVDP-voorwaarden.

Deze gids en de bijbehorende documenten zijn opgesteld door het Centrum voor Cybersecurity België (CCB), een federale overheidsdienst opgericht bij koninklijk besluit van 10 oktober 2014 en onder het gezag van de eerste minister.

Het Centrum voor Cybersecurity België wijst alle aansprakelijkheid voor de inhoud van deze gids af.

De verstrekte informatie:
- is uitsluitend van algemene aard en heeft niet tot doel alle specifieke gevallen te behandelen;
- is niet noodzakelijk op alle punten volledig, nauwkeurig of up-to-date.

Prepress en druk
Centrale drukkerij van de Kamer van Volksvertegenwoordigers

Brussel, oktober 2020

Verantwoordelijke uitgever
Centrum voor Cybersecurity België
M. De Bruycker, Directeur
Wetstraat, 16
1000 Brussel

D/2020/14828/011