CENTRE FOR
CYBER SECURITY
BELGIUM

GIDS OVER HET BELEID VOOR DE GECOÖRDINEERDE BEKENDMAKING VAN KWETSBAARHEDEN

DEEL I: GOEDE PRAKTIJKEN

COORDINATED VULNERABILITY DISCLOSURE POLICIES -"CVDP"
RESPONSIBLE DISCLOSURE POLICIES -"RD"

CENTRUM VOOR
CYBERSECURITY BELGIË
Wetstraat 16
1000 Brussel

info@ccb.belgium.be
www.ccb.belgium.be

UNDER THE AUTHORITY
OF THE PRIME MINISTER

.be

CENTRE FOR CYBER SECURITY BELGIUM

A. INHOUDSOPGAVE

B. INLEIDING 4
I. Achtergrond 4
II. Begrippen 4
III. Doelstellingen 7
a. Een juridisch kader bieden voor een nuttige, eerlijke, doeltreffende, wettelijke en budgetvriendelijke samenwerking 7
b. Informatiesystemen beter beveiligen en onderzoek aanmoedigen 9
c. Ervoor zorgen dat gebruikers vertrouwen hebben in informatietechnologieën 10
d. Vertrouwelijkheid garanderen 10
e. Zorgen voor een betere naleving van de wettelijke verplichtingen op het vlak van de beveiliging van informatietechnologieën 12

C. GOEDE PRAKTIJKEN 17
I. Inhoud van een CVDP 19
a. Gemachtigde personen 19
b. Openbaarheid 19
c. Contactpunt 20
d. Veiligheid en vertrouwelijkheid van de communicatie 21
e. Beschrijving van de wederzijdse verplichtingen 22
II. Procedure 30
a. Ontdekking 30
b. Melding 31
c. Onderzoek 31
d. Toepassing van een oplossing 32
e. Eventuele openbare bekendmaking 33

D. REFERENTIES 37

CENTRE FOR
CYBER SECURITY
BELGIUM

<u>Waarschuwing</u>:

In deze gids vindt u een overzicht van de begrippen, doelstellingen, juridische vraagstukken en goede praktijken rond de invoering van een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden (of Coordinated Vulnerability Disclosure Policy – "CVDP") in de huidige stand van de Belgische wetgeving – zie de voorbeelden op de website van het CCB.

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.

** Shutterstock - 2020*

CENTRE FOR CYBER SECURITY BELGIUM

B. INLEIDING

I. Achtergrond

Het toenemende belang van informatiesystemen in onze samenleving vergroot aanzienlijk het risico op incidenten in verband met de beveiliging van deze systemen. Deze incidenten kunnen bijvoorbeeld de beschikbaarheid van een bepaalde dienst of de integriteit, authenticiteit of vertrouwelijkheid van gegevens in het gedrang brengen. Aangezien meer en meer objecten worden gebruikt die verbonden zijn met internet, zal een eventueel incident nog grotere gevolgen hebben.

Wat de oorzaken van deze incidenten betreft, vormt het bestaan van kwetsbaarheden een groot risico. Dit risico is evenwel inherent aan het ontwikkelings-, gebruiks- en updateproces van deze systemen. Rekening houdend met de omvang en techniciteit van dit probleem lijkt het een illusie te geloven dat alle producenten of verantwoordelijken van informatiesystemen in staat zullen zijn dit in hun eentje te verhelpen.

Een organisatie kan ervoor kiezen een beroep te doen op een bepaalde onderneming om de beveiliging van haar informatiesystemen na te gaan (bijvoorbeeld door middel van een veiligheidsaudit), of, op openbare wijze, op personen met goede bedoelingen ("*ethische hackers*") die wensen bij te dragen aan een betere beveiliging van deze technologieën door bestaande kwetsbaarheden te identificeren en ze te helpen oplossen.

II. Begrippen

A. ***Een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden[1] (CVDP)*** is een geheel van regels die vooraf zijn bepaald door een organisatie die verantwoordelijk is voor informatiesystemen

[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.

waardoor deelnemers[2] (of "*ethische hackers*"), met goede bedoelingen, mogelijke kwetsbaarheden 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 de ontdekte kwetsbaarheden op een verantwoorde en gecoördineerde manier omkaderen.

Het begrip "bekendmaking" betekent dus niet noodzakelijk dat de kwetsbaarheid openbaar wordt gemaakt, maar veeleer dat de deelnemer deze meedeelt aan de verantwoordelijke organisatie. De deelnemer is verplicht de kwetsbaarheid mee te delen aan de verantwoordelijke organisatie, maar de openbare bekendmaking ervan (door de deelnemer of de betrokken organisatie) is facultatief in het kader van een CVDP.

B. *Een kwetsbaarheid*[3] is een gebrek of een zwakke plek, een ontwerp[4]- of uitvoeringsfout[5], het ontbreken van updates in het licht van de bestaande technische kennis, die de veiligheid van informatietechnologieën[6] in het gedrang kan brengen. Een kwetsbaarheid kan leiden tot een onverwacht of ongewenst voorval en uitgebuit worden door kwaadwillige derden om de integriteit, authenticiteit, vertrouwelijkheid of beschikbaarheid van een systeem[7] te schenden of om een systeem schade toe te brengen.

---

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

[3] EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA), *Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations*, 2015, p. 14, punt 2.2, www.enisa.europa.eu/publications/vulnerability-disclosure.

[4] Bijvoorbeeld een fout of een vergetelheid in het ontwerp van een systeem of protocol die het intrinsiek kwetsbaar maken.

[5] Bijvoorbeeld een fout tijdens de implementering, de configuratie of het gebruik.

[6] Bijvoorbeeld een systeem, netwerk, proces, programma, toepassing, dienst, protocol of component.

[7] Of van de informatie die het bevat.

C. ***Een verantwoordelijke organisatie*** is een natuurlijke of rechtspersoon die een systeem of product in verband met informatietechnologieën beheert, bezit, verkoopt of produceert en in dat opzicht verantwoordelijk is voor de veiligheid en de goede werking ervan.

D. ***De deelnemer aan een CVDP[8] (of "ethische hacker")*** is een persoon met goede bedoelingen die, met toestemming van de verantwoordelijke organisatie, wenst bij te dragen aan een betere beveiliging van de informatiesystemen. Hij kan bijvoorbeeld pentests uitvoeren of andere methoden gebruiken om de beveiliging van informatiesystemen na te gaan. Hij staat lijnrecht tegenover de *hacker* die zijn vaardigheden gebruikt om met slechte bedoelingen ongeoorloofd binnen te dringen in een systeem[9]. De deelnemer wil de verantwoordelijke van het informatiesysteem of een coördinator op de hoogte brengen van eventueel ontdekte kwetsbaarheden, zodat ze kunnen worden weggewerkt.

E. ***Een coördinator*** is een natuurlijke of rechtspersoon die als tussenpersoon optreedt tussen de deelnemer en de organisatie die verantwoordelijk is voor een informatiesysteem door logistieke, technische en juridische bijstand te bieden of een andere functie te vervullen[10] om de samenwerking te vergemakkelijken. Als geen coördinator is aangewezen in het kader van het beleid, kan het Centrum voor Cybersecurity België (vulnerabilityreport@cert.be) die rol vervullen.

F. ***Een beloningsprogramma voor het opsporen van kwetsbaarheden (of bug bounty-programma)[11]*** 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

[8] In het Engels gewoonlijk "white hat" genoemd, waarbij wordt verwezen naar het feit dat helden in Amerikaanse westerns traditioneel een witte hoed droegen.
[9] In het Engels gewoonlijk "black hat" genoemd, waarbij wordt verwezen naar het feit dat boeven in Amerikaanse westerns traditioneel een zwarte hoed droegen.
[10] Bijvoorbeeld een rol als beoordelaar van kwetsbaarheidsverslagen of als bemiddelaar.
[11] In het Engels "vulnerability rewards program" of "bug bounty program".

beloning aan de deelnemer naargelang de hoeveelheid, het belang of de kwaliteit van de overgemaakte 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).

III. Doelstellingen

a. Een juridisch kader bieden voor een nuttige, eerlijke, doeltreffende, wettelijke en budgetvriendelijke samenwerking

Wanneer een organisatie een beroep doet op een bepaalde externe dienstverlener om de beveiliging van haar informatiesystemen na te gaan, sluit ze met hem een veiligheidsauditovereenkomst die de uitvoering van pentests kan omvatten (in het Engels “penetration test” of “pentest”), waarbij een aanval van personen met slechte bedoelingen wordt gesimuleerd om bestaande kwetsbaarheden aan te tonen. In dat geval worden de wederzijdse juridische verplichtingen van de partijen in principe omschreven in een specifieke overeenkomst of algemene voorwaarden[12].

Dat is echter niet altijd het geval wanneer een organisatie wil samenwerken met niet nader bepaalde personen (*deelnemers* of *ethische hackers*) die kwetsbaarheden in haar informatiesystemen kunnen identificeren. Er bestaat dan geen duidelijk contractueel kader tussen de partijen. In dat geval blijkt het noodzakelijk dat de organisatie vóór elke samenwerking haar verwachtingen en de juridische verplichtingen van de deelnemers bepaalt.

[12] De verantwoordelijke organisatie kan deze taken ook toevertrouwen aan bepaalde werknemers. De respectieve verplichtingen van de partijen zullen dan worden omschreven in een specifiek intern reglement of in het algemeen arbeidsreglement.

Het beleid voor de gecoördineerde bekendmaking van kwetsbaarheden is in dat opzicht 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 over het beleid voor de gecoördineerde bekendmaking van kwetsbaarheden. Deel II: Wettelijke aspecten*).

Deze samenwerking kan de verantwoordelijke organisatie op eerlijke en rechtmatige wijze informatie verschaffen over kwetsbaarheden van haar systemen en haar in staat stellen adequaat en tijdig op te treden. Zo kunnen potentiële risico's en schade die deze kwetsbaarheden kunnen veroorzaken, zoveel mogelijk doeltreffend worden voorkomen of beperkt.

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[13]).

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

[13] Buiten een beloningsprogramma voor het opsporen van kwetsbaarheden kan de verantwoordelijke organisatie eenzijdig beslissen over de toekenning van een (niet voorziene) beloning aan de deelnemer na de procedure.

externe bedrijven.[14] De toekenning van een beloning in het kader van een *bug bounty*-programma vloeit immers voort uit een resultaatsverbintenis in hoofde van de deelnemer, terwijl een externe auditor doorgaans slechts gebonden is door een middelenverbintenis. Die laatste moet dus worden vergoed voor al zijn prestaties, ook al heeft hij na afloop van zijn onderzoek geen kwetsbaarheden of enkel minder belangrijke kwetsbaarheden gevonden.

b. Informatiesystemen beter beveiligen en onderzoek aanmoedigen

De invoering van een beleid biedt de verantwoordelijke organisatie de kans om vanuit diverse bronnen informatie over de beveiliging van haar informatiesystemen te verkrijgen. Rekening houdend met de huidige complexiteit en techniciteit van deze systemen blijkt het heel nuttig om gebruik te maken van een groot aantal potentiële experten in plaats van een beroep te doen op enkele externe dienstverleners die moeilijk deskundig kunnen zijn in alle door de organisatie gebruikte technologieën.

Naast andere technische en organisatorische maatregelen kan het opzetten van deze samenwerking een passende maatregel zijn om incidenten te voorkomen die de beveiliging van haar netwerk- en informatiesystemen in het gedrang zouden brengen. Ze biedt het onmiskenbare voordeel dat kwetsbaarheden worden geïdentificeerd en verholpen voordat zich een beveiligingsincident voordoet.

Een betere beveiliging kan worden bereikt door kwetsbaarheden te verhelpen, de risico's in verband met het bestaan van kwetsbaarheden tot een minimum te beperken en deze risico's voor de informatiesystemen van de verantwoordelijke organisatie voortdurend te evalueren.

[14] Sommige kosten moeten noodzakelijk worden voorzien, zoals bijvoorbeeld de kosten voor het technisch team dat nodig is voor de analyse van de informatie die de deelnemers verstrekken.

De invoering van een CVDP impliceert uiteraard dat de organisatie beschikt over beveiligingsmaatregelen die kunnen worden getest en over een intern (of extern) team dat de door de deelnemers verstrekte informatie kan opvolgen.

Naast het verhogen van de veiligheid kan dit soort beleid ook de kennis inzake cybersecurity verbeteren en het onderzoek in dit domein aanmoedigen. De werkzaamheden van onderzoekers maken het mogelijk om nieuwe kwetsbaarheden te identificeren, alsook de omstandigheden waarin ze zich voordoen, de methodes om ze te vermijden en de middelen om ze te verhelpen.

c. Ervoor zorgen 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 geïdentificeerde 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. Vertrouwelijkheid garanderen

De vertrouwelijkheid van de informatie over een kwetsbaarheid in een informaticasysteem moet zoveel mogelijk worden gegarandeerd.

De volledige bekendmaking van een kwetsbaarheid[15], 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.

Het is dus niet wenselijk om een beveiligingsprobleem openbaar te maken voordat het door de verantwoordelijke organisatie wordt verholpen, die daartoe de nodige tijd moet krijgen, of voordat de verantwoordelijke organisatie de overheden belast met de beveiliging van netwerk- en informatiesystemen[16] hierover heeft kunnen informeren.

De volledige bekendmaking kan ook de doeltreffende toepassing van een oplossing voor de kwetsbaarheid vertragen door de verantwoordelijke organisatie te verplichten om in een crisissituatie te reageren.

De openbaarmaking van beveiligingsproblemen kan ook de reputatie van de verantwoordelijke organisatie schaden en het vertrouwen van de gebruikers in de betrokken technologieën aantasten.

Bovendien kan de verspreiding of beschikbaarstelling aan het publiek van informaticagegevens, zoals software of instructies, die het mogelijk maken om door de beveiliging van informaticasystemen te breken, een misdrijf zijn[17] of diegene die de informatie heeft bekendgemaakt burgerlijk aansprakelijk stellen[18] (*zie Gids - Deel II Wettelijke aspecten*).

---

[15] "Full disclosure".
[16] In België neemt het Centrum voor Cybersecurity België (CCB) deze rol hoofdzakelijk op zich. In voorkomend geval kan het CCB organisaties van essentieel belang (overheden, aanbieders van essentiële diensten, digitaledienstverleners, kritieke infrastructuren, enz.) informeren.
[17] Art. 550 *bis*, § 5, van het Strafwetboek.
[18] Art. 1382 van het Burgerlijk Wetboek.

Bijgevolg moet de openbare bekendmaking van informatie over een kwetsbaarheid uiterst zorgvuldig en in coördinatie met de verantwoordelijke organisatie gebeuren.

De verantwoordelijke organisatie moet binnen een redelijke termijn reageren: ze implementeert een oplossing of informeert minstens de gebruikers van de door de kwetsbaarheid getroffen informatiesystemen. De organisatie kan immers, bijvoorbeeld, aansprakelijk worden gesteld omdat zij haar klanten in het ongewisse heeft gelaten over het bestaan van de kwetsbaarheid (zie punt e hieronder).

Het kan ook heel nuttig blijken om, wanneer de belangrijkste veiligheidsrisico's zijn weggewerkt, informatie over de ontdekte kwetsbaarheden en de oplossing ervan bekend te maken, in een passend kader[19], om het onderzoek inzake informaticabeveiliging vooruit te helpen.

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. Zorgen voor een betere naleving van de wettelijke verplichtingen op het vlak van de beveiliging van informatietechnologieën

Door een beleid voor gecoördineerde bekendmaking te voeren, kan de organisatie 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.

[19] Bijvoorbeeld in wetenschappelijke publicaties of technische verslagen die worden verspreid onder onderzoekers inzake informaticabeveiliging.

Artikel 32 van de AVG bepaalt dat de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen moeten nemen om een op het risico afgestemd beveiligingsniveau te waarborgen, rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de risico's voor de rechten en vrijheden van natuurlijke personen (die qua waarschijnlijkheid en ernst uiteenlopend zijn).

De bepaling verduidelijkt dat de verwerkingsverantwoordelijke en de verwerker met name een beroep kunnen doen op:

a) de pseudonimisering en versleuteling van persoonsgegevens;
b) het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
c) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

In haar aanbeveling betreffende de na te leven veiligheidsmaatregelen ter voorkoming van gegevenslekken (nr. 01-2013) herinnert de Commissie voor de bescherming van de persoonlijke levenssfeer (nu Gegevensbeschermingsautoriteit) eraan dat het belangrijk is om de informatiebeveiligingsmaatregelen zo vaak als nodig te documenteren, te controleren en te verbeteren[20].

Ook de richtsnoeren met betrekking tot de informatiebeveiliging van persoonsgegevens van de voormalige Commissie voor de bescherming van de persoonlijke levenssfeer wijzen erop dat de verwerkingsverantwoordelijke op regelmatige basis een degelijke audit moet organiseren met

[20] Aanbeveling betreffende de na te leven veiligheidsmaatregelen ter voorkoming van gegevenslekken (nr. 01-2013), https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/aanbeveling_01_2013_0.pdf, p. 3, punt 6.

betrekking tot informatiebeveiliging van persoonsgegevens en beheersmaatregelen moet nemen om de vertrouwelijkheid en de integriteit van de gegevens te garanderen.[21]

De uitvoering van een CVDP is een passende technische en organisatorische maatregel om, naast andere maatregelen, aan te tonen dat de verwerkingsverantwoordelijke zich inspant om enerzijds op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van zijn verwerkingssystemen te garanderen[22] en anderzijds regelmatig de doeltreffendheid van de maatregelen ter beveiliging van de verwerking te testen, te beoordelen en te evalueren[23]. De internationale technische normen inzake de beveiliging van informatietechnologieën raden overigens uitdrukkelijk aan om een CVDP uit te voeren (zie bijvoorbeeld de internationale normen ISO/IEC 29147[24] en 30111[25]).

De verantwoordelijke organisatie kan dan op haar CVDP steunen om, ten aanzien van de toezichthoudende autoriteiten persoonsgegevens, aan te tonen dat zij zich inspant om de risico's in verband met kwetsbaarheden in haar informatiesystemen te evalueren en te beheersen.

[21] Commissie voor de bescherming van de persoonlijke levenssfeer, *Richtsnoeren met betrekking tot de informatiebeveiliging van persoonsgegevens*, (versie 2.0 dec. 2014), p. 20 en 27, https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/Richtsnoeren_CBPL_V%202%200_3.pdf.
[22] Art. 32 (1), punt b, van de AVG.
[23] Art. 32 (1), punt d, van de AVG.
[24] ISO/IEC 29147:2018 Information technology — Security techniques — Vulnerability disclosure (https://www.iso.org/standard/72311.html).
[25] ISO/IEC 30111:2019 Information technology — Security techniques — Vulnerability handling processes (https://www.iso.org/standard/53231.html).

Een CVDP laat de verwerkingsverantwoordelijke ook toe beter geïnformeerd te zijn over mogelijke inbreuken in verband met persoonsgegevens en te beoordelen welke inbreuken zo snel mogelijk aan een toezichthoudende autoriteit[26] of een natuurlijke persoon[27] moeten worden gemeld.

Vervolgens bepaalt artikel 20 van de NIS-wet dat de aanbieder van essentiële diensten ("AED") "passende en evenredige technische en organisatorische maatregelen [moet nemen] om de risico's voor de beveiliging van netwerk- en informatiesystemen waarvan zijn essentiële diensten afhankelijk zijn, te beheersen. Deze maatregelen zorgen, rekening houdend met de stand van de technische kennis, voor een niveau van fysieke en logische beveiliging van netwerk- en informatiesystemen dat is afgestemd op de risico's die zich voordoen".

De AED moet ook "passende maatregelen [nemen] om incidenten die de beveiliging van de voor de verlening van die essentiële diensten gebruikte netwerk- en informatiesystemen aantasten, te voorkomen of de gevolgen ervan te minimaliseren, teneinde de continuïteit van deze diensten te waarborgen"[28].

Beveiligingsmaatregelen worden in de NIS-wet omschreven als maatregelen die een systeem in staat stellen om, met een bepaalde mate van betrouwbaarheid, bestand te zijn tegen acties die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van de opgeslagen, verzonden of verwerkte gegevens of de daaraan gerelateerde diensten die via die netwerk- en informatiesystemen

[26] Art. 33 van de AVG bepaalt dat de verwerkingsverantwoordelijke inbreuken in verband met persoonsgegevens onverwijld en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft genomen, moet melden aan de bevoegde toezichthoudende autoriteit, tenzij het niet waarschijnlijk is dat deze inbreuken een risico inhouden voor de rechten en vrijheden van natuurlijke personen. Ook de verwerker moet de verwerkingsverantwoordelijke onverwijld informeren zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens.

[27] Art. 34 van de AVG bepaalt dat de verwerkingsverantwoordelijke de betrokkene onverwijld op de hoogte moet brengen van een inbreuk in verband met persoonsgegevens wanneer deze inbreuk waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van een natuurlijke persoon.

[28] Art. 20 van de NIS-wet; zie ook art. 33 van de NIS-wet voor de beveiligingsmaatregelen van digitaledienstverleners (DDV's) – bijvoorbeeld aanbieders van cloudcomputerdiensten.

worden aangeboden of toegankelijk zijn, in gevaar brengen[29]. Om de nodige maatregelen te nemen die in verhouding staan tot de risico's[30], moeten de risico's op incidenten worden geïdentificeerd en de gevolgen ervan voor de beveiliging van netwerk- en informatiesystemen worden geminimaliseerd.

In casu biedt de uitvoering van een CVDP de AED of digitaledienstverlener de mogelijkheid om een beter zicht te hebben op eventuele kwetsbaarheden en bedreigingen voor zijn netwerk- en informatiesystemen teneinde een adequaat antwoord te bieden op de eisen van de NIS-wet.

Daarnaast bepaalt de Europese Cyberbeveiligingsverordening ("Cyber Security Act")[31] dat een Europese cyberbeveiligingscertificeringsregeling ten minste regels moet omvatten over de wijze waarop voorheen onopgemerkte kwetsbaarheden in de cyberbeveiliging van ICT-producten[32], -diensten[33] en -processen[34] moeten worden gemeld en aangepakt.[35]

Zo verplicht de Verordening de fabrikant of aanbieder van gecertificeerde ICT-producten, - diensten en -processen om de contactgegevens van de fabrikant of aanbieder en aanvaarde methoden voor het ontvangen, van eindgebruikers en beveiligingsonderzoekers, van kwetsbaarheidsinformatie openbaar te maken.[36]

---

[29] Art. 6, 9°, van de NIS-wet.
[30] Art. 6, 15°, van de NIS-wet omschrijft het risico als "elke redelijkerwijs vast te stellen omstandigheid of gebeurtenis met een mogelijke negatieve impact op de beveiliging van netwerk- en informatiesystemen".
[31] Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013.
[32] Een element of groep elementen van een netwerk- of informatiesysteem (art. 2, 12, van de Cyberbeveiligingsverordening).
[33] Een dienst die volledig of hoofdzakelijk bestaat in de verzending, opslag, opvraging of verwerking van gegevens door middel van netwerk- en informatiesystemen (art. 2, 13 van de Cyberbeveiligingsverordening).
[34] Een reeks activiteiten die wordt uitgevoerd om een ICT-product of ICT-dienst te ontwerpen, ontwikkelen, leveren of onderhouden (art. 2, 14, van de Cyberbeveiligingsverordening).
[35] Art. 54, 1, m, van de Cyberbeveiligingsverordening.
[36] Art. 55, 1, c, van de Cyberbeveiligingsverordening.

Bovendien kan de verantwoordelijke organisatie (contractueel of buitencontractueel) burgerlijk aansprakelijk worden gesteld wanneer een beveiligingsprobleem van haar technologieën schade heeft veroorzaakt aan een derde.[37]

Tot slot moet de verantwoordelijke organisatie die informatiesystemen verkoopt haar klanten vrijwaren voor verborgen gebreken of conformiteitsgebreken van de verkochte goederen.[38] Als producent van een product (lichamelijk goed) of aanbieder van een dienst mag ze ook enkel veilige producten op de markt brengen en veilige diensten aanbieden.[39] De overeenstemming met die algemene veiligheidsverplichting kan worden beoordeeld rekening houdend met de nationale of internationale normen, de gedragscodes die gelden in de betrokken sector, de huidige stand van de kennis en van de techniek, en de beveiliging die gebruikers redelijkerwijs mogen verwachten.[40]

C. GOEDE PRAKTIJKEN

Momenteel zijn er in België al tal van ondernemingen die een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden toepassen en een beroep doen op *bug bounty*-platformen.

Er bestaan twee internationale ISO/IEC-normen inzake CVDP: ISO/IEC 29147[41] en ISO/IEC 30111[42]. De eerste beschrijft de procedure voor de bekendmaking van een kwetsbaarheid, terwijl de tweede handelt over de verwerkingsprocedures voor de gemelde kwetsbaarheid. Deze twee normen beschrijven een volledig model met de verschillende aspecten van een CVDP.

---

[37] Art. 1382 van het Burgerlijk Wetboek.
[38] Zie art. 1641 en 1625 van het Burgerlijk Wetboek voor de vrijwaring voor verborgen gebreken of art. 1649 *bis* e.v. van het Burgerlijk Wetboek over de vrijwaring voor het gebrek aan overeenstemming voor verkopen aan consumenten.
[39] Zie art. IX.2 e.v. van het Wetboek van economisch recht.
[40] Bij gebrek aan geharmoniseerde Europese normen.
[41] ISO/IEC 29147:2018 Information technology — Security techniques — Vulnerability disclosure (https://www.iso.org/standard/72311.html).
[42] ISO/IEC 30111:2019 Information technology — Security techniques — Vulnerability handling processes (https://www.iso.org/standard/53231.html).

ENISA (Agentschap van de Europese Unie voor cyberbeveiliging) heeft eveneens aanbevelingen gepubliceerd over goede praktijken met betrekking tot de invoering van een CVDP.[43]

** Colored-security-background-flat-design Free licence - Designed Freepik - 2020*

[43] 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. Art. 6 (1), b, van Verordening (EU) 2019/881 belast ENISA overigens met het verlenen van bijstand aan de lidstaten van de Unie en de Europese instellingen bij de opstelling en uitvoering van een openbaarmakingsbeleid inzake kwetsbaarheden op vrijwillige basis.

CENTRE FOR CYBER SECURITY BELGIUM

I. Inhoud van een CVDP

a. Gemachtigde personen

Het beleid moet worden ingevoerd door personen of organen die de verantwoordelijke organisatie rechtsgeldig kunnen vertegenwoordigen en niet, bijvoorbeeld, door een lid van het informaticateam dat daartoe niet rechtsgeldig gemachtigd is[44]. Machtigingen in het kader van het beleid voor gecoördineerde bekendmaking moeten immers noodzakelijkerwijs afkomstig zijn van een persoon die daartoe gemachtigd is door de houder van de rechten op het betrokken systeem of de betrokken uitrusting[45].

b. Openbaarheid

De openbaarheid die aan het beleid voor verantwoorde bekendmaking wordt gegeven, is een belangrijk element voor het succes ervan[46]. De inhoud ervan moet dus gemakkelijk toegankelijk zijn voor potentiële deelnemers, bij voorkeur op de website van de verantwoordelijke organisatie. Het bestaan van het CVDP moet daarom duidelijk en zichtbaar vermeld worden op de website van de verantwoordelijke organisatie (bijvoorbeeld met een specifieke tab of een onderdeel met de volledige inhoud van het beleid)[47]. Hiervoor bestaan standaardiseringsvoorstellen waarbij het CVDP van een organisatie wordt opgenomen in een “security.txt”-bestand op een gekende locatie van de

[44] Onder voorbehoud van de leer van de schijnvertegenwoordiging of van het algemene rechtsbeginsel van de eerbied voor de gewettigde verwachtingen van de ander.
[45] Dit is standaard de eigenaar van het systeem.
[46] Om te vermijden dat een misdrijf wordt gepleegd (ongeoorloofd binnendringen in een informatiesysteem), is het noodzakelijk dat het beleid voor gecoördineerde bekendmaking bestaat vooraleer de deelnemer enige stap zet. De beste manier om twijfels over het al dan niet bestaan van een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden te vermijden, is het openbaar maken ervan. (Zie Deel II. Wettelijke aspecten). Het is evenwel mogelijk dat de organisatie een niet-openbaar CVDP heeft, dat beperkt is tot enkele vooraf geselecteerde deelnemers (zie met name sommige particuliere *bug bounty*-programma’s).
[47] Bijvoorbeeld: https://www.[organisatie].be/security of /disclosurepolicy of nog /vulnerability-policy.

boomstructuur van iedere website[48] of extensies voor webbrowsers om websites die over een CVDP beschikken op te sporen[49].

Indien een beroep wordt gedaan op een beloningsprogramma voor het opsporen van kwetsbaarheden via een *bug bounty*-platform, moet ook de volledige inhoud van het CVDP worden opgenomen op dat platform[50].

Het CVDP moet opgesteld zijn in alle talen van de website en voor zover mogelijk ook in het Engels. Het kan eveneens nuttig zijn om op andere locaties een link te plaatsen naar de pagina van het CVDP (bijvoorbeeld, in de hulprubriek van het programma, in de gebruiksaanwijzing, in de gebruikslicentie enz.).

Tot slot is het belangrijk dat de verantwoordelijke organisatie haar eventuele onderaannemers informeert over de inhoud van haar CVDP en dat ze haar onderaannemingscontracten indien nodig aanpast.

c. Contactpunt

De verantwoordelijke organisatie moet in haar beleid een contactpunt vermelden, waarnaar alle inlichtingen over kwetsbaarheden kunnen worden gestuurd. Hiervoor kan een specifiek e-mailadres worden gebruikt[51]. Ook moet de verantwoordelijke organisatie ervoor zorgen dat mails die binnenkomen op andere e-mailadressen[52] intern naar dit contactpunt worden doorgestuurd.

Het gebruik van een onlineformulier is ook interessant om informatie over ontdekte kwetsbaarheden te ontvangen. Deze werkwijze biedt het voordeel dat de invoering en verwerking van gegevens en de verzending van een ontvangstbevestiging automatisch kunnen gebeuren.

---

[48] Zie het project https://securitytxt.org/
[49] Zie bijvoorbeeld de extensie YesWeHack VDP Finder voor Chrome en Firefox.
[50] Bijvoorbeeld, www.intigriti.be; www.bountyfactory.io; www.yeswehack.com; www.bugcrowd.com; www.hackerone.com.
[51] Zoals bijvoorbeeld: vulnerabilitypolicy@organisation.com; security@organisation.com; csirt@organisation.com; support@organisation.com; security-alert@organisation.com, enz.
[52] Bijvoorbeeld: info@organisation.com of contact@organisation.com.

Bovendien kan het nuttig zijn de telefoongegevens van de dienst of persoon die bevoegd is voor de behandeling van meldingen over informaticakwetsbaarheden te vermelden.

Tot slot moet worden verduidelijkt welke inlichtingen de deelnemer moet verstrekken (zie hieronder deel II Procedure).

d. Veiligheid en vertrouwelijkheid van de communicatie

Dit is van cruciaal belang aangezien risico's op het lekken van informatie over kwetsbaarheden zoveel mogelijk moeten worden vermeden, door de vertrouwelijkheid en integriteit van de communicatie zo goed mogelijk te waarborgen.

Het is dus sterk aangewezen om een beveiligde communicatiemethode te gebruiken. Die kan bestaan in het gebruik van een middel voor het versleutelen van gegevens[53], het opzetten van een beveiligd internetportaal[54] of ten minste het beveiligen van de documenten met een paswoord[55]. Bij het uitwerken van de aan de deelnemers aanbevolen communicatiemodaliteiten moet de verantwoordelijke organisatie dus heel in het bijzonder rekening houden met de veiligheid ervan[56].

[53] Bijvoorbeeld: Transport Layer Security (TLS) of zijn voorganger Secure Sockets Layer (SSL), Secure Multipurpose Internet Mail Extensions (S/MIME) en Pretty Good Privacy (PGP).
[54] in HTTPS of via versleuteling in de webbrowser.
[55] Idealiter bezorgt de deelnemer het paswoord dan via een ander communicatiemiddel (telefoon, sms, berichtenapplicatie, ander e-mailadres, enz.) aan de verantwoordelijke organisatie.
[56] Bijvoorbeeld, de openbare sleutel en de fingerprint van haar contactpunt verstrekken om informatie versleuteld te verzenden, of haar onlineformulier in HTTPS beveiligen.

e. Beschrijving van de wederzijdse verplichtingen

1. Toepassingsgebied van het beleid

De verantwoordelijke organisatie moet het toepassingsgebied van haar beleid voor gecoördineerde bekendmaking uitdrukkelijk definiëren: op welke sites, producten, toestellen, diensten, systemen of netwerken is haar beleid van toepassing?

Idealiter moet de verantwoordelijke organisatie de regels van haar CVDP toepasbaar maken op haar verschillende informatiesystemen en op haar contractuele verbintenissen (leveranciers, klanten, onderaannemers, personeel, enz.).

Zo niet moet het CVDP informatiesystemen van derden die (bij gebrek aan toestemming van deze derden) worden uitgesloten van het toepassingsgebied van het beleid, uitdrukkelijk oplijsten. In geval van twijfel over de grenzen van het CVDP moet de deelnemer vooraf de goedkeuring van de verantwoordelijke organisatie vragen alvorens zijn onderzoek voort te zetten.

Het CVDP moet ook duidelijk vermelden dat het onderzoek van de deelnemer met betrekking tot informatiesystemen die niet uitdrukkelijk onder het beleid vallen, kan leiden tot de gerechtelijke vervolging van deze deelnemer (door het openbaar ministerie, de verantwoordelijke organisatie of derden buiten het CVDP).

2. Voorwaarden van het beleid

Het bestaan zelf van een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden of van een *bug bounty*-programma impliceert noodzakelijkerwijs dat een – minstens stilzwijgende – toegangsmachtiging tot het informaticasysteem werd verleend aan de deelnemer[57]. De deelnemer beschikt in principe eveneens over een machtiging om informaticagegevens in het betrokken systeem in te voeren of dit te proberen (zie *Gids - Deel II Wettelijke aspecten*).

[57] Het beleid voor de gecoördineerde bekendmaking van kwetsbaarheden zal bepalingen bevatten die, naargelang de exacte formulering ervan, als uitdrukkelijke of als stilzwijgende machtigingen kunnen worden beschouwd.

De verantwoordelijke organisatie moet in haar beleid voor gecoördineerde bekendmaking echter duidelijk vermelden onder welke voorwaarden deelnemers toegang kunnen krijgen tot het informaticasysteem, en kunnen proberen gegevens in te voeren of te wijzigen. De al dan niet toegestane acties moeten duidelijk worden vastgelegd, op basis van de beoogde doeleinden.

De machtiging om informaticagegevens te wijzigen of te schrappen[58] hangt af van de manier waarop het beleid voor de gecoördineerde bekendmaking van kwetsbaarheden is opgesteld. Bij het opstellen van dit beleid moet de verantwoordelijke organisatie de voordelen, de opgelegde specifieke voorwaarden en de risico's beoordelen om deze acties al dan niet toe te staan. Er moet worden vermeld dat de deelnemer de voorwaarden van het beleid omtrent het wijzigen en verwijderen van informaticagegevens strikt moet naleven. Zo niet maakt hij zich schuldig aan een misdrijf, namelijk een inbreuk in verband met informaticagegevens.

Zo is het bijvoorbeeld een goede praktijk om deelnemers te verbieden een beroep te doen op “Distributed Denial Of Service (DDoS)”-aanvallen of “social engineering”-aanvallen, malware of virussen te installeren, paswoorden te stelen, phishing- of spammails te sturen, gegevens/parameters van het systeem te verwijderen of te wijzigen, enz.

Het CVDP moet opzettelijke pogingen[59] om communicatie die niet toegankelijk is voor het publiek of elektronische communicatie te onderscheppen, op te nemen of er kennis van te nemen, uitdrukkelijk uitsluiten.[60] Niettemin kan worden toegestaan dat de inhoud van communicatie, op strikt toevallige wijze, aan deelnemers wordt onthuld in het kader van het opsporen van kwetsbaarheden.[61]

[58] Of om dergelijke acties te proberen.
[59] Wat verschilt van een toevallige onderschepping (zie Gids Deel II Wettelijke aspecten).
[60] Behalve in het eerder uitzonderlijke geval waarin de deelnemer over de toestemming van alle deelnemers beschikt of zelf aan de elektronische communicatie deelneemt.
[61] Zie de geheimhouding van elektronische communicatie (wet van 13 juni 2005).

Voorts moet worden vermeld dat de deelnemer geen communicatie die niet toegankelijk is voor het publiek, noch de gegevens van een informaticasysteem waarvan hij redelijkerwijs kan aannemen dat deze illegaal verkregen zijn, mag gebruiken, bijhouden, onthullen of bekendmaken.

Het moet voor de deelnemer ook verboden zijn om een toestel te installeren of te laten installeren dat het onderscheppen, kennisnemen of opnemen van communicatie die niet toegankelijk is voor het publiek, mogelijk maakt, behalve indien hij kan aantonen dat hij niet de bedoeling heeft het betrokken toestel te gebruiken voor voormelde doeleinden, hetzij met de toestemming van alle deelnemers aan de communicatie, hetzij door zelf aan de communicatie deel te nemen.

3. Melding

Het CVDP moet duidelijk vermelden welke inlichtingen de deelnemer moet verstrekken bij de melding van een kwetsbaarheid: soort kwetsbaarheid, configuratiedetails, verrichte handelingen, gebruikte tools, data van de tests, bewijzen, IP-adres of URL van het getroffen systeem, screenshot, contactgegevens, enz.

4. Evenredigheid

Over het algemeen moet de deelnemer zich ertoe verbinden om bij zijn acties het evenredigheidsbeginsel na te leven, d.w.z. de beschikbaarheid van de door het systeem geleverde diensten niet te verstoren en geen gebruik te maken van de kwetsbaarheid buiten wat strikt noodzakelijk is voor het aantonen van het beveiligingsprobleem. Zijn houding moet evenredig blijven: indien het probleem op kleine schaal is aangetoond, moet niet verder worden gegaan.

Indien het gebruik van persoonsgegevens door de deelnemer niet noodzakelijk is voor het aantonen van de informaticakwetsbaarheid, moet het uitdrukkelijk worden uitgesloten.

Bovendien moet het beleid voor gecoördineerde bekendmaking duidelijk vermelden dat de deelnemer de gegevens van de verantwoordelijke organisatie, waaronder eventuele persoonsgegevens, niet langer dan nodig mag bijhouden. Alle door de deelnemer ingezamelde persoonsgegevens moeten

onmiddellijk worden verwijderd. Indien het noodzakelijk blijkt om deze gegevens nog een bepaalde tijd bij te houden, moet de deelnemer erop toezien dat deze gegevens tijdens deze periode veilig worden bewaard.

5. Vertrouwelijkheid

Een van de essentiële elementen van een beleid voor gecoördineerde bekendmaking moet het in acht nemen van de vertrouwelijkheid zijn: de deelnemer mag de ingezamelde informatie niet delen met derden of verspreiden onder derden, zonder de uitdrukkelijke toestemming van de verantwoordelijke organisatie[62].

Ook moet elke onthulling van informatica-, communicatie- of persoonsgegevens aan personen buiten de verantwoordelijke organisatie of verspreiding van deze gegevens onder personen buiten de verantwoordelijke organisatie door de deelnemer uitdrukkelijk worden uitgesloten, behoudens voorafgaande toestemming van de verantwoordelijke organisatie.

De tekst van het beleid voor gecoördineerde bekendmaking moet vermelden dat het beleid niet tot doel heeft de opzettelijke kennisneming van de inhoud van informatica-, communicatie- of persoonsgegevens mogelijk te maken en dat een dergelijke kennisneming slechts toevallig en incidenteel kan plaatsvinden in het kader van het opsporen van kwetsbaarheden in de betrokken technologieën.

6. Uitvoering te goeder trouw

De organisatie die verantwoordelijk is voor het informatiesysteem moet zich ertoe verbinden haar beleid voor gecoördineerde bekendmaking te goeder trouw uit te voeren en de deelnemer die de voorwaarden ervan naleeft noch burgerrechtelijk noch strafrechtelijk te vervolgen.

[62] Opnieuw onder voorbehoud van een beperkte bekendmaking aan de overheden die bevoegd zijn inzake cybersecurity.

In hoofde van de deelnemer mag er geen sprake zijn 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. Dat geldt ook voor derde systemen in België of in het buitenland.

Wat betreft de instrumenten die een inbreuk in verband met informaticagegevens mogelijk maken, kan de deelnemer dergelijke instrumenten uitwerken, bezitten of ter beschikking stellen in het kader van de deelname aan een beleid voor de bekendmaking van kwetsbaarheden. Die acties zijn niet onwettig, zolang ze worden gerechtvaardigd door legitieme doeleinden met betrekking tot het opsporen van kwetsbaarheden met de toestemming van de organisatie van de verantwoordelijke van het betrokken informaticasysteem.

7. Verwerking van persoonsgegevens

Een CVDP heeft niet tot doel om intentioneel persoonsgegevens te verwerken. Het is echter wel mogelijk dat de deelnemer, zelfs toevallig, persoonsgegevens moet verwerken in het kader van zijn onderzoek naar kwetsbaarheden.

De verwerking van persoonsgegevens heeft een ruime betekenis en omvat met name het opslaan, wijzigen, opvragen, raadplegen, gebruiken of verstrekken van elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Het “identificeerbare” karakter van de persoon hangt niet af van de loutere wil tot identificatie van de gegevensverwerker, maar van de mogelijkheid om de persoon direct of indirect te identificeren aan de hand van deze gegevens (bijvoorbeeld: een e-mailadres, identificatienummer, online identificator, IP-adres of nog, locatiegegevens).

De verwerkingsverantwoordelijke is een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking vaststelt.[63]

[63] Art. 4, 7), van de AVG.

Aangezien het CVDP een vorm van toetredingsovereenkomst is die de ethische hacker ten aanzien van de verantwoordelijke organisatie bindt, moeten hierin de verplichtingen van de partijen inzake de verwerking van persoonsgegevens worden vermeld, met name het doel van en de essentiële middelen voor de eventuele verwerking in het kader van dit beleid (*zie Gids – Deel II Wettelijke aspecten).*

8. Proceduretermijnen

Er wordt aanbevolen voor elke fase van de procedure duidelijke termijnen te bepalen die moeten worden nageleefd, met name voor het versturen van een ontvangstbevestiging aan de deelnemer, het meedelen van bijkomende informatie, de onderzoeken, het ontwikkelen van een oplossing, het antwoord aan de deelnemer, de toekenning van een beloning of een eventuele publicatie. De termijnen moeten echter in zekere mate flexibel blijven, naargelang de complexiteit van de kwetsbaarheid, het aantal getroffen systemen, de dringendheid of de ernst van de situatie.

9. Doorlopende communicatie

Een goede samenwerking veronderstelt een doorlopende en efficiënte communicatie. De inlichtingen die door de deelnemer worden verstrekt, kunnen immers heel nuttig zijn om de kwetsbaarheid te identificeren en er een oplossing voor te vinden. Het is dus belangrijk ontvangstbevestigingen te sturen, de deelnemer op de hoogte te houden van het gevolg dat aan zijn melding wordt gegeven, hem te herinneren aan de inhoud van zijn verplichtingen en te preciseren wat de volgende stappen in de procedure te zijn.

Bovendien kan de tussenkomst van een coördinator (bij voorkeur aangewezen in het CVDP) of van een platform waarop beloningen voor het opsporen van kwetsbaarheden worden aangeboden, helpen om een constructieve relatie tussen de partijen tot stand te brengen en te behouden, of eventueel de anonimiteit van de deelnemer waarborgen.

Indien een van de partijen of de aangewezen coördinator niet reageren, kunnen de partijen steeds een beroep doen op het Centrum voor Cybersecurity België (vulnerabilityreport@cert.be).

10. Toekenning van een beloning

De toekenning van een beloning of van een publieke erkenning[64] door de verantwoordelijke organisatie maakt het CVDP aantrekkelijker voor de deelnemers en leidt vaak tot betere resultaten voor de organisatie. Het kan zelfs om een louter symbolisch geschenk gaan: bijvoorbeeld een T-shirt, een sticker of een speciale tas.

In het kader van een beloningsprogramma voor het opsporen van kwetsbaarheden (of *bug bounty*-programma) is de beloning afhankelijk van de hoeveelheid, het belang of de kwaliteit van de overgemaakte informatie.

Het is essentieel dat de verantwoordelijke organisatie de aard van deze beloning vooraf duidelijk vermeldt in haar beleid. Elk verzoek om een beloning buiten de door het CVDP bepaalde voorwaarden kan dan worden gelijkgesteld met een illegale poging tot afpersing.

De organisatie kan gebruikmaken van een *bug bounty*-platform[65], dat samen met haar de technische en administratieve aspecten van haar beloningsprogramma zal coördineren.

[64] Rangschikking onder de beste deelnemers, publicatie, conferentie, enz.
[65] Bijvoorbeeld: www.intigriti.com (platform gevestigd in België); www.yeswehack.com (platform gevestigd in Frankrijk); www.yogosha.com; www.hackerone.com (platform gevestigd in de VS).

11. Eventuele openbare bekendmaking

De eventuele bekendmaking van de kwetsbaarheid moet gecoördineerd en gesynchroniseerd gebeuren tussen de partijen, om de verantwoordelijke organisatie voldoende tijd te geven om het probleem op te lossen en de getroffen kritieke aanbieders vooraf te informeren.

In geval van een kwetsbaarheid die nog niet gekend is en die elders een rechtstreekse of onrechtstreekse impact dreigt te hebben, moet de verantwoordelijke organisatie het Centrum voor Cybersecurity België (vulnerabilityreport@cert.be) en de andere mogelijk betrokken organisaties vooraf op de hoogte brengen, zelfs indien ze niet wil dat de kwetsbaarheid openbaar wordt gemaakt.

Wanneer een kwetsbaarheid wordt geïdentificeerd in een programma, een component, een protocol of een format verstrekt door een derde leverancier, moet de verantwoordelijke organisatie deze hiervan rechtstreeks op de hoogte brengen, voor enige openbare bekendmaking.

Hetzelfde geldt wanneer de geïdentificeerde kwetsbaarheid andere organisaties die gebruikmaken van een gelijkaardige technologie, in ruimere zin dreigt te treffen, of wanneer de getroffen IT-component door de verantwoordelijke organisatie aan andere organisaties wordt verstrekt (bijvoorbeeld via gebruikerslicenties). In deze gevallen is het onontbeerlijk dat een verslag over de kwetsbaarheid en de oplossing ervoor aan de betrokken partijen wordt bezorgd, zodat zij zich kunnen beschermen.

In geval van openbare bekendmaking moeten het verslag over de kwetsbaarheid en de oplossing idealiter tegelijkertijd worden bekendgemaakt.

De verantwoordelijke organisatie moet verschillende middelen aanbieden om haar gebruikers te informeren en te beschermen: bijvoorbeeld, automatische systeemupdate, publicatie van beveiligingsberichten op haar website, mailings met een link naar een specifieke internetpagina, verspreiding van deze informatie onder haar netwerk van verkopers, enz.

** tech-support-concept. Free licence. Designed by macrovector / Freepik (2020)*

II. Procedure

a. Ontdekking

Wanneer een deelnemer informatie over een potentiële kwetsbaarheid ontdekt, moet hij voor zover mogelijk vooraf controles uitvoeren om het bestaan van de kwetsbaarheid te bevestigen en de eventuele risico's te identificeren.

Vervolgens moet hij de verantwoordelijke organisatie minstens voldoende technische informatie bezorgen om het bestaan van dit probleem te kunnen bevestigen en zijn contactgegevens verschaffen. Deze elementen kunnen worden aangevuld naargelang de specificaties van het beleid voor gecoördineerde bekendmaking of van de inhoud van het onlineformulier van de verantwoordelijke organisatie.

b. Melding

De deelnemer moet de technische informatie zo snel mogelijk bezorgen aan het contactpunt of aan de door de verantwoordelijke organisatie aangewezen coördinator, via beveiligde communicatiemiddelen.

Wanneer de verantwoordelijke organisatie een melding ontvangt, moet ze de deelnemer zo snel mogelijk een ontvangstbevestiging sturen, met vermelding van de interne referentie en de volgende fase van de procedure.

Samen met deze ontvangstbevestiging kan de verantwoordelijke organisatie wijzen op de inhoud van haar beleid voor gecoördineerde bekendmaking, of op zijn minst een link hiernaar bezorgen, en eventuele bijkomende informatie vragen.

Het is met name interessant om te vragen of de deelnemer dit probleem al aan andere verantwoordelijke organisaties heeft gemeld.

c. Onderzoek

Tijdens de onderzoeksfase kan de verantwoordelijke organisatie de omgeving en het gesignaleerde gedrag reproduceren om de meegedeelde informatie te controleren.

De deelnemer moet regelmatig op de hoogte worden gebracht van de resultaten van het onderzoek en van het gevolg dat aan de melding wordt gegeven.

Tijdens deze procedure moeten de partijen de link leggen met gelijkaardige of aanverwante veiligheidsverslagen, het risico en de ernst van de kwetsbaarheid beoordelen en eventuele andere getroffen producten of systemen identificeren.

d. Toepassing van een oplossing

Het bekendmakingsbeleid heeft tot doel de ontwikkeling en toepassing van een oplossing mogelijk te maken om de kwetsbaarheid van het informaticasysteem weg te werken.

Het staat de verantwoordelijke organisatie vrij al dan niet een oplossing te ontwikkelen en toe te passen, behalve indien ze daar wettelijk of contractueel toe verplicht is.

Indien ervoor gekozen wordt om een aangetoond beveiligingsprobleem niet op te lossen, kan de verantwoordelijke organisatie in voorkomend geval natuurlijk burgerlijk aansprakelijk worden gesteld, mocht een derde hierdoor schade ondervinden[66].

Voor zover mogelijk moet de oplossing uiterlijk binnen de 90 kalenderdagen worden ontwikkeld.

Deze termijnen moeten tot het strikte minimum worden beperkt indien de gebruikers van de getroffen systemen in gevaar zijn of indien er risico's bestaan voor de bescherming van persoonsgegevens. Indien de organisatie niet in staat is het probleem onmiddellijk op te lossen, moet het betrokken informaticasysteem in dat geval tijdelijk volledig buiten werking worden gesteld.

Door de bevoorradingsketen (*supply chain*) en de vele onderlinge afhankelijkheden tussen de informatiesystemen kan de termijn die nodig is voor het ontwikkelen en toepassen van een oplossing, echter langer zijn.

Tijdens deze fase moet de verantwoordelijke organisatie (of haar dienstverlener) enerzijds positieve testen uitvoeren om te controleren of de oplossing correct werkt en anderzijds negatieve testen om er zeker van te zijn dat de oplossing de goede werking van andere bestaande functionaliteiten niet verstoort.

[66] Onafhankelijk zelfs van het bestaan van een beleid voor verantwoorde bekendmaking.

Wanneer de oplossing klaar is en de kwetsbaarheid die ook andere organisaties zou treffen, moet die prioritair en vóór elke openbare bekendmaking worden overgemaakt aan het CCB (vulnerabilityreport@cert.be).

De verantwoordelijke organisatie moet vanaf deze overdracht een redelijke termijn naleven vóór een eventuele algemene bekendmaking aan de gebruikers, om aanbieders van essentieel belang (NIS-aanbieders van essentiële diensten, kritieke infrastructuren, overheidsinstellingen, enz.) de mogelijkheid te bieden de oplossing prioritair te implementeren.

e. Eventuele openbare bekendmaking

Behoudens een bijzondere wettelijke verplichting is de openbare bekendmaking van een kwetsbaarheid geen verplichte fase van een CVDP. De deelnemer en de verantwoordelijke organisatie kunnen immers beslissen om het bestaan van de kwetsbaarheid niet openbaar te maken. Dat kan het geval zijn indien de kwetsbaarheid te moeilijk of onmogelijk op te lossen is, of indien de oplossing ervan buitensporige kosten zou meebrengen in vergelijking met de eventuele risico's.

Dit moet echter de uitzondering blijven, aangezien een CVDP tot doel heeft de beveiliging en de transparantie ten opzichte van de gebruikers te verbeteren. Sommige wettelijke bepalingen verplichten de verantwoordelijke organisatie overigens om de gebruikers van de informatiesystemen[67] of de natuurlijke personen die betrokken zijn bij een inbreuk in verband met persoonsgegevens[68], te informeren.

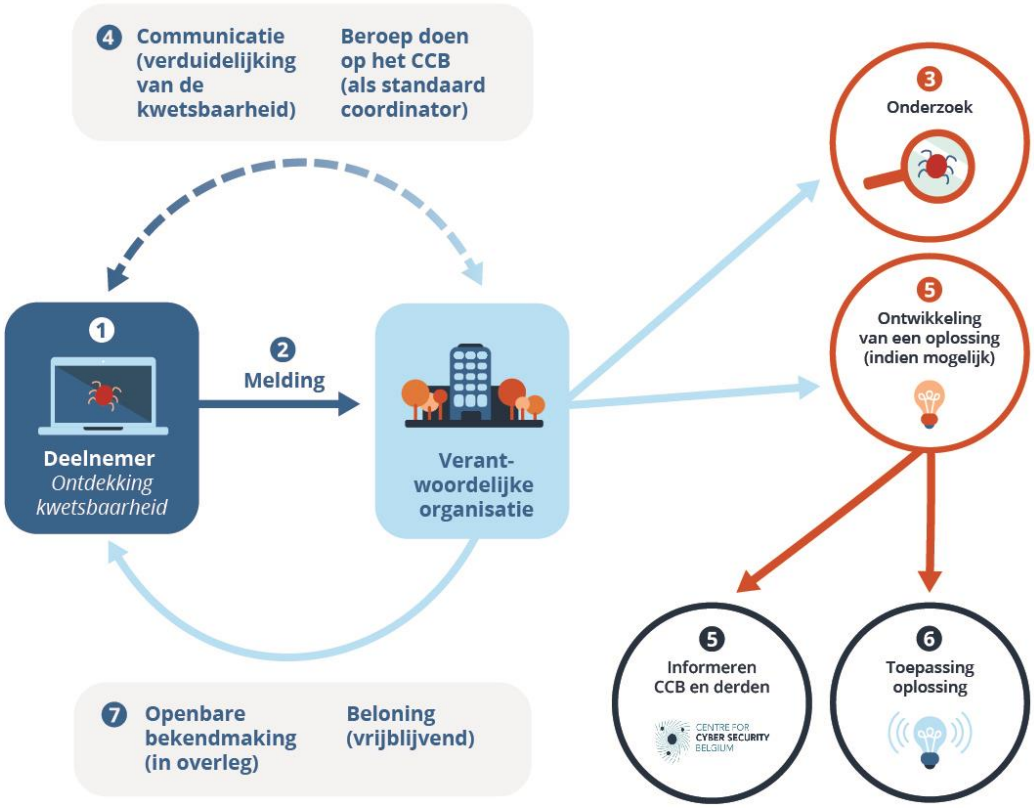
In elk geval moet de informatie met betrekking tot een kwetsbaarheid die ook andere organisaties zou treffen op zijn minst aan het CCB (vulnerabilityreport@cert.be) worden overgemaakt.

[67] Zie met name de regels inzake contractuele en buitencontractuele aansprakelijkheid.
[68] Art. 34 van de AVG.

Indien de kwetsbaarheid openbaar wordt gemaakt, legt de verantwoordelijke organisatie, in overleg met de deelnemer, de modaliteiten van de bekendmaking vast. Idealiter wordt de informatie over de kwetsbaarheid tegelijkertijd met de oplossing bekendgemaakt. De verantwoordelijke organisatie wordt aanbevolen haar klanten te informeren door een beveiligingsbericht op haar website te plaatsen of via andere communicatiemiddelen (e-mail, infobrief, systeemupdate, enz.).

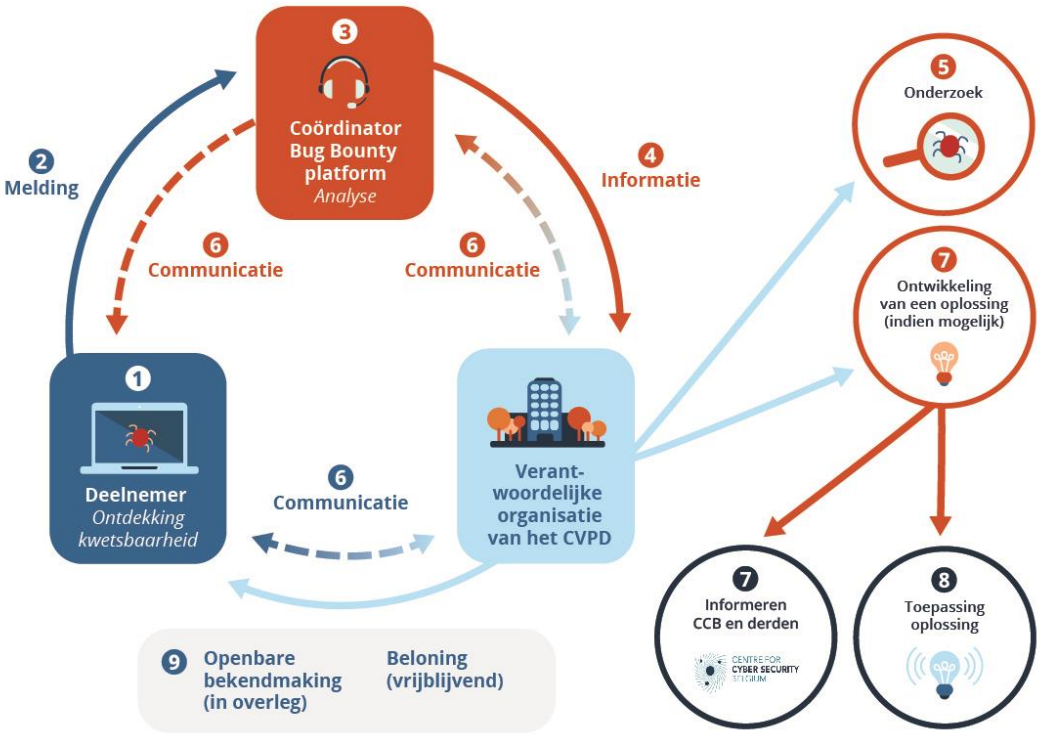
Tevens moet de verantwoordelijke organisatie andere organisaties die waarschijnlijk ook bij dezelfde kwetsbaarheid zijn betrokken, inlichten. De eventuele onderlinge afhankelijkheid van de informatiesystemen of de bevoorradingsketen kunnen leiden tot een bredere coördinatie van de eventuele bekendmaking.

Het is ook belangrijk om opmerkingen van gebruikers over de toepassing van de oplossing te verzamelen en de nodige corrigerende maatregelen te nemen om eventuele problemen veroorzaakt door de oplossing te regelen, met name inzake compatibiliteit met andere producten of diensten.



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.

** Designed by CCB and Intigriti - 2020*



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. 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. 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.

** Designed by CCB and Intigriti - 2020*

CENTRE FOR CYBER SECURITY BELGIUM

D. REFERENTIES

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

CENTRE FOR EUROPEAN POLICY STUDIES (CEPS), *Software vulnerability disclosure in Europe. Technology, Policies and Legal Challenges, Report of a CEPS Task Force, 2018,* www.ceps.eu/ceps-publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges

GLOBAL CONFERENCE CYBER SPACE, *Best practice guide Responsible Disclosure*, 2015, www.gccs2015.com/sites/default/files/documents/BestPracticeRD-20150409_0.pdf

INTERNET ENGINEERING TASK FORCE (IETF) - CHRISTEY S. & WYSOPAL C., *Responsible Vulnerability Disclosure Process*, 2002, https://tools.ietf.org/html/draft-christey-wysopal-vuln-disclosure-00 (www.circl.lu/pub/responsible-vulnerability-disclosure)

ORGANIZATION FOR INTERNET SAFETY, *Guidelines for responsible disclosure*, 2004, www.symantec.com/security/OIS_Guidelines%20for%20responsible%20disclosure.pdf

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)

CENTRE FOR CYBER SECURITY BELGIUM

GIDS OVER HET BELEID VOOR DE GECOÖRDINEERDE BEKENDMAKING VAN KWETSBAARHEDEN
DEEL I: GOEDE PRAKTIJKEN

Dit document en de bijlagen werden opgesteld door het Centrum voor Cybersecurity België (CCB). Deze federale overheidsinstelling werd opgericht bij het koninklijk besluit van 10 oktober 2014 en staat onder het gezag van de Eerste Minister.

Het CCB wijst alle aansprakelijkheid in verband met de inhoud van dit document af.

De vermelde informatie:
• is louter algemeen van aard en heeft niet tot doel alle specifieke situaties te behandelen;
• is niet noodzakelijk op alle vlakken volledig, nauwkeurig of up-to-date.

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

Wettelijk depot:

D/2020/14828/014

2020