



CENTRE FOR
CYBER SECURITY
BELGIUM

GIDS OVER HET BELEID VOOR DE GECOÖRDINEERDE BEKENDMAKING VAN KWETSBAARHEDEN

DEEL I: GOEDE PRAKTIJEN

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

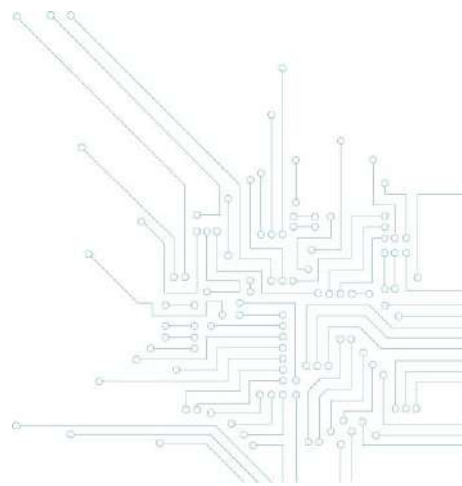


.be

UNDER THE AUTHORITY
OF THE PRIME MINISTER

A. INHOUDSOPGAVE

B. INLEIDING	4
<i>I. Achtergrond.....</i>	<i>4</i>
<i>II. Begrippen</i>	<i>4</i>
<i>III. Doelstellingen.....</i>	<i>7</i>
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>I. Inhoud van een CVDP</i>	<i>19</i>
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
<i>II. Procedure</i>	<i>30</i>
a. Ontdekking.....	30
b. Melding	31
c. Onderzoek.....	31
d. Toepassing van een oplossing.....	32
e. Eventuele openbare bekendmaking	33
D. REFERENTIES	37



Waarschuwing:

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

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.

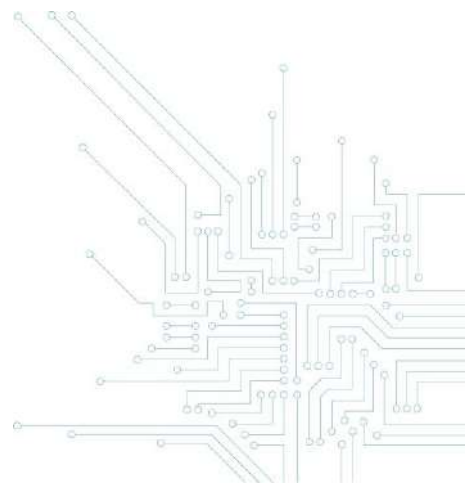
Wat de oorzaken van deze incidenten betreft, vormt het bestaan van kwetsbaarheden een groot risico. Dit risico is evenwel inherent aan het ontwikkelings-, gebruiks- en updateproces van deze systemen. Rekening houdend met de omvang en techniciteit van dit probleem lijkt het een illusie te geloven dat 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 kwetsbaarheden¹ (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 deelnemers² (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 kwetsbaarheid³ is een gebrek of een zwakke plek, een ontwerp⁴- of uitvoeringsfout⁵, het ontbreken van updates in het licht van de bestaande technische kennis, die de veiligheid van informatietechnologieën⁶ 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 systeem⁷ 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”).

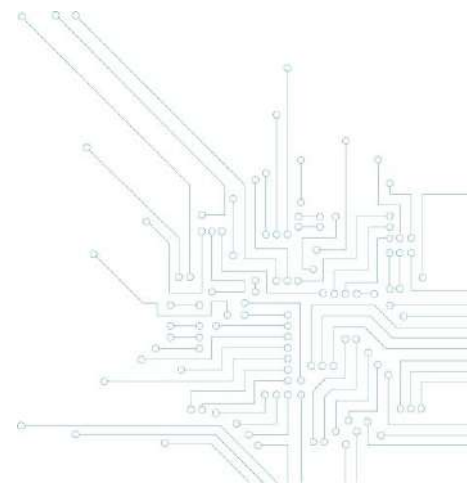
³ EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA), *Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations*, 2015, p. 14, punt 2.2, www.enisa.europa.eu/publications/vulnerability-disclosure.

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 CVDP⁸ (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 systeem⁹. 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 vervullen¹⁰ 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.

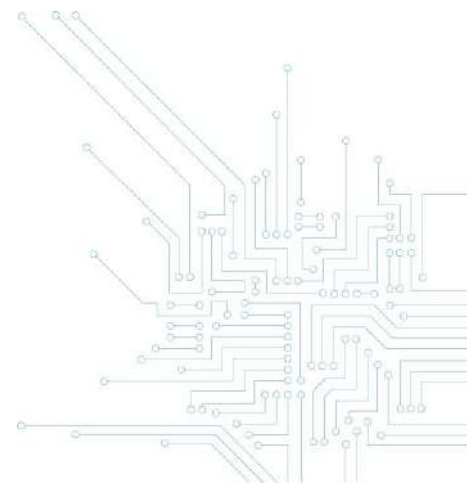
F. Een beloningsprogramma voor het opsporen van kwetsbaarheden (of bug bounty-programma)¹¹ heeft betrekking op alle regels die een verantwoordelijke organisatie heeft bepaald om beloningen toe te kennen aan deelnemers die kwetsbaarheden identificeren in de door haar gebruikte technologieën. Deze beloning 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).

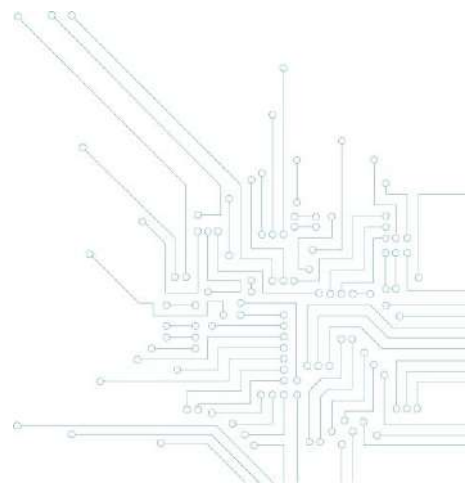
III. Doelstellingen

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 voorwaarden¹².

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.

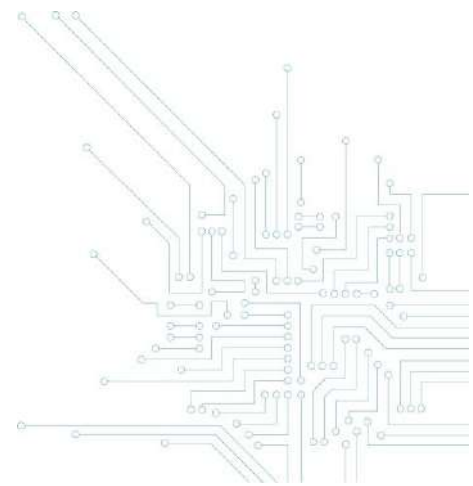
De invoering van een dergelijk beleid verduidelijkt de juridische situatie van de deelnemers. Ze kunnen immers aantonen dat ze over een voorafgaande toegangsmachtiging tot de betrokken informaticasystemen beschikken en dus niet ongeoorloofd binnendringen in die systemen, mits de in het beleid vermelde 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*-programma¹³).

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.

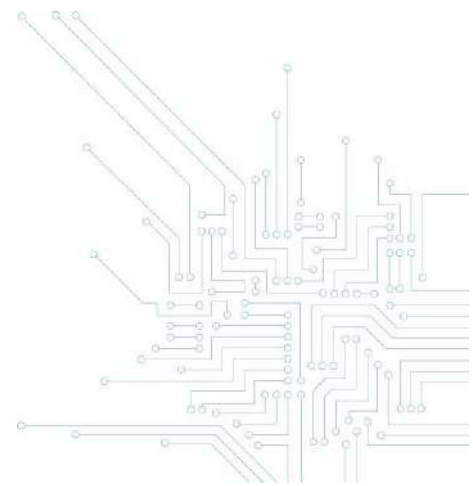
b. Informatiesystemen beter beveiligen en onderzoek aanmoedigen

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 experts 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

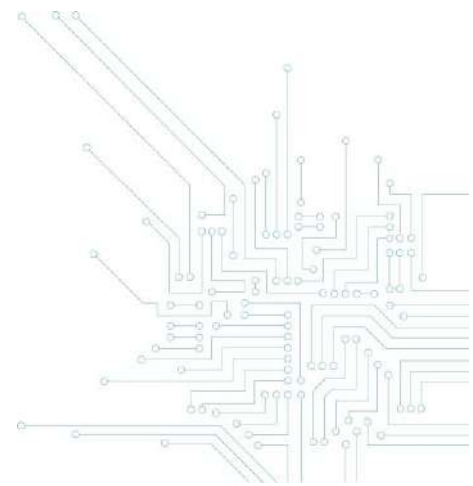
De uitvoering van een CVDP toont het publiek en de gebruikers dat de verantwoordelijke organisatie veel waarde hecht aan de veiligheid van haar informatietechnologieën.

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 kwetsbaarheid¹⁵, 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 informatiesystemen¹⁶ 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.

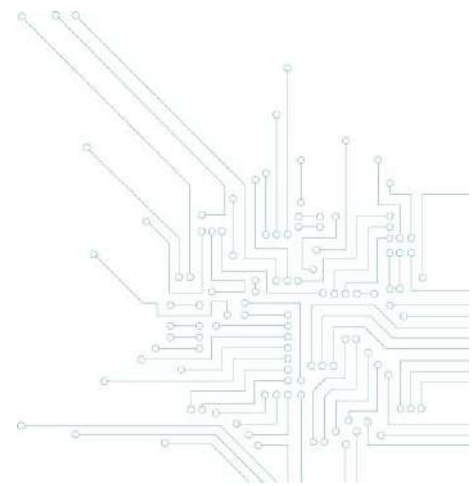
Bovendien kan de verspreiding of beschikbaarstelling aan het publiek van informaticagegevens, zoals software of instructies, die het mogelijk maken om door de beveiliging van informaticasystemen te breken, een misdrijf zijn¹⁷ of diegene die de informatie heeft bekendgemaakt burgerlijk aansprakelijk stellen¹⁸ (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, digitaal dienstverleners, 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).

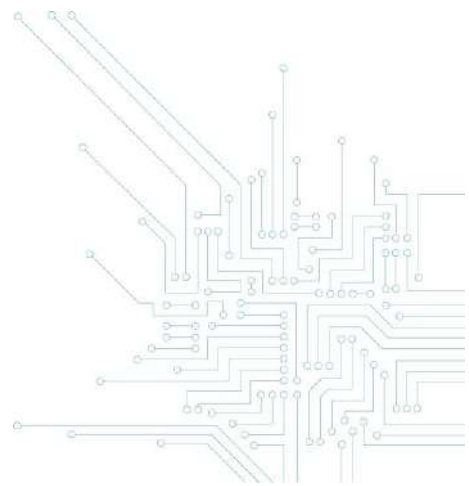
Het kan ook heel nuttig blijken om, wanneer de belangrijkste veiligheidsrisico's zijn weggewerkt, informatie over de ontdekte kwetsbaarheden en de oplossing ervan bekend te maken, in een passend kader¹⁹, om het onderzoek inzake informaticabeveiliging vooruit te helpen.

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).

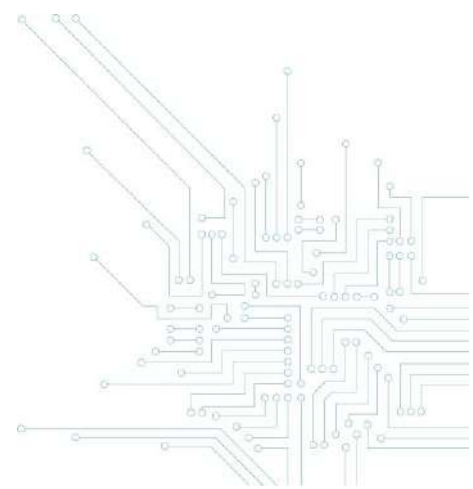
De bepaling verduidelijkt dat de verwerkingsverantwoordelijke en de verwerker met name een beroep kunnen doen op:

- a) de pseudonimisering en versleuteling van persoonsgegevens;
- b) het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingsystemen 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 verbeteren²⁰.

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 garanderen²² en anderzijds regelmatig de doeltreffendheid van de maatregelen ter beveiliging van de verwerking te testen, te beoordelen en te evalueren²³. 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 29147²⁴ en 30111²⁵).

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%2000_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 autoriteit²⁶ of een natuurlijke persoon²⁷ 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”.

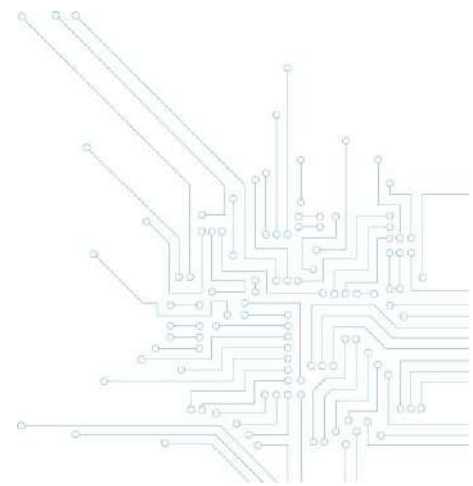
De AED moet ook “passende maatregelen [nemen] om incidenten die de beveiliging van de voor de verlening van die essentiële diensten gebruikte netwerk- en informatiesystemen aantasten, te voorkomen of de gevolgen ervan te minimaliseren, teneinde de continuïteit van deze diensten te waarborgen”²⁸.

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 digitaal dienstverleners (DDV's) – bijvoorbeeld aanbieders van cloudcomputerdiensten.



worden aangeboden of toegankelijk zijn, in gevaar brengen²⁹. Om de nodige maatregelen te nemen die in verhouding staan tot de risico's³⁰, 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 digitaalendienstverlener 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-producten³², -diensten³³ en -processen³⁴ 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.

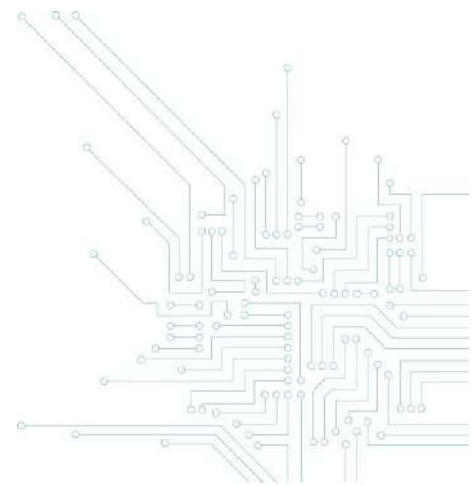
³² Een element of groep elementen van een netwerk- of informatiesysteem (art. 2, 12, van de Cyberbeveiligingsverordening).

³³ Een dienst die volledig of hoofdzakelijk bestaat in de verzending, opslag, opraging 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 29147⁴¹ en ISO/IEC 30111⁴². 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>).

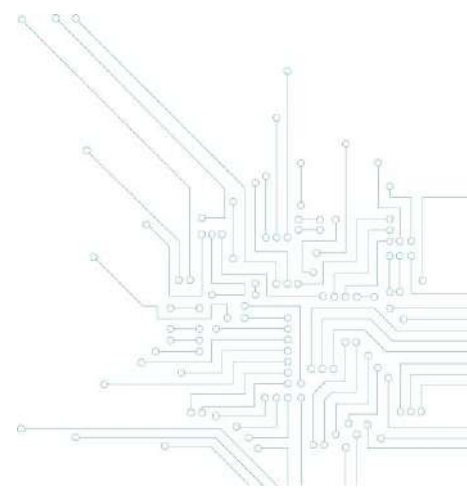
⁴² ISO/IEC 30111:2019 Information technology — Security techniques — Vulnerability handling processes (<https://www.iso.org/standard/53231.html>).

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.



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 is⁴⁴. 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 uitrusting⁴⁵.

b. Openbaarheid

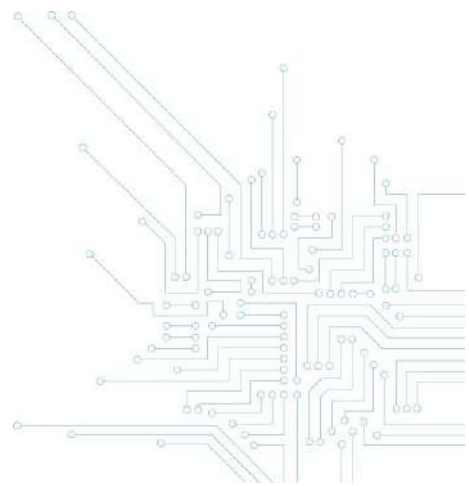
De openbaarheid die aan het beleid voor verantwoorde bekendmaking wordt gegeven, is een belangrijk element voor het succes ervan⁴⁶. De inhoud ervan moet dus gemakkelijk toegankelijk zijn voor potentiële deelnemers, bij voorkeur op de website van de verantwoordelijke organisatie. Het bestaan van het CVDP 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 /vulnerability-policy](https://www.[organisatie].be/security of /disclosurepolicy of /vulnerability-policy).



boomstructuur van iedere website⁴⁸ of extensies voor webbrowsers om websites die over een CVDP beschikken op te sporen⁴⁹.

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 platform⁵⁰.

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 gebruikt⁵¹. Ook moet de verantwoordelijke organisatie ervoor zorgen dat mails die binnenkomen op andere e-mailadressen⁵² 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.

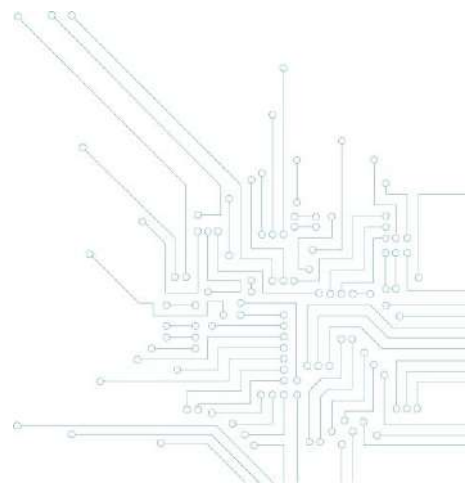
⁴⁸ Zie het project <https://securitytxt.org/>

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.

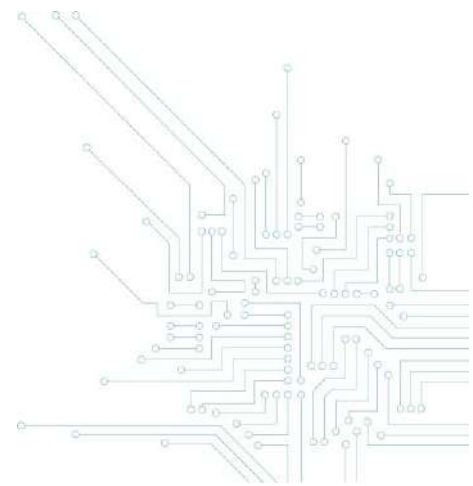
Het is dus sterk aangewezen om een beveiligde communicatiemethode te gebruiken. Die kan bestaan in het gebruik van een middel voor het versleutelen van gegevens⁵³, het opzetten van een beveiligd internetportaal⁵⁴ of ten minste het beveiligen van de documenten met een wachtwoord⁵⁵. Bij het uitwerken van de aan de deelnemers aanbevolen communicatiemodaliteiten moet de verantwoordelijke organisatie dus heel in het bijzonder rekening houden met de veiligheid ervan⁵⁶.

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 wachtwoord 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.).

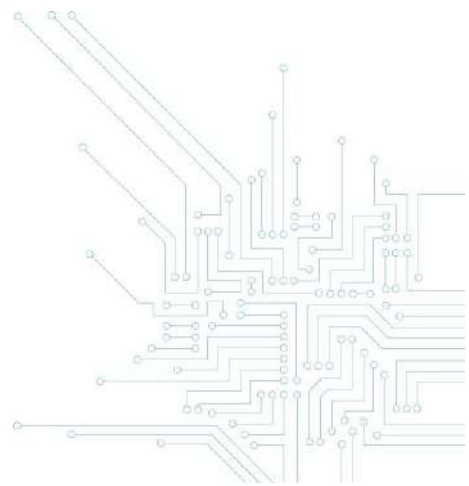
Zo niet moet het CVDP informatiesystemen van derden die (bij gebrek aan toestemming van deze derden) worden uitgesloten van het toepassingsgebied van het beleid, uitdrukkelijk oplijsten. In geval van twijfel over de grenzen van het CVDP moet de deelnemer vooraf de goedkeuring van de verantwoordelijke 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 deelnemer⁵⁷. 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 schrappen⁵⁸ 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.

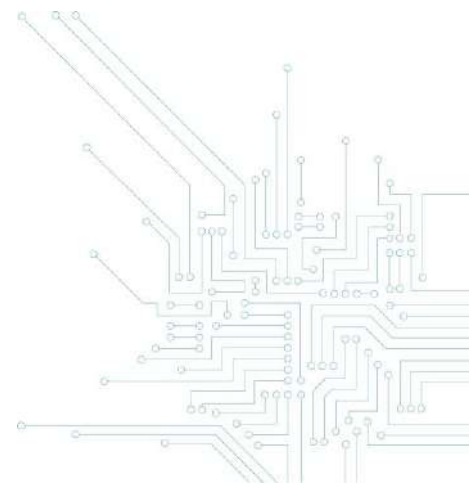
Het CVDP moet opzettelijke pogingen⁵⁹ om communicatie die niet toegankelijk is voor het publiek of elektronische communicatie te onderscheppen, op te nemen of er kennis van te nemen, uitdrukkelijk uitsluiten.⁶⁰ Niettemin kan worden toegestaan dat de inhoud van communicatie, op strikt toevallige wijze, 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, kennismaken 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

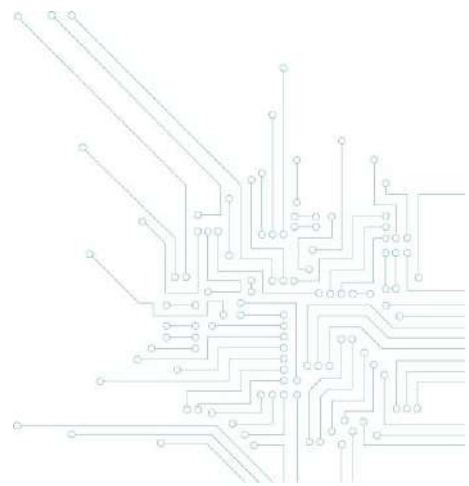
Het CVDP moet duidelijk vermelden welke inlichtingen de deelnemer moet verstrekken bij de melding van een kwetsbaarheid: soort kwetsbaarheid, configuratiedetails, verrichte handelingen, gebruikte tools, data van de tests, bewijzen, IP-adres of URL van het getroffen systeem, screenshot, contactgegevens, 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 organisatie⁶².

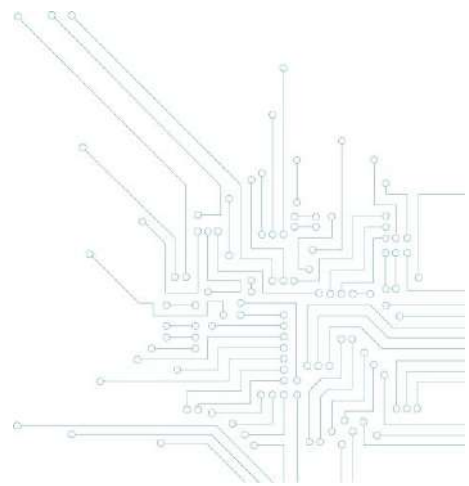
Ook moet elke onthulling van informatica-, communicatie- of persoonsgegevens aan personen buiten de verantwoordelijke organisatie of verspreiding van deze gegevens onder personen buiten de verantwoordelijke organisatie door de deelnemer uitdrukkelijk worden uitgesloten, behoudens voorafgaande toestemming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

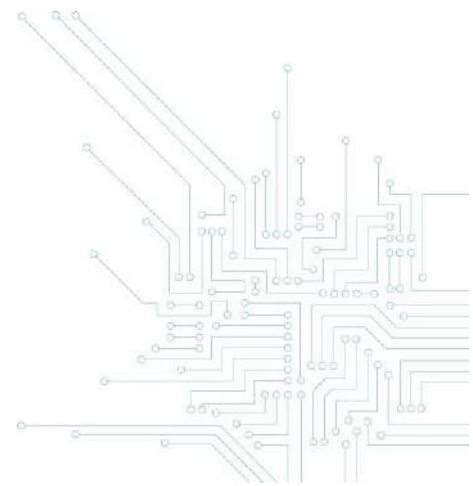
7. Verwerking van persoonsgegevens

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 identifier, 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*).

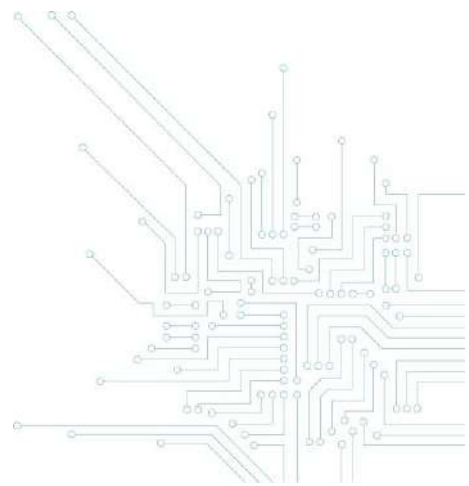
8. Proceduretermijnen

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 erkenning⁶⁴ 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.

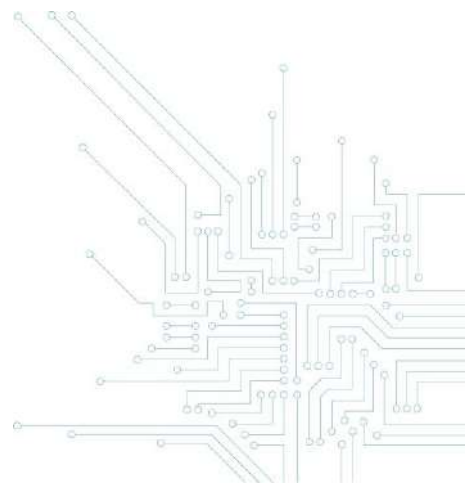
In het kader van een beloningsprogramma voor het opsporen van kwetsbaarheden (of *bug bounty*-programma) is de beloning afhankelijk van de hoeveelheid, het belang of de kwaliteit van de overgemaakte informatie.

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*-platform⁶⁵, 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.

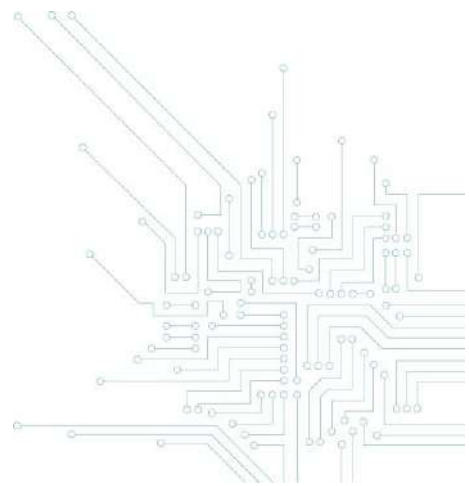
In geval van een kwetsbaarheid die nog niet gekend is en die elders een rechtstreekse of onrechtstreekse impact dreigt te hebben, moet de verantwoordelijke organisatie het Centrum voor Cybersecurity België (vulnerabilityreport@cert.be) en de andere mogelijk betrokken organisaties vooraf op de hoogte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



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.

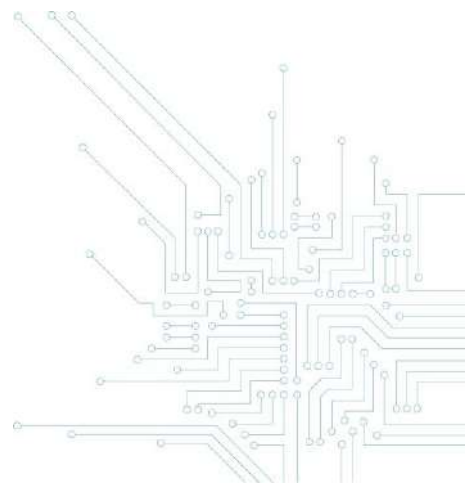
Het is met name interessant om te vragen of de deelnemer dit probleem al aan andere verantwoordelijke organisaties heeft gemeld.

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 ondervinden⁶⁶.

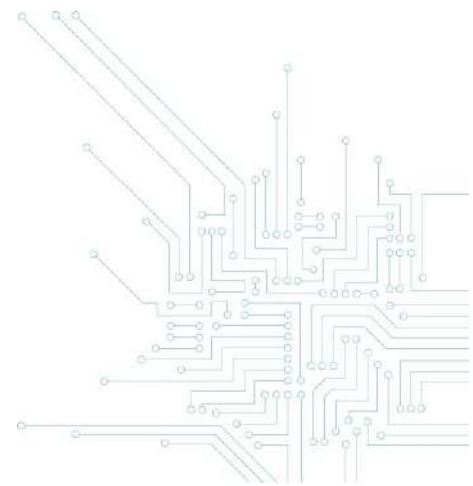
Voor zover mogelijk moet de oplossing uiterlijk binnen de 90 kalenderdagen worden ontwikkeld.

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

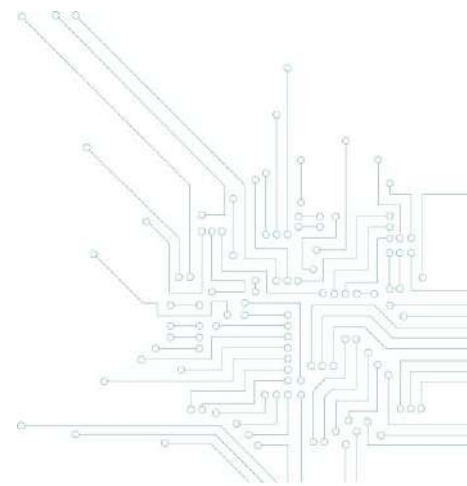
Behoudens een bijzondere wettelijke verplichting is de openbare bekendmaking van een kwetsbaarheid geen verplichte fase van een CVDP. De deelnemer en de verantwoordelijke organisatie kunnen immers beslissen om het bestaan van de kwetsbaarheid niet openbaar te maken. Dat kan het geval zijn indien de kwetsbaarheid 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 informatiesystemen⁶⁷ of de natuurlijke personen die betrokken zijn bij een inbreuk in verband met persoonsgegevens⁶⁸, 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.

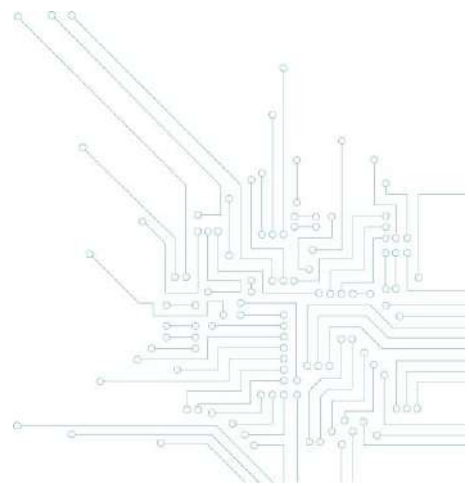
⁶⁸ Art. 34 van de AVG.

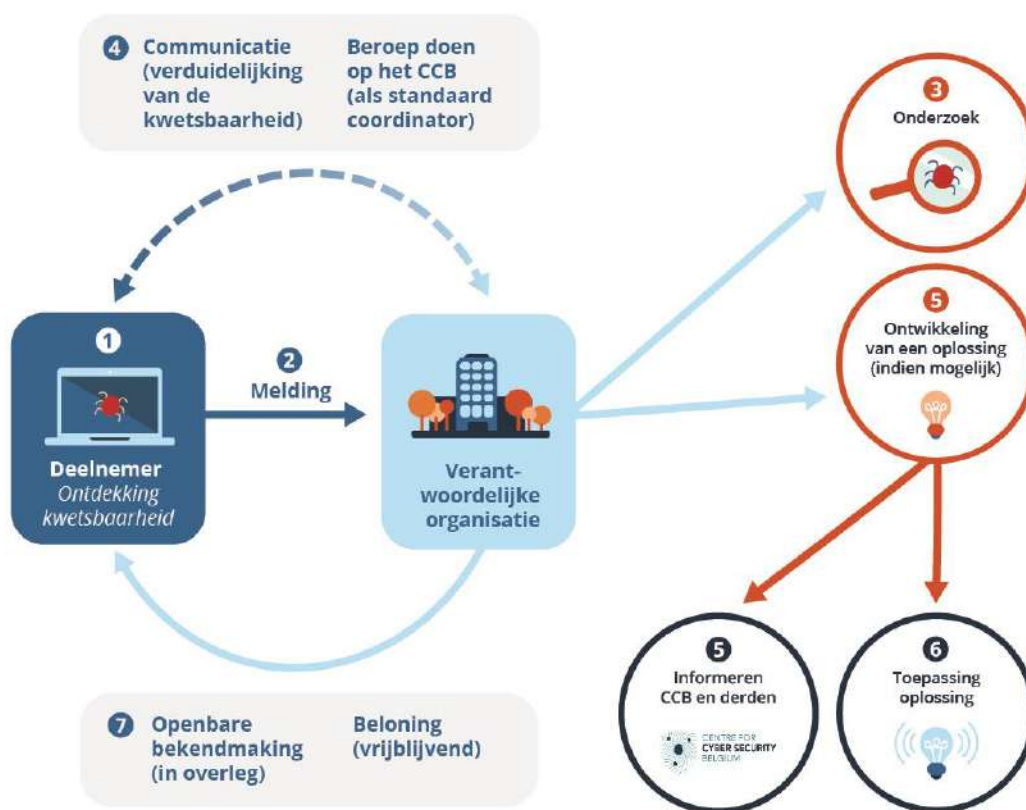


Indien de kwetsbaarheid openbaar wordt gemaakt, legt de verantwoordelijke organisatie, in overleg met de deelnemer, de modaliteiten van de bekendmaking vast. Idealiter wordt de informatie over de kwetsbaarheid tegelijkertijd met de oplossing bekendgemaakt. De verantwoordelijke organisatie wordt aanbevolen 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.

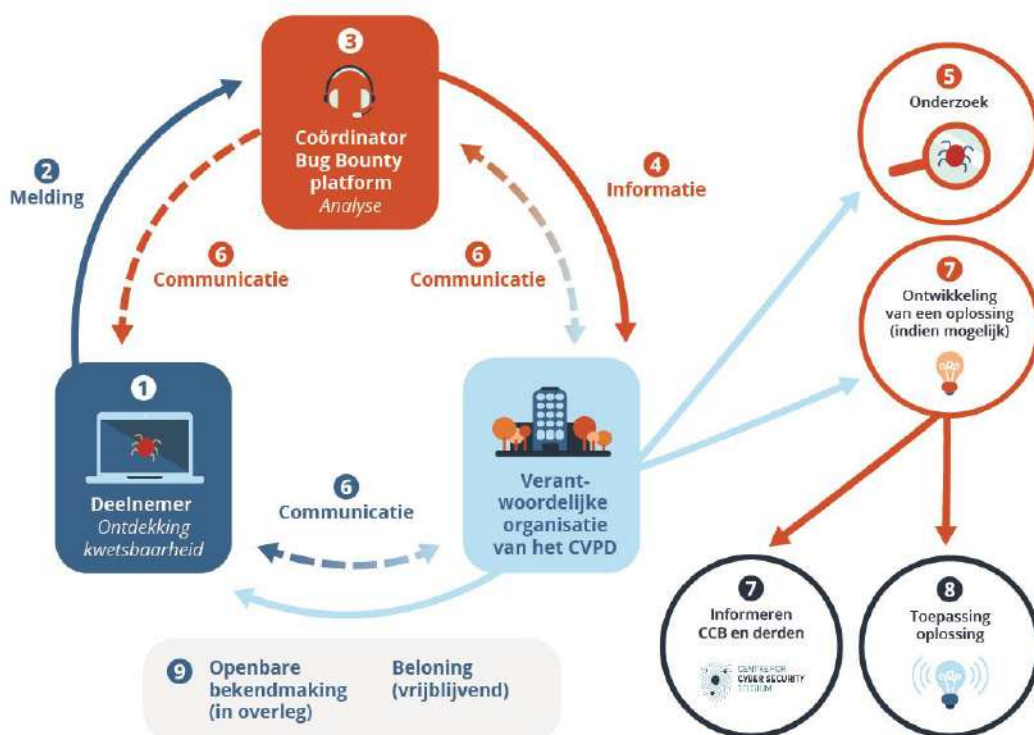
Het is ook belangrijk om opmerkingen van gebruikers over de toepassing van de oplossing te verzamelen en de nodige corrigerende maatregelen te nemen om eventuele problemen veroorzaakt door de oplossing te regelen, met name inzake compatibiliteit met andere producten of diensten.





- 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 kwetsbaarheid kan onderling overlegd worden en een beloning uitreiken kan op basis van de CVDP-voorwaarden.

* Designed by CCB and Intigrity - 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 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 kwetsbaarheid kan onderling overlegd worden en een beloning uitreiken kan op basis van de CVDP-voorwaarden.

* Designed by CCB and Intigrity - 2020

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 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

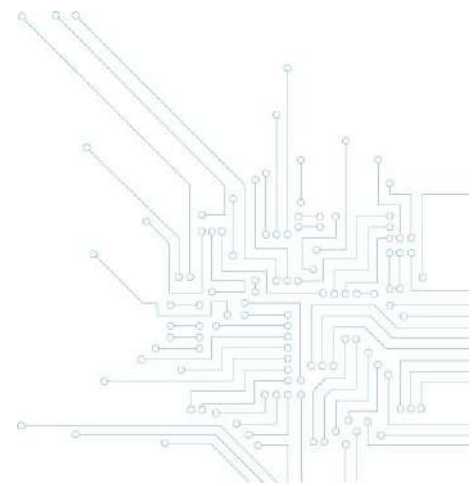
SOFTWARE ENGINEERING INSTITUTE, *The CERT Guide to Coordinated Vulnerability Disclosure*, 2013 (updated in 2019) <https://vuls.cert.org/confluence/display/CVD>

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](http://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>)



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.

Alle teksten, lay-out, ontwerpen en overige elementen van welke aard ook in dit document zijn onderworpen aan de wetgeving op de auteursrechten. Uittreksels uit dit document mogen alleen voor niet-commerciële doeleinden en met bronvermelding worden gereproduceerd.

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.

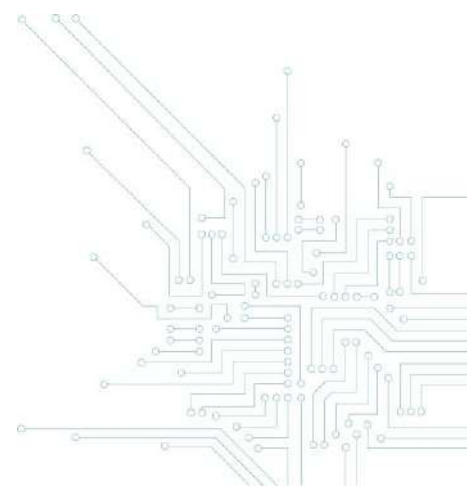
Verantwoordelijke uitgever:
Centrum voor Cybersecurity België

M. De Bruycker, Directeur
Wetstraat 16
1000 Brussel

Wettelijk depot:

D/2020/14828/014

2020





CENTRE FOR
CYBER SECURITY
BELGIUM

GIDS OVER HET BELEID VOOR DE GECOÖRDINEERDE BEKENDMAKING VAN KWETSBAARHEDEN

DEEL II: WETTELIJKE ASPECTEN

COORDINATED VULNERABILITY DISCLOSURE POLICIES - “CVDP”
RESPONSIBLE DISCLOSURE POLICIES - “RDP”

CENTRUM VOOR
CYBERSECURITY BELGIË
Wetstraat 16
1000 Brussel

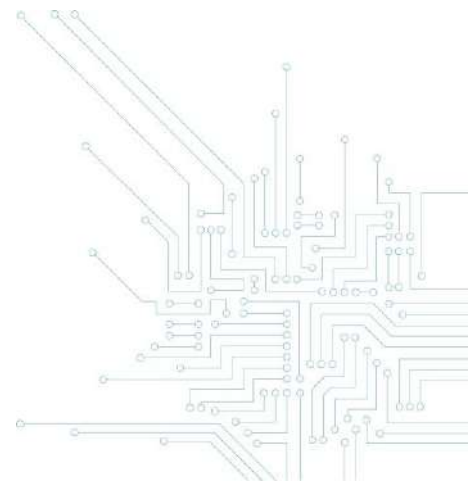
info@ccb.belgium.be
www.ccb.belgium.be



.be

UNDER THE AUTHORITY
OF THE PRIME MINISTER

A.	Inhoudsopgave	
B.	Toepassing van het Belgisch strafrecht	4
C.	Indringing in een informaticasysteem	5
	<i>Afdeling 1. Externe indringing</i>	<i>5</i>
	<i>Afdeling 2. Interne indringing</i>	<i>10</i>
	<i>Afdeling 3. Verzwarende omstandigheden van de indringing</i>	<i>13</i>
	<i>Afdeling 4. Beleid voor de gecoördineerde bekendmaking van kwetsbaarheden en indringing</i>	<i>15</i>
D.	Inbreuk in verband met informaticagegevens	17
	<i>Afdeling 1. Materiële constitutieve elementen</i>	<i>18</i>
	<i>Afdeling 2. Moreel element</i>	<i>18</i>
	<i>Afdeling 3. Verzwarende omstandigheden</i>	<i>19</i>
	<i>Afdeling 4. Ter beschikking stellen van middelen om de inbreuk in verband met gegevens mogelijk te maken</i>	<i>19</i>
	<i>Afdeling 5. Poging</i>	<i>20</i>
	<i>Afdeling 6. Beleid voor de gecoördineerde bekendmaking van kwetsbaarheden en inbreuk in verband met informaticagegevens</i>	<i>20</i>
E.	Valsheid in informatica en informaticabedrog	21
	<i>Afdeling 1. Valsheid in informatica en het gebruik van valse stukken in informatica</i>	<i>21</i>
	<i>Afdeling 2. Informaticabedrog</i>	<i>23</i>
	<i>Afdeling 3. Beleid voor de gecoördineerde bekendmaking van kwetsbaarheden, valsheid in informatica en informaticabedrog</i>	<i>24</i>
F.	Misdrijven betreffende het geheim van communicatie	24
	<i>Afdeling 1. Misdrijven betreffende het geheim van niet voor het publiek toegankelijke communicatie en gegevens van een informaticasysteem</i>	<i>24</i>
	<i>Afdeling 2. Voorbereidende handelingen</i>	<i>27</i>
	<i>Afdeling 3. Helen van onrechtmatig verkregen communicatie</i>	<i>28</i>
	<i>Afdeling 4. Poging</i>	<i>29</i>
	<i>Afdeling 6. Beleid voor de gecoördineerde bekendmaking van kwetsbaarheden en communicatie</i>	<i>33</i>
G.	Naleving van andere wettelijke bepalingen	35
	<i>Afdeling 1. Begrippen in verband met persoonsgegevens</i>	<i>35</i>
	<i>Afdeling 2. Juridische invulling van de rol van deelnemer</i>	<i>37</i>
	<i>Afdeling 3. Gevolgen voor de inhoud van het CVDP</i>	<i>39</i>
H.	Juridische referenties	41



Opgelet:

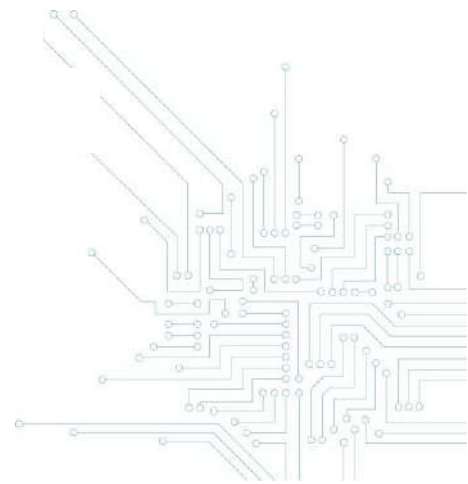
In deze gids vindt u een overzicht van de begrippen, doelstellingen, juridische vraagstukken en goede praktijken rond de invoering van een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden (of Coordinated Vulnerability Disclosure Policy – “CVDP”) in de huidige stand van de Belgische wetgeving – 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, blijft 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 behoedzaam te werk gaan en alle voorwaarden van het beleid en de toepasselijke wettelijke bepalingen nauwgezet naleven.



Designed by CCB and Intigrity (2020)



B. Toepassing van het Belgisch strafrecht

De toepassing van het Belgisch strafrecht hangt voornamelijk af van de lokalisering van het misdrijf. Volgens de objectieve ubiciteitstheorie wordt een misdrijf gelokaliseerd op de plaats waar de daad heeft plaatsgevonden en op de plaats(en) waar het resultaat ervan verschijnt.¹

Daarvoor volstaat het dat een van de materiële constitutieve of materiële verzwarende elementen² van een misdrijf plaatsvond op Belgisch grondgebied, zonder dat het misdrijf volledig in België moet zijn gepleegd. Zo kan het Belgisch strafrecht worden toegepast als de dader materiële handelingen heeft gesteld in België, als het informaticasysteem of de gegevens zich in België bevinden, of als de eventuele schade in België is aangebracht.

In die context kunnen de in deze gids beschreven regels worden toegepast als de dader zich in België bevindt tijdens zijn deelname aan het beleid voor gecoördineerde bekendmaking of als het bezochte informaticasysteem zich in België bevindt.

Gezien de gemeenschappelijke regels van het Cybercrimeverdrag van Boedapest³ en de Europese wetgeving⁴ zijn sommige elementen van deze juridische analyse in België ook toepasselijk op andere landen, met name in Europa. Niettemin moet telkens bij de bevoegde nationale autoriteiten worden nagegaan of dat wel degelijk het geval is.

¹ Cass., 23 januari 1979, *Pas.*, I, 1979, p. 582; Cass., 4 februari 1986, *Pas.*, 1986, blz. 664.

² En niet louter intentionele elementen.

³ Cybercrimeverdrag van de Raad van Europa, opgemaakt in Boedapest op 23 november 2001, in werking getreden op 1 juli 2004.

⁴ Richtlijn 2013/40/EU van het Europees Parlement en de Raad van 12 augustus 2013 over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad, Pb., 14 augustus 2013.

C. Indringing in een informaticasysteem⁵

Afdeling 1. Externe indringing

Artikel 550*bis*, § 1, van het Strafwetboek bestraft degene die, wetende dat hij er niet toe gerechtigd is, zich toegang verschafft tot een informaticasysteem of zich daarin handhaaft.

1. Materiële constitutieve elementen

1.1. Toegang tot of handhaving in een informaticasysteem

a) Informaticasysteem

De wet van 28 november 2000 inzake informaticacriminaliteit, die artikel 550*bis* heeft ingevoerd in het Strafwetboek, heeft niet bepaald wat moest worden verstaan onder "informaticasysteem".⁶ Niettemin beschrijven de voorbereidende werkzaamheden van de wet enerzijds het begrip "informaticasysteem" als elk systeem voor de opslag, verwerking of overdracht van gegevens en anderzijds het begrip "gegevens" als voorstellingen van informatie, ongeacht de materiële vormgeving ervan (elektromagnetisch, optisch of anderszins) die geschikt zijn voor opslag, verwerking en overdracht via een informaticasysteem.⁷

We kunnen ook verwijzen naar de Europese richtlijn 2013/40/EU van 12 augustus 2013 over aanvallen op informatiesystemen⁸, die deze twee begrippen definieert:

- een "informatiesysteem" is een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er een of meer op basis van een programma automatisch computergegevens verwerken, alsmede de computergegevens die met dat apparaat of die groep van apparaten

⁵ Wij verkiezen hier de term "indringing" in plaats van "hacking" omdat "hacking" op informaticagebied niet volledig overeenstemt met het begrip "illegale informaticapiraterij" en ook kan verwijzen naar activiteiten die met de toestemming van de verantwoordelijke van het informaticasysteem worden uitgevoerd. Het begrip "indringing" betekent wel degelijk het binnendringen in (een deel van) een informaticasysteem, zonder daartoe gemachtigd te zijn.

⁶ Op dit punt lijkt de wetgever met opzet onduidelijk te zijn gebleven om te vermijden dat de concepten al te snel achterhaald zouden zijn door de evolutie van de informatietechnologieën: cf. in dat opzicht, *Parl.St.*, Kamer, 1999-2000, nr. 50, 0213/001, blz. 12. De Belgische wetgever heeft rekening gehouden met de snelle evolutie van de technologie bij het opstellen van de wet van 28 november 2000 inzake informaticacriminaliteit, zodat de terminologie van de wet technologisch neutraal is: *Parl.St.*, Kamer, 2003-2004, nr. 1284/001, blz. 5.

⁷ *Parl.St.*, Kamer, 1999-2000, nr. 50, 0213/001, blz. 12.

⁸ Pb., 14 augustus 2013. Zie ook de definities in art. 1 van het Cybercrimeverdrag van de Raad van Europa, opgemaakt in Boedapest op 23 november 2001, in werking getreden op 1 juli 2004 en goedgekeurd door België (wet van 3 augustus 2012, B.S. van 21 november 2012, blz. 69092).

worden opgeslagen, verwerkt, opgehaald of verzonden met het oog op de werking, het gebruik, de beveiliging en het onderhoud daarvan⁹;

- “computergegevens” zijn een weergave van feiten, gegevens of begrippen in een vorm die geschikt is voor verwerking in een informatiesysteem, met inbegrip van programma’s die een informatiesysteem een bepaalde functie kunnen laten vervullen.

Het begrip “informaticasysteem” gaat dus verder dan dat van de gewone personal computer en betreft, in ruime zin, alle vormen van systemen die gegevens verwerken: een elektronische tablet, een gps, een smartphone, een elektronisch horloge, een netwerk, een server, een router, een decoder, een internettelevisie, de boordcomputer van een voertuig, een elektronische betaalterminal, een chipkaart, enz.

b) Toegang of handhaving

Aangezien de begrippen “toegang” of “handhaving” niet zijn gedefinieerd in het Strafwetboek of de parlementaire werkzaamheden, moeten ze worden begrepen in de zin van het normale taalgebruik, zonder het gebruik van een bijzondere techniek te vereisen.

Het begrip “toegang” impliceert een positieve indringingshandeling die met zekerheid de wil vertolkt om binnen te dringen in het informaticasysteem¹⁰, zonder noodzakelijkerwijs complexe informaticamanipulaties te vereisen¹¹: het volstaat bijvoorbeeld om een opdracht uit te voeren die het mogelijk maakt om een systeem op te starten, een programma te openen, een bestand op te zoeken of door een tekst te scrollen.

In geval van indringing handelt de dader van het misdrijf doorgaans van buiten het systeem via een telecommunicatie-infrastructuur en omzeilt hij daarbij beveiligingsmaatregelen.

Het begrip “toegang” vereist echter niet dat er gegevens zijn ingevoerd, gewijzigd of verwijderd in het informaticasysteem.

De handhaving betreft met name het geval waarbij een persoon zich door onachtzaamheid (zonder het te beseffen) zonder machtiging toegang verschaft tot een informaticasysteem, en zich daarin handhaaft nadat hij dit heeft ingezien. Het kan ook gaan om het geval waarbij een persoon zijn toegang

⁹ Deze elementen zijn ook opgenomen in de definitie van “netwerk- en informatiesysteem” van richtlijn 2016/1148 van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (NIS-richtlijn).

¹⁰ De geïnformatiseerde terminal van een banktransactiesysteem is, in de zin van deze bepaling, een informaticasysteem: Corr. Dendermonde, 14 mei 2007, *T. Strafr.*, 2007, blz. 403.

¹¹ Corr. Antwerpen, 10 november 2014, *T. Strafr.*, 2015, blz. 94.

tot het systeem behoudt hoewel zijn toegangsmachtiging is verlopen (door het verstrijken van een bepaalde termijn of door het einde van de uitoefening van een functie).¹²

c) Beveiliging van het informaticasysteem

Het misdrijf vereist niet dat de toegang tot of handhaving in een informaticasysteem plaatsvond ingevolge het doorbreken van het systeem of het omzeilen van beveiligingsmaatregelen (paswoord, firewall, identificatie, versleuteling, enz.). Het ontbreken van beveiligingsmaatregelen voor het informaticasysteem sluit het bestaan van een externe indringing dus niet uit.

Tijdens de parlementaire werkzaamheden werd deze keuze gerechtvaardigd door het feit dat het begrip “doorbreken” enerzijds een aantal praktische complicaties zou meebrengen (het bepalen van een vereist beveiligingsniveau en de noodzaak om beveiligingssystemen openbaar te maken bij de bewijsvoering) en anderzijds wellicht niet zinvol zou zijn door de toenemende standaardisering van systeembeveiliging.¹³

Een externe indringing kan dus bestaan in het loutere gebruik van een onbeveiligd draadloos netwerk om verbinding te maken met het internet zonder de toestemming van de beheerder van dat netwerk.¹⁴

d) Schade veroorzaakt aan het informaticasysteem

Het is niet vereist dat de indringing of handhaving schade heeft veroorzaakt aan het informaticasysteem. Een louter risico volstaat, ook als het zich niet realiseert.¹⁵ De wetgever beschouwt externe indringing immers als “een gevaarzettingsdelict dat als zodanig strafwaardig is, ongeacht de bijzondere kwaadwillige bedoelingen of de gerealiseerde effecten”.

De wetgever heeft de ongeoorloofde toegang tot een informaticasysteem als dusdanig strafrechtelijk willen bestraffen. Zo kan de loutere kennisneming van de inhoud of van de werkings- of beveiligingsparameters van het informaticasysteem van een derde, zelfs zonder deze te wijzigen of te schaden, een misdrijf zijn.

¹² Bijvoorbeeld het behoud van een verbinding met het informaticasysteem van een bedrijf door een ex-werknemer.

¹³ *Parl.St.*, Kamer, 1999-2000, nr. 50, 0213/001, blz. 17.

¹⁴ Corr. Dendermonde, 14 november 2008, *T. Straf.*, 2009, blz. 114.

¹⁵ Overeenkomstig art. 550bis, § 3, 3°, van het Strafwetboek vormt het bestaan van schade niettemin een verzwarende omstandigheid van het misdrijf.



1.2. Totaal gebrek aan machtiging

Het begrip “machtiging” wordt niet verduidelijkt in het Strafwetboek en moet dus, volgens de interpretatiebeginselen in strafzaken, worden begrepen in de zin van het normale taalgebruik. In voorkomend geval betreft het de toestemming die een gemachtigd persoon aan een ander heeft gegeven om zich toegang te verschaffen tot het betrokken informaticasysteem of zich daarin te handhaven.

Concreet kunnen zich twee situaties voordoen: ofwel dringt een persoon bewust binnen in een informaticasysteem hoewel hij geen toegangsmachtiging heeft, zelfs geen gedeeltelijke, ofwel verschaft een persoon zich door onachtzaamheid toegang tot een informaticasysteem, of bewust na het verstrijken van zijn machtiging, en handhaaft hij zich daar onrechtmatig in.

De externe indringing is een aflopend misdrijf en bestaat dus vanaf het ogenblik dat het individu zich zonder machtiging toegang verschaft tot het informaticasysteem of zich daarin zonder machtiging handhaaft. De eventueel na de feiten verleende machtiging doet het bestaan van een strafrechtelijk misdrijf dus niet verdwijnen.

Om geldig te zijn, moet de toestemming om zich toegang te verschaffen tot een informaticasysteem of zich daarin te handhaven noodzakelijkerwijs komen van een persoon die daartoe gemachtigd is door de houder van de rechten op het systeem, namelijk de verantwoordelijke van dit systeem.¹⁶ Het zijn tenslotte de verantwoordelijke van het systeem en zijn gedelegeerden die de taak hebben om de voorwaarden van een dergelijke machtiging toe te kennen, in te trekken en te bepalen. Deze machtiging kan uitdrukkelijk of stilzwijgend zijn, voor zover ze met zekerheid bestaat.

a) Uitdrukkelijke machtiging

De uitdrukkelijke machtiging bestaat erin dat de beheerder van het informaticasysteem een bepaalde natuurlijke of rechtspersoon uitdrukkelijk machtigt om zich toegang te verschaffen tot zijn informaticasysteem, bijvoorbeeld om er onderhoudswerkzaamheden, beveiligingstests of programma-updates uit te voeren. Deze uitdrukkelijke machtiging is doorgaans opgenomen in contractuele bepalingen of in interne documenten van de organisatie.

Als een organisatie een beveiligingsauditovereenkomst sluit die de uitvoering van binnendringingstests omvat¹⁷, geeft ze uitdrukkelijk toestemming voor toegang tot – op zijn minst een deel van – haar

¹⁶ Naargelang de structuur van de organisatie kan deze persoon bijvoorbeeld de eigenaar van het systeem zijn, het hoofd van de organisatie, de informaticaverantwoordelijke of de informatiebeveiligingsadviseur.

¹⁷ "Pentesting"-overeenkomst.



informaticasysteem. In dat geval beschikt de dienstverlener, een informatiebeveiligingsspecialist, over een toegangsmachtiging en moet hij geen strafrechtelijke vervolging voor externe hacking vrezen.

b) Stilzwijgende machtiging

De stilzwijgende machtiging vloeit voort uit de bijzondere omstandigheden van de zaak. Bijvoorbeeld de uitoefening van een functie voor rekening van een bedrijf die noodzakelijkerwijs de toegang tot de informaticamiddelen ervan impliceert om de taken uit te voeren, zelfs zonder uitdrukkelijke machtiging.¹⁸

In dezelfde zin kan een stilzwijgende machtiging ook voortvloeien uit het bestaan van een informaticasysteem dat duidelijk ter beschikking van het publiek wordt gesteld.¹⁹

Uiteraard beschikken de eigenaar van het informaticasysteem en zijn wettelijke vertegenwoordigers over een – minstens stilzwijgende – toegangsmachtiging voor het betrokken informaticasysteem, zolang ze zich rechtsgeldig kunnen beroepen op die hoedanigheden.

De stilzwijgende machtiging verdwijnt evenwel vanaf het ogenblik dat de voor rekening van het bedrijf uitgeoefende functie, het publieke karakter van de toegang, de terbeschikkingstelling van de klanten of het eigendomsrecht afloopt. Indien de betrokkene zich achteraf handhaaft in het informaticasysteem of zich daar achteraf toegang toe verschafft, wordt dit dus beschouwd als een indringing.

2. Moreel element

2.1. Wil om zich toegang te verschaffen tot het systeem en kennis van het gebrek aan machtiging

Het misdrijf vereist eenvoudigweg de bewuste en vrije wil om zich toegang te verschaffen tot een informaticasysteem of zich daarin te handhaven hoewel men weet dat men er niet toe gerechtigd is. Artikel 550*bis* van het Strafwetboek vereist geen bijzonder opzet, zoals bijvoorbeeld een bedrieglijk opzet of het oogmerk om te schaden. De opzettelijke en ongeoorloofde indringing of handhaving in een informaticasysteem volstaat om het misdrijf te plegen. De indringing die het gevolg is van onachtzaamheid, verstrooidheid, een manipulatiefout of een onvoldoende beheersing van de

¹⁸ Werknemers krijgen echter vaak wel een login en een paswoord van hun werkgever waardoor ze uitdrukkelijk worden gemachtigd om toegang te hebben tot het informaticasysteem.

¹⁹ Bijvoorbeeld een draadloos netwerk in een openbare ruimte en zonder paswoord (hotspots), een draadloze computer of een draadloos netwerk van een instelling die/dat ter beschikking wordt gesteld van klanten, een automatische betaalkassa, een kiosk voor het inchecken van bagage door passagiers in een luchthaven, enz.

informaticatool (waarbij de persoon te goeder trouw heeft gehandeld) wordt daarentegen niet strafbaar gesteld (indien de persoon zich daarna niet met kennis van zaken handhaaft in het informaticasysteem).

De opzettelijke (ongeoorloofde) indringing met een eerbaar motief, zoals bijvoorbeeld het opsporen van informaticabeveiligingsgebreken in het informaticasysteem van een derde, wordt wel strafbaar gesteld.²⁰ De wetgever wilde immers elke indringing – behalve de onopzettelijke – in een informaticasysteem bestraffen zonder rekening te houden met het opzet van de indringer.²¹ Doel is de vertrouwelijkheid, integriteit en beschikbaarheid van informaticasystemen en van de gegevens die erin worden opgeslagen, verwerkt of overgedragen zoveel mogelijk te beschermen.

Het feit dat de indringer goede bedoelingen had of na de feiten de toestemming kreeg van de verantwoordelijke van het informaticasysteem, is dus geen rechtvaardigingsgrond voor het uitsluiten van een mogelijke strafrechtelijke veroordeling voor externe indringing. Het zou voor indringers inderdaad gemakkelijk zijn om zogenaamde goede bedoelingen aan te voeren na het begin van hun vervolging en het zou moeilijk zijn om deze a posteriori te controleren.

De rechtspraak heeft aldus bevestigd dat externe indringing met als doel louter na te gaan of de informaticabeveiligingsmaatregelen van een concurrent voor diens gegevensbescherming even onbetrouwbaar zijn als de zijne, wel degelijk een misdrijf is.²²

Het bedrieglijk opzet van de dader geldt niettemin als een verzwarende omstandigheid van het misdrijf, die de opgelegde straf zal verzwaren.²³

Afdeling 2. Interne indringing

Artikel 550*bis*, § 2, van het Strafwetboek betreft diegene die, met bedrieglijk opzet of met het oogmerk om te schaden, zijn toegangsbevoegdheid tot een informaticasysteem overschrijdt.

²⁰ Corr. Hasselt, 21 januari 2004, *Lim. Rechtsl.*, 2005, blz. 133; *Computerr.*, 2004, boek 3, blz. 131: het bestaan van een misdrijf is bijvoorbeeld niet uitgesloten wanneer een gebruiker die de beveiliging van het pc-bankingsysteem van zijn bank nagaat, ontdekt dat het mogelijk is om verrichtingen te doen die gebruikers van het systeem schade kunnen berokkenen (zoals lijsten met begunstigen van overschrijvingen van andere gebruikers downloaden, bankrekeningnummers van deze lijsten wijzigen en die gewijzigde lijst terug op hun harde schijf zetten, waardoor overschrijvingen naar andere rekeningnummers dan die van de begunstigen mogelijk zijn) en zijn bank daarvan op de hoogte brengt; Corr. Eupen, 15 dec. 2003, *R.D.T.I.*, 2004, blz. 61 en nota O. LEROUX; Corr. Leuven, 15 juni 2010, *T. Strafr.*, 2011, blz. 270; Corr. Dendermonde, 25 mei 2007, *T.G.R.*, 2007, blz. 351 e.v.

²¹ Corr. Brussel, 8 jan. 2008, *J.T.*, 2008, blz. 337.

²² Corr. Eupen, 15 dec. 2003, *R.D.T.I.*, 2004, blz. 61.

²³ Art. 550*bis*, § 1, tweede lid, van het Strafwetboek.

1. Materiële constitutieve elementen

1.1. Bestaan van een gedeeltelijke machtiging

Interne indringing veronderstelt het bestaan, vóór het plegen van het misdrijf, van een gedeeltelijke toegangsmachtiging voor het betrokken informaticasysteem.²⁴ Bij gebrek aan nadere toelichting in het Strafwetboek moet de machtiging worden begrepen in de gebruikelijke zin, net zoals bij de externe indringing (*supra*).

De aard en de omvang van de toegangsbevoegdheid tot een informaticasysteem worden immers in beginsel niet bepaald door de wetgever, maar overgelaten aan de beoordelingsbevoegdheid van de eigenaar van het systeem, aangezien deze het best geplaatst is om te bepalen wie toegangsbevoegdheid krijgt en binnen welke grenzen.²⁵

De grenzen die aan de toegangsmachtiging worden gesteld, kunnen bijvoorbeeld “ruimtelijk” zijn, dat wil zeggen gelinkt aan bepaalde verboden delen van het informaticasysteem, of “functioneel”, dat wil zeggen gelinkt aan bepaalde verboden verrichtingen of bepaalde verboden gegevenscategorieën voor het hele systeem. De beperking is duidelijk als het systeem bijvoorbeeld voorzien is van een voorafgaand identificatieproces om toegang te krijgen tot bepaalde gegevens of programma’s.²⁶

De finaliteit waarvoor een persoon een toegangsmachtiging voor een informaticasysteem krijgt, beperkt dit toegangsrecht niet, tenzij uitdrukkelijk anders is bepaald door de verantwoordelijke van het systeem. Er kan niet worden gesteld dat een persoon zijn toegangsrecht heeft overschreden in de zin van artikel 550*bis*, § 2, van het Strafwetboek enkel en alleen omdat hij deze machtiging heeft afgewend van de finaliteit ervan.²⁷ Bijgevolg pleegt de persoon die zijn toegangsrecht tot een informaticasysteem voor persoonlijke doeleinden gebruikt, hoewel hij een toegangsmachtiging heeft gekregen voor welbepaalde professionele doeleinden, geen interne indringing.

Het begrip betreft zowel personen met een permanente gedeeltelijke machtiging, zoals deze die wordt toegekend aan het personeel van een bedrijf, als personen die een gedeeltelijke machtiging hebben die beperkt is in de tijd, zoals deze die tijdelijk wordt toegekend aan een consultant van een extern bedrijf dat gespecialiseerd is in informaticabeveiliging.

²⁴ Corr. Leuven, 15 juni 2010, *T. Strafr.*, 2011, blz. 270: de rechtbank oordeelde dat het feit klant te zijn van een bank en een toegangsbevoegdheid te hebben voor het pc-bankingsysteem, die persoon geen toegangsbevoegdheid verleent voor het informaticasysteem van de bank.

²⁵ Arbitragehof, 24 maart 2004, nr. 51/2004, B.4.3, blz. 7.

²⁶ Corr. Brussel, 8 jan. 2008, *J.T.*, 2008, blz. 337.

²⁷ Cass., 24 januari 2017, P.16.0048.N, www.cass.be.



Hoewel vaak sprake is van een voorafgaande gedeeltelijke machtiging in het kader van een contractuele verbintenis, impliceert dit begrip niet noodzakelijk een band van ondergeschiktheid, een hiërarchische band of een contractuele band tussen de verlener van de machtiging en de begunstigde.

1.2. Overschrijden van de machtiging

Het misdrijf bestaat vanaf het ogenblik dat de dader zijn toegangsrechten overschrijdt om binnen te dringen of zich te handhaven in een deel van het informaticasysteem waarvoor hij geen toegangsmachtiging (meer) heeft op het ogenblik van het misdrijf.²⁸

Dit geval betreft onder andere de situatie van een werknemer die een gedeeltelijke toegangsbevoegdheid tot de server van zijn bedrijf heeft gekregen om zijn taken te vervullen, maar de hem opgelegde grenzen overschrijdt.

Net als bij de externe indringing moet de interne indringing niet noodzakelijk schade hebben toegebracht aan het bezochte systeem om bestraft te worden.

2. Moreel element

2.1. Wil om zijn machtiging te overschrijden

Het misdrijf vereist de wil om zich, opzettelijk en met kennis van zaken, toegang te verschaffen tot een deel van het informaticasysteem of zich erin te handhaven hoewel de persoon weet dat hij zo zijn toegangsbevoegdheid voor het informaticasysteem overschrijdt.

2.2. Bijzonder opzet: bedrieglijk opzet of oogmerk om te schaden

Het louter zonder toestemming binnendringen in bepaalde delen van het informaticasysteem, bijvoorbeeld uit pure nieuwsgierigheid, wordt niet strafrechtelijk bestraft. De indringing moet zijn ingegeven door een bijzonder opzet, d.w.z. onrechtmatig winstbejag (fraude) of kwaadwillige bedoelingen (oogmerk om te schaden), om een misdrijf te zijn. Dat kan bijvoorbeeld het geval zijn wanneer een werknemer die toegang heeft tot een deel van het bedrijfsnetwerk, deze machtiging

²⁸ Zie Cass., 5 januari 2011, P.10.1094.F., www.cass.be: de vaststelling dat de vervolgte personen toegangsrecht hadden tot de litigieuze gegevens toen ze de kopie ervan vroegen en kregen, sluit de overschrijding van de toegangsbevoegdheid uit die bij artikel 550bis, § 2, Strafwetboek, strafbaar is gesteld.

overschrijdt om zich toegang te verschaffen tot het boekhoudprogramma en er ongeoorloofde bankverrichtingen te doen, of nog, bepaalde data voor eigen rekening te commercialiseren.²⁹

De wetgever heeft dit onderscheid met het misdrijf van externe indringing verantwoord door het feit dat derden die niet over een toegangsmachtiging beschikken de veiligheid van het informaticasysteem meer in gevaar zouden brengen dan een persoon die een gedeeltelijke machtiging heeft.³⁰ Bovendien hebben de parlementaire werkzaamheden erop gewezen dat de verantwoordelijke van het systeem over andere sancties (burgerrechtelijke of contractuele sancties, of tuchtstraffen) beschikt tegen de begunstigde van een gedeeltelijke machtiging die zonder bedrieglijk of kwaadwillig opzet zou zijn overschreden.³¹

Afdeling 3. Verzwarende omstandigheden van de indringing

Artikel 550*bis*, § 3, van het Strafwetboek voorziet in een aantal verzwarende omstandigheden die gelden voor beide misdrijven met betrekking tot indringing.

1. Overname van gegevens

De eerste verzwarende omstandigheid is de overname, op enige manier, van gegevens die worden opgeslagen, verwerkt of overgedragen door middel van het bezochte informaticasysteem.³² Het betreft het overnemen van informaticagegevens (origineel of kopie) uit het bezochte systeem om deze in voorkomend geval opnieuw te kunnen gebruiken.³³ De gebruikte formulering “op enige manier” is heel ruim en kan dus verwijzen naar het afdrukken, het via mail versturen, het kopiëren op een drager, het opslaan in een cloudsysteem, het maken van een screenshot, enz.³⁴ Doel van de wetgever was hier onder meer het stelen van industriële geheimen in het kader van bedrijfsspionage te bestrijden.³⁵

Het begrip “overname” van gegevens lijkt ten slotte een moreel element te vereisen aangezien het voortvloeit uit het feit dat de dader zelf het initiatief neemt om deze gegevens op te halen en niet uit

²⁹ *Parl.St.*, Kamer, 1999-2000, nr. 50, 0213/004, blz. 6.

³⁰ *Parl.St.*, Kamer, 1999-2000, nr. 50, 0213/001, blz. 16.

³¹ *Parl.St.*, Senaat, 1999-2000, 2-392/3, blz. 6; *Parl.St.*, Kamer, 1999-2000, nr. 50, 0213/001, blz. 16.

³² *Corr. Dendermonde*, 14 mei 2007, *T. Strafr.*, 2007, blz. 403.

³³ Dit gedrag wordt soms “bitnapping” genoemd, een verwijzing naar de kidnapping van gegevens.

³⁴ Er moet echter worden verduidelijkt dat deze bepaling niet verwijst naar het materieel meenemen van de drager waarop informaticagegevens waren afgedrukt of opgeslagen (bv. het stelen van afgedrukte gegevens, van een harde schijf of van een USB-stick), wat een ander misdrijf is, namelijk het stelen van de drager zelf.

³⁵ *Parl.St.*, Kamer, 1999-2000, nr. 50, 0213/001, blz.17: een werknemer die zakengeheimen van zijn werkgever tracht te stelen, kan ook worden vervolgd voor het misdrijf van het meedelen van fabrieksgeheimen, zoals bedoeld in art. 309 van het Strafwetboek.

het louter automatisch opslaan van gegevens door het informaticasysteem dat voor de indringing wordt gebruikt.

2. Gebruik van het bezochte systeem

De tweede verzwarende omstandigheid is enig gebruik van een informaticasysteem van een derde of het feit dat gebruik wordt gemaakt van het informaticasysteem om toegang te krijgen tot het informaticasysteem van een derde. Enerzijds betreft de bepaling het benutten van de capaciteit van het bezochte informaticasysteem, waardoor de gebruiksmogelijkheden van andere gebruikers tijdelijk beperkt worden (bv. tijdsdiefstal of diefstal van bandbreedte).³⁶ Anderzijds betreft ze het feit zich toegang te verschaffen tot een ander informaticasysteem via het bezochte systeem, dat gebruikt wordt als tussenschakel voor een informatica-aanval waarbij de indruk wordt gewekt dat de aanval van een tussensysteem komt.³⁷

De twee bedoelde gevallen veronderstellen wel degelijk een moreel element, nl. dat de dader wetens en willens de bedoeling had om voor deze doeleinden gebruik te maken van het informaticasysteem. Dit element sluit bijvoorbeeld het geval uit waarbij de vermindering van de capaciteit van het informaticasysteem onverwachts zou voortvloeien uit de indringing.

3. Schade aan het informaticasysteem of aan de gegevens

De derde verzwarende omstandigheid bestaat erin enige schade te veroorzaken, zelfs onopzettelijk, aan het informaticasysteem of aan de gegevens die erin worden opgeslagen, verwerkt of overgedragen, of aan het informaticasysteem of de informaticagegevens van een derde.

Dit omvat elke soort schade, zowel materiële (fysieke beschadiging van het systeem, kabels of randapparatuur) als immateriële (verzadiging van het systeem, onbeschikbaarheid) schade aan het bezochte informaticasysteem of aan de gegevens ervan.

In dit geval kan de schade opzettelijk of onopzettelijk zijn veroorzaakt, zodat er geen moreel element vereist is in hoofde van de dader.³⁸

³⁶ *Parl.St.*, Kamer, 1999-2000, nr. 50, 0213/001, blz. 17.

³⁷ C. MEUNIER, "La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique", *op. cit.*, blz. 639. Het kan bijvoorbeeld gaan om het gebruik van het informaticasysteem in een botnet-netwerk, d.w.z. in een groep van geïnfecteerde computers ("zombies") die op afstand gecontroleerd worden door een hacker om andere informaticasystemen aan te vallen en daarbij de echte oorsprong van de aanval te verbergen.

³⁸ Niettemin moet het optreden van deze omstandigheid voor de dader wel voorzienbaar zijn en er moet een oorzakelijk verband zijn tussen deze omstandigheid en het plegen van het hoofdmisdrijf. De opzettelijk veroorzaakte schade die

Afdeling 4. Beleid voor de gecoördineerde bekendmaking van kwetsbaarheden en indringing

Zoals eerder uiteengezet, bestaat het misdrijf van externe indringing in een informaticasysteem zelfs als de dader geen kwaadwillige bedoelingen heeft, geen beveiligingsmaatregelen omzeilt, het bezochte systeem niet gebruikt, geen gegevens overneemt en geen schade veroorzaakt aan het systeem of aan de gegevens. De goede bedoelingen van de deelnemer aan een CVDP volstaan dus niet om het bestaan van dit strafrechtelijk misdrijf te vermijden.

Er is echter alleen sprake van externe indringing als de deelnemer niet beschikt over een machtiging van de verantwoordelijke organisatie om zich toegang te verschaffen tot haar informaticasysteem. Als de deelnemer in het kader van een machtiging handelt, is er geen sprake van externe indringing.

In het kader van een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden of een beloningsprogramma voor het opsporen van kwetsbaarheden bestaat een dergelijke – uitdrukkelijke of stilzwijgende – machtiging.

Bij de invoering van een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden, met inbegrip van een beloningsprogramma, wordt de facto op zijn minst een stilzwijgende en duidelijke machtiging verleend. Dat beleid verduidelijkt immers de samenwerkingsmodaliteiten tussen een organisatie die verantwoordelijk is voor het betrokken informaticasysteem en deelnemers die bereid zijn om haar te informeren over kwetsbaarheden van haar informaticasysteem. Deze samenwerking houdt noodzakelijkerwijs een machtiging in om zich toegang te verschaffen tot het betrokken informaticasysteem of om zich daarin te handhaven, met als doel de veiligheid ervan te verbeteren en met inachtneming van de vooraf bepaalde voorwaarden. Ook al is de begunstigde van de machtiging niet precies gekend op het ogenblik dat het beleid voor gecoördineerde bekendmaking wordt ingevoerd, gaat het wel degelijk om een machtiging die eenzijdig wordt toegekend door de verantwoordelijke van het informaticasysteem aan personen die wensen deel te nemen aan zijn programma voor gecoördineerde bekendmaking.

Gelet op het legaliteitsbeginsel moet het strafrecht restrictief worden geïnterpreteerd. In geval van twijfel over de draagwijdte van de gebruikte repressieve termen is de rechter dus verplicht om het toepassingsgebied ervan te beperken. Bijgevolg moet het gebrek aan machtiging, in de zin van artikel 550bis van het Strafwetboek, strikt worden geïnterpreteerd, d.w.z. in het geval dat geen enkele handeling derden terecht kan doen aannemen dat de verantwoordelijke organisatie de toegang tot haar informaticasysteem toestaat. Als de verantwoordelijke organisatie weloverwogen en bewust een beleid voor gecoördineerde bekendmaking heeft ingevoerd, is zij vooraf duidelijk bereid om de toegang tot haar informaticasysteem toe te staan, mits de vastgestelde voorwaarden worden

voortvloeit uit het invoeren, wijzigen of verwijderen van gegevens zal in voorkomend geval aanleiding geven tot een ander misdrijf, nl. de inbreuk in verband met informaticagegevens bedoeld in art. 550ter van het Strafwetboek.

nageleefd. Tevens moet worden opgemerkt dat een deel van de rechtspraak een extensieve uitleg geeft aan de voor de beklagde gunstige bepalingen, wat ook het geval kan zijn voor het begrip “machtiging”. Aangezien de machtiging gunstig is voor de dader van de feiten en het bestaan van een misdrijf uitsluit, moet ze worden geïnterpreteerd als zijnde inherent aan de invoering van een beleid voor gecoördineerde bekendmaking.

Het belang van een beleid voor gecoördineerde bekendmaking bestaat er dus in dat, voor zover de door de verantwoordelijke organisatie geformuleerde voorwaarden worden nageleefd, een van de materiële constitutieve voorwaarden voor het misdrijf van externe indringing, nl. het totale gebrek aan machtiging, wordt uitgesloten. De persoon die deelneemt aan een dergelijk beleid en de voorwaarden ervan naleeft, pleegt dus geen externe indringing.

De deelnemer die over een gedeeltelijke toegangsmachtiging voor een informaticasysteem beschikt, pleegt geen misdrijf van interne indringing als hij met goede bedoelingen beveiligingsgebreken opspoot in delen van dit systeem waarvoor hij geen toegangsmachtiging heeft. Zolang de deelnemer zijn toegangsmachtiging overschrijdt zonder bedrieglijk opzet of het oogmerk om te schaden, is er geen sprake van interne indringing, die strafrechtelijk wordt bestraft.

Hoewel het de bedoeling is dat een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden voornamelijk van toepassing is op personen buiten de verantwoordelijke organisatie die geen toegangsbevoegdheid voor het informaticasysteem hebben, kan dit beleid in voorkomend geval ook een kader bieden voor de handelswijze van deelnemers met goede bedoelingen binnen de organisatie. Bij gebrek aan contractuele regels voor deze gevallen of ingeval deze regels lacunes vertonen, kan een beleid voor gecoördineerde bekendmaking van de verantwoordelijke organisatie immers daadwerkelijk worden toegepast door de partijen. Een dergelijk beleid is dus niet enkel van belang voor personen die geen juridische banden met de verantwoordelijke organisatie hebben.

Uiteraard moeten de omstandigheden waarin een dergelijke “goedwillende” overtreding kan plaatsvinden en de in dat geval te volgen regels strikt worden begrensd in contractuele documenten³⁹ of in het beleid voor de gecoördineerde bekendmaking van kwetsbaarheden⁴⁰.

³⁹ Bijvoorbeeld een arbeidsovereenkomst, een statutaire relatie of een dienstenovereenkomst.

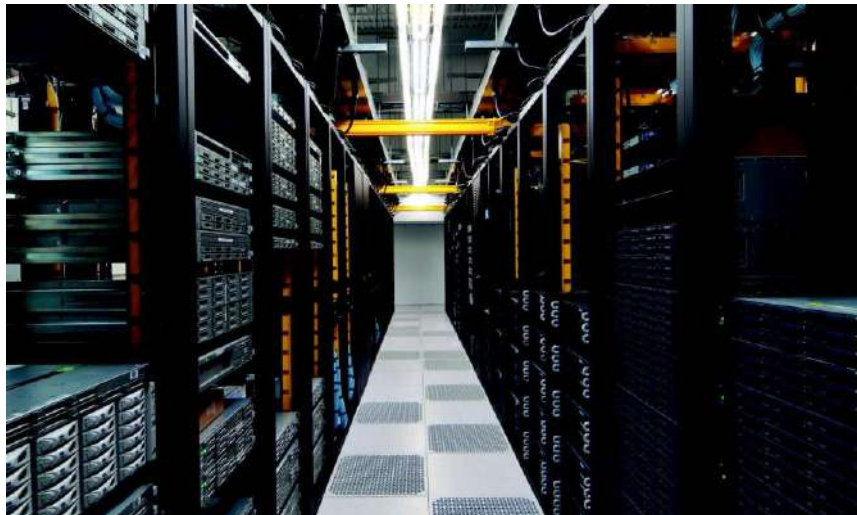
⁴⁰ Het kan gaan om het geval waarbij de begunstigde van een gedeeltelijke machtiging, bijvoorbeeld een werknemer van de informaticadienst, gegronde redenen heeft om te vermoeden dat er sprake is van een kwetsbaarheid, een virus, een worm, een Trojaans paard of ransomware in een deel van het systeem waarvoor hij in principe geen toegangsmachtiging heeft.



Opgelet:

De deelnemer moet er ook voor zorgen dat hij, zonder aanvullende machtiging, geen handelingen stelt met betrekking tot informaticasystemen of gegevens die worden beheerd door derden die niet onder het beleid voor gecoördineerde bekendmaking van de verantwoordelijke organisatie vallen.

Derden zijn immers niet onderworpen aan de inhoud van het beleid voor verantwoorde bekendmaking en kunnen gerechtelijke acties ondernemen wegens het gedrag van de deelnemer.



D. Inbreuk in verband met informaticagegevens⁴¹

Artikel 550ter van het Strafwetboek bestraft degene die, terwijl hij weet dat hij daartoe niet gerechtigd is, rechtstreeks of onrechtstreeks, gegevens in een informaticasysteem invoert, wijzigt of wist, of die met enig technologisch middel de normale aanwending van gegevens in een informaticasysteem verandert.

⁴¹ De keuze voor de term "informaticasabotage" is niet ideaal aangezien hieruit ten onrechte afgeleid kan worden dat er schade is, wat geen constitutief element van het misdrijf is. Het misdrijf betreft in ruimere zin een inbreuk op de integriteit en de authenticiteit van informaticagegevens.



Afdeling 1. Materiële constitutieve elementen

1.1. Invoeren, wijzigen of verwijderen van informaticagegevens met enig technologisch middel

Het doel van het misdrijf is het invoeren, wijzigen, verwijderen van gegevens of het veranderen van de normale aanwending van gegevens met enig technologisch middel in een informaticasysteem. Deze bepaling is er hoofdzakelijk op gericht de integriteit van een informaticasysteem of van de gegevens die het systeem bevat, opslaat en overmaakt, te beschermen tegen informaticamanipulaties in ruime zin. De tussenkomst in het systeem kan rechtstreeks zijn, d.w.z. via het gebruik van een computer die rechtstreeks verbonden is met het netwerk, of onrechtstreeks, d.w.z. via een verbinding op afstand door middel van een telecommunicatienetwerk of een intermediaire computer.

In de praktijk kan het gaan om het invoeren van een virus, een logische bom, een worm, een Trojaans paard, het verwijderen of aanmaken van een bestand, het ontregelen van een besturingssysteem, het versleutelen van bestanden, het onbruikbaar maken van een harde schijf of eenvoudigweg het wijzigen van het paswoord van een gebruiker.

In tegenstelling tot wat men zou kunnen denken, is de schade geen constitutief element van het misdrijf, maar enkel een verzwarende omstandigheid. Het louter achterlaten van een vermelding in het systeem, zoals “X was hier”, is een inbreuk in verband met informaticagegevens. Er blijft echter sprake van een misdrijf ook al heeft het opzettelijk invoeren van gegevens in een computer zijn doel niet bereikt, bv. door een technische storing.

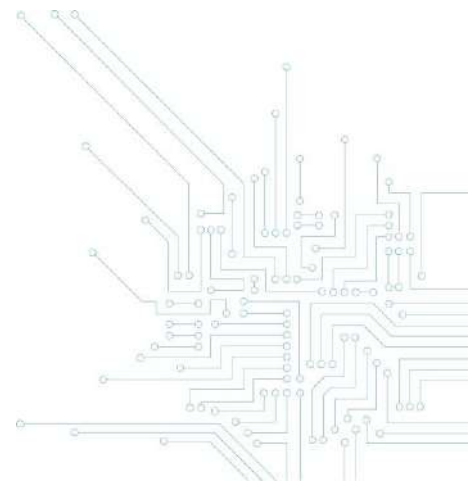
1.2. Gebrek aan machtiging

Het is de bedoeling om elke manipulatie van informaticagegevens⁴² die niet vooraf werd toegestaan door de verantwoordelijke van het betrokken informaticasysteem te bestraffen. De machtiging moet betrekking hebben op de wijziging van gegevens in het informaticasysteem, ongeacht de vraag of de toegang tot het informaticasysteem al dan niet werd toegestaan.

Afdeling 2. Moreel element

De dader moet zich ervan bewust zijn geweest dat hij een ongeoorloofde handeling uitvoerde. De onopzettelijke en onbewuste overdracht van een virus als bijlage bij een mail is dus geen misdrijf in hoofde van de afzender.

⁴² *Parl.St.*, Kamer, 1999-2000, nr. 50, 0213/001, blz. 19.



Afdeling 3. Verzwarende omstandigheden

1. Bedrieglijk opzet of oogmerk om te schaden

Hoewel het bestaan van een bijzonder opzet in hoofde van de dader niet vereist is voor het misdrijf, is het niettemin een verzwarende omstandigheid.⁴³

2. Schade aan gegevens

De schade aan gegevens in het betrokken informaticasysteem of in enig ander informaticasysteem is een verzwarende omstandigheid van het misdrijf.⁴⁴ Het gaat hier om de wijziging van gegevens die door het informaticasysteem worden opgeslagen, overgedragen of verwerkt, in tegenstelling tot de schade aan het systeem zelf.

3. Belemmeren van de werking van het systeem

Deze verzwarende omstandigheid betreft de inbreuk met betrekking tot informaticagegevens die ertoe leidt dat de correcte werking van het betrokken of enig ander informaticasysteem geheel of gedeeltelijk wordt belemmerd.⁴⁵ Het gaat hier om de vernietiging van de inhoud, een totale of gedeeltelijke lamlegging van het informaticasysteem of een vertraging ervan, bijvoorbeeld het massaal versturen van query's om de server te overbelasten of zelfs het toebrengen, vanop afstand, van fysieke schade aan het informaticasysteem. Aangezien deze bepaling ook handelt over "enig ander informaticasysteem", betreft ze ook de uitwerking of verspreiding van computerwormen, die zichzelf automatisch kunnen vermenigvuldigen en kopiëren via communicatienetwerken. Er moet echter een oorzakelijk verband bestaan tussen het hoofdmisdrijf en de veroorzaakte voorzienbare schade.

Afdeling 4. Ter beschikking stellen van middelen om de inbreuk in verband met gegevens mogelijk te maken

Los van het misdrijf van de inbreuk in verband met informaticagegevens bestraft het Strafwetboek ook degene die onrechtmatig enig instrument, met inbegrip van informaticagegevens, dat hoofdzakelijk is ontworpen of aangepast om misdrijven van inbreuken in verband met informaticagegevens mogelijk te maken, bezit, produceert, verkoopt, verkrijgt met het oog op het gebruik ervan, invoert, verspreidt of op enige andere manier ter beschikking stelt terwijl hij weet dat deze gegevens aangewend kunnen worden om schade te berokkenen aan gegevens of, geheel of gedeeltelijk, de correcte werking van een informaticasysteem te belemmeren.⁴⁶

⁴³ Zie de overwegingen over het bijzonder opzet dat vereist is voor het misdrijf van interne ongeoorloofde indringing; art. 550ter, § 1, van het Strafwetboek.

⁴⁴ Art. 550ter, § 2, van het Strafwetboek.

⁴⁵ Art. 550ter, § 3, van het Strafwetboek voorziet in een gevangenisstraf van één jaar tot vijf jaar en een geldboete van 26 tot 100.000 € of een van die straffen. Gelet op het belang van informaticasystemen in onze maatschappij wordt het belemmeren van de goede werking van een informaticasysteem overigens strenger bestraft dan het louter veroorzaken van schade aan gegevens.

⁴⁶ Art. 550ter, § 4, van het Strafwetboek.



1. Materiële constitutieve elementen

Het misdrijf betreft het uitwerken, bezitten of ter beschikking stellen van instrumenten of informaticagegevens die hoofdzakelijk zijn ontworpen of aangepast om een inbreuk in verband met informaticagegevens te plegen. Het begrip “instrument” stemt hier overeen met dat met betrekking tot de middelen om een indringing mogelijk te maken.

2. Moreel element

Het misdrijf vereist een intentioneel element, namelijk dat de dader weet dat de instrumenten of gegevens kunnen worden aangewend om schade te berokkenen aan gegevens of de correcte werking van een informaticasysteem geheel of gedeeltelijk te belemmeren. De dader moet aldus met kennis van zaken handelen en bereid zijn om dergelijke instrumenten uit te werken, te bezitten of ter beschikking te stellen.⁴⁷ Bijgevolg is het onopzettelijk en onbewust bezitten van dergelijke instrumenten geen constitutief element van het misdrijf. Ook het louter bezitten van een programma dat zowel een wettig als een onwettig gebruik mogelijk maakt, is niet noodzakelijk een misdrijf.

Net als bij het misdrijf met betrekking tot hacker tools betekent de term “onrechtmatig” dat het opzettelijke bezit of de opzettelijke terbeschikkingstelling die wordt verantwoord door een academisch⁴⁸, wetenschappelijk of professioneel gebruik, niet strafrechtelijk wordt bestraft.

Afdeling 5. Poging

De poging wordt bestraft met dezelfde straffen als de inbreuk in verband met informaticagegevens zelf.⁴⁹

De poging is echter maar gerealiseerd als de dader niet alleen voorbereidende handelingen maar ook eenduidige uitvoerende handelingen heeft gesteld.⁵⁰

Afdeling 6. Beleid voor de gecoördineerde bekendmaking van kwetsbaarheden en inbreuk in verband met informaticagegevens

Door deel te nemen aan een beleid van gecoördineerde bekendmaking van kwetsbaarheden beschikt de deelnemer in principe over een machtiging om informaticagegevens in het betrokken systeem in te voeren of dit te proberen. Het is inderdaad moeilijk om veiligheidsgebreken op te sporen zonder ten

⁴⁷ O. LEROUX, "La Criminalité informatique", *op. cit.*, blz. 437.

⁴⁸ Bijvoorbeeld de opleiding informatica-beveiliging.

⁴⁹ Art. 550 *ter*, § 6, van het Strafwetboek.

⁵⁰ Zie de uiteenzetting over de poging tot indringing in een informaticasysteem.

minste te proberen gegevens in te voeren of opdrachten uit te voeren die dergelijke gegevens bevatten.

De machtiging om informaticagegevens te wijzigen of te verwijderen (of om dergelijke handelingen te proberen) hangt evenwel af van de manier waarop het beleid voor de gecoördineerde bekendmaking van kwetsbaarheden is opgesteld. Om een inbreuk in verband met informaticagegevens te vermijden, moet de deelnemer de voorwaarden van het beleid omtrent het wijzigen en verwijderen van informaticagegevens strikt naleven.

Naargelang de inhoud van het beleid voor de gecoördineerde bekendmaking van kwetsbaarheden en de naleving van deze voorwaarden door de deelnemer zal er al dan niet sprake zijn van een misdrijf betreffende een inbreuk in verband met informaticagegevens.⁵¹

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 zijn deelname aan een beleid voor de bekendmaking van kwetsbaarheden. Die handelingen zijn niet ongeoorloofd, zolang ze verantwoord zijn door legitieme doeleinden met betrekking tot het opsporen van kwetsbaarheden met de toestemming van de organisatie van de verantwoordelijke van het betrokken informaticasysteem, en dus niet onrechtmatig worden gesteld.

Niettemin zal de deelnemer ook hier moeten bewijzen dat hij concreet deelneemt aan een bestaand beleid voor de bekendmaking van kwetsbaarheden en dat dat beleid duidelijk identificeerbaar is. De loutere intentie om hypothetisch en in het algemeen aan een dergelijk beleid deel te nemen, volstaat niet.

E. Valsheid in informatica en informaticabedrog

Afdeling 1. Valsheid in informatica⁵² en het gebruik van valse stukken in informatica⁵³

Artikel 210*bis* van het Strafwetboek bestraft de valsheid die erin bestaat gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem, in te voeren in een informaticasysteem, te wijzigen, te wissen, of met enig ander technologisch middel de mogelijke aanwending van gegevens in een informaticasysteem te veranderen, waardoor de juridische draagwijdte van dergelijke gegevens verandert.⁵⁴

⁵¹ En dit misdrijf kan, in voorkomend geval, gepaard gaan met verzwarende omstandigheden.

⁵² Art. 210 *bis*, § 1.

⁵³ Art. 550 *bis*, § 4.

⁵⁴ Art. 210*bis*, § 1, van het Strafwetboek.

Deze bepaling bestraft enerzijds ook het gebruik van gegevens verkregen door valsheid in informatica, terwijl men weet dat deze gegevens vals zijn⁵⁵, en anderzijds de poging tot het plegen van valsheid in informatica⁵⁶.

1. Materiële constitutieve elementen

1.1. Verdraaien van de waarheid op een van de manieren bepaald in de wet (invoeren, wijzigen of verwijderen van gegevens)

Valsheid is niet bij wet bepaald, maar de rechtspraak heeft verduidelijkt dat valsheid een verdraaiing van de waarheid inhoudt die rechten kan doen ontstaan tegenover derden waarvan laatstgenoemden in de praktijk onmogelijk de juistheid kunnen nagaan. Het kan bijvoorbeeld gaan om het aanmaken en gebruiken van een vals e-mailadres op naam van een derde persoon, een valse online verkoopadvertentie of een vals profiel op een sociaal netwerk. Gegevens die kunnen worden vervalst moeten dus een juridische draagwijdte hebben en zich aan de openbare trouw opdringen.⁵⁷

Het kan gaan om informaticabestanden die zijn opgeslagen op de harde schijf van een terminal of op een optische of digitale drager (op voorwaarde dat deze wordt uitgevoerd op een systeem) of nog, om gegevens die in een netwerk worden overgedragen. De vervalsing van een papieren document waarop informaticagegevens afgedrukt zijn, valt daarentegen onder valsheid in geschrifte.⁵⁸

1.2. Wijzigen van de juridische draagwijdte van de gegevens

Opdat het misdrijf voltrokken zou zijn, moet de manipulatie van de gegevens hebben geleid tot een wijziging van de juridische draagwijdte ervan. De juridische draagwijdte stemt overeen met de gewijzigde gegevens in hun geheel en niet met een eenheid. De wijziging kan betrekking hebben op de informaticagegevens zelf of op de gedachte die ze uitdrukken.

De parlementaire werkzaamheden vermelden bijvoorbeeld het namaken of vervalsen van kredietkaarten⁵⁹ en digitale contracten of het invoeren van een vals kredietkaartnummer in een informaticasysteem.

2. Moreel element

Het misdrijf vereist een bedrieglijk opzet of het oogmerk om te schaden.⁶⁰ Dit bijzonder opzet wordt verantwoord door het feit dat valsheid in informatica wordt gelijkgesteld met de andere categorieën van valsheid. Het bedrieglijk opzet bestaat in de wil om zichzelf of iemand anders een onrechtmatig

⁵⁵ Art. 210bis, § 2, van het Strafwetboek.

⁵⁶ Art. 210bis, § 3, van het Strafwetboek.

⁵⁷ *Parl.St.*, Kamer, 1999-2000, nr. 0213/001, blz. 10.

⁵⁸ Art. 194 e.v. van het Strafwetboek.

⁵⁹ Het betreft met name het bestraffen van "skimming", m.a.w. het illegaal kopiëren van de gegevens van een betaalkaart, dat vaak misdrijven m.b.t. valsheid in informatica, informaticabedrog en ongeoorloofde indringing in een derde informaticasysteem omvat.

⁶⁰ Zie artikel 193 van het Strafwetboek.

gewin of voordeel te verschaffen. Het oogmerk om te schaden betreft de wil om een natuurlijk of rechtspersoon schade te berokkenen.

Vergissingen, nalatigheden of onvoorzichtigheden alleen volstaan dus niet om een misdrijf van valsheid in informatica te vormen.

Ook het aanmaken of gebruiken van een vals stuk in informatica wordt niet strafrechtelijk bestraft als de dader handelt met het oog op wetenschappelijke, professionele of onderwijsdoeleinden.

3. Poging

De poging om valsheid in informatie te plegen wordt ook strafbaar gesteld, zonder dat er dus effectief schade moet zijn berokkend.

Niettemin houdt de poging zowel voorbereidende handelingen in als uitvoerende handelingen die geen twijfel laten bestaan over het misdadig opzet van de dader.⁶¹

Afdeling 2. Informaticabedrog

Artikel 504^{quater} van het Strafwetboek stelt degene strafbaar die, met bedrieglijk opzet, beoogt een onrechtmatig economisch voordeel voor zichzelf of voor een ander te verwerven, door gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem, in een informaticasysteem in te voeren, te wijzigen of te wissen of met enig technologisch middel de normale aanwending van gegevens in een informaticasysteem te veranderen.

1. Materiële constitutieve elementen

1.1. Manipuleren van gegevens

Het misdrijf impliceert het invoeren, wijzigen⁶² of verwijderen van gegevens in een informaticasysteem of het gebruik van eender welke technologie om de normale aanwending van gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem te veranderen (zie *supra* valsheid in informatica).

1.2. Nastreven van een onrechtmatig economisch voordeel

Het misdrijf vereist niet dat het beoogde onrechtmatig economisch voordeel concreet verworven wordt, maar het louter nastreven van een dergelijk doel, ook al is dat doel uiteindelijk niet bereikt. Informaticabedrog is een misdrijf waarbij een louter risico volstaat of "formeel" misdrijf, waarbij enkel moet worden aangetoond dat de gegevensverwerking in oorzakelijk verband staat met het nastreven

⁶¹ Zie de poging tot indringing in een informaticasysteem.

⁶² Bijvoorbeeld het wijzigen van het saldo op een bankrekening.



van een onrechtmatig economisch voordeel. Het economisch voordeel⁶³ kan rechtstreeks of onrechtstreeks zijn en verschillende vormen aannemen: materiële goederen, immateriële goederen, dienstverlening. Het kan ten voordele van de dader of van een andere persoon zijn.

2. Moreel element

Informaticabedrog veronderstelt niet alleen dat de dader het misdrijf wetens en willens pleegde, maar ook dat hij een bijzonder opzet nastreefde, namelijk een bedrieglijk opzet om voor zichzelf of voor iemand anders een onrechtmatig economisch voordeel te verwerven.

3. Poging

De poging tot informaticabedrog wordt ook bestraft.⁶⁴

Ook hier zal de poging pas bewezen zijn als het openbaar ministerie aantoont dat de dader niet alleen voorbereidende handelingen maar ook eenduidige uitvoerende handelingen heeft gesteld.

Afdeling 3. Beleid voor de gecoördineerde bekendmaking van kwetsbaarheden, valsheid in informatica en informaticabedrog

Aangezien valsheid in informatica een bedrieglijk opzet of het oogmerk om te schaden vereist, sluit de deelname aan een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden dit misdrijf in hoofde van de deelnemer uit. In dezelfde zin loopt de deelnemer aan een beleid voor gecoördineerde bekendmaking of een beloningsprogramma voor kwetsbaarheden in principe geen gevaar strafrechtelijk te worden vervolgd voor informaticabedrog, aangezien er geen sprake is van bedrieglijk opzet in hoofde van de deelnemer.

F. Misdrijven betreffende het geheim van communicatie

Afdeling 1. Misdrijven betreffende het geheim van niet voor het publiek toegankelijke communicatie en gegevens van een informaticasysteem

Artikel 314*bis* van het Strafwetboek bestraft eenieder die, opzettelijk en met behulp van enig toestel, niet voor het publiek toegankelijke communicatie, waaraan hij niet deelneemt, onderschept of doet onderscheppen, er kennis van neemt of doet van nemen, opneemt of doet opnemen, zonder de toestemming van alle deelnemers aan die communicatie.⁶⁵

⁶³ Artikel 504*quater* vereiste voorheen dat de dader voor zichzelf of voor een ander een bedrieglijk vermogensvoordeel verwierf, wat niet volledig in overeenstemming was met artikel 8 van het Cybercrimeverdrag van de Raad van Europa: *Parl.St.*, Kamer, 2003-2004, 1284/001, blz. 6 en 8.

⁶⁴ Zie de overwegingen met betrekking tot een poging tot ongeoorloofde indringing.

⁶⁵ Art. 314*bis*, § 1, 1°, van het Strafwetboek.



1. Materieel element

1.1. Onderscheppen, kennismemen van of opnemen met behulp van een toestel

Bij gebrek aan een wettelijke definitie moet het onderscheppen, kennismemen of opnemen van communicatie worden begrepen in de zin van het normale taalgebruik. Eerst en vooral bestaat het onderscheppen erin communicatie die aan iemand anders is gericht, aan iemand anders wordt verstuurd of voor iemand anders is bestemd, onderweg, bij verrassing, op te vangen. Vervolgens betekent het kennismemen van communicatie het op de hoogte zijn van het bestaan en de inhoud van communicatie tussen personen hoewel men niet de bestemming van deze communicatie is. Dit laatste begrip heeft een ruime betekenis en is ook toepasselijk op technische vormen van communicatie, zoals elektronische gegevensoverdracht. Tot slot betreft het opnemen het vastleggen van gegevens op een lokale materiële drager of op een materiële drager op afstand⁶⁶, om deze later te kunnen gebruiken.

De strafbaarstelling van het onderscheppen van communicatie heeft tot doel om naast de dader van het misdrijf ook de opdrachtgever ervan te bestraffen.⁶⁷

De bepaling verduidelijkt nog dat het onderscheppen⁶⁸, kennismemen van of opnemen moet gebeuren met behulp van enig toestel⁶⁹. Dat is een ruime formulering, maar ze houdt noodzakelijkerwijs het gebruik van een technisch hulpmiddel in. Zo niet zijn de feiten niet strafbaar. Aan deze vereiste lijkt te zijn voldaan zodra een informaticamanipulatie wordt uitgevoerd of een programma wordt gebruikt.⁷⁰

1.2. Niet voor het publiek toegankelijke communicatie waaraan men niet deelneemt

Artikel 314*bis* van het Strafwetboek verduidelijkt voortaan dat de bedoelde communicatie “niet voor het publiek toegankelijke communicatie” is en niet langer “privécommunicatie of -telecommunicatie”.⁷¹ Dit begrip lijkt net als voorheen te kunnen worden geïnterpreteerd in functie

⁶⁶ Bijvoorbeeld via een cloudopslagdienst.

⁶⁷ *Parl.St.*, Senaat, 1992-1993, nr. 843/1, blz. 8-9.

⁶⁸ De bepaling vereist voortaan niet meer dat de communicatie “tijdens de overbrenging ervan” wordt onderschept. De parlementaire werkzaamheden verklaren deze aanpassing door het feit dat de nieuwe ontwikkelingen op informaticagebied het vaak onmogelijk maken om precies uit te maken wanneer communicatie nog in “overbrenging” is, dan wel reeds afgeleverd. Het is immers moeilijk te bepalen of een ongelezen e-mail moet worden beschouwd als afgeleverde communicatie of als communicatie die wordt overgebracht. *Parl.St.*, Kamer, 2015-2016, nr. 1966/001, blz. 54.

⁶⁹ *Parl.St.*, Senaat, 1992-1993, nr. 843/1, blz. 6.

⁷⁰ Omgekeerd valt het louter rechtstreeks op een computerscherm weergeven van een e-mail of een webpagina, die open worden gelaten en waarop geen enkele manipulatie wordt uitgevoerd, niet onder het misdrijf.

⁷¹ Artikel 32 van de wet van 25 december 2016 houdende diverse wijzigingen van het Wetboek van strafvordering en het Strafwetboek, met het oog op de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische en telecommunicaties en tot oprichting van een gegevensbank stemafdrukken, *BS*

van de context en de bedoelingen van de deelnemers aan de communicatie.⁷² Het niet voor het publiek toegankelijke karakter houdt in dat de communicatie niet bestemd is om door andere personen dan de correspondenten van de communicatie te worden gehoord.⁷³ Het al dan niet beroepsmatige karakter van een communicatie heeft in principe geen gevolgen voor het beoordelen van de niet voor het publiek toegankelijke aard.⁷⁴

De communicatie betreft met name de elektronische gegevensoverdracht in computers en computernetwerken.⁷⁵ Hiermee worden met name e-mails bedoeld.

De bepaling stelt enkel de personen strafbaar die niet deelnemen aan de communicatie. Omgekeerd pleegt de persoon die deelneemt aan een niet voor het publiek toegankelijke communicatie en die deze communicatie opneemt, zelfs zonder dat de andere deelnemers dat weten, geen misdrijf in de zin van artikel 314*bis* van het Strafwetboek.

1.3. Ontbreken van de toestemming van de deelnemers

Om aan het misdrijf te ontkomen, moet men vooraf de toestemming hebben gekregen van alle deelnemers aan de elektronische communicatie en niet alleen van sommigen onder hen. De toestemming van de deelnemers, die voortvloeit uit een geheel van omstandigheden, kan uitdrukkelijk of stilzwijgend zijn, voor zover ze duidelijk is. Sommige auteurs voegen hieraan toe dat deze toestemming noodzakelijkerwijs op specifieke en individuele wijze moet zijn gegeven, en niet mag zijn afgeleid uit een voorafgaand akkoord dat bijvoorbeeld is opgenomen in een clause van een arbeidsovereenkomst of van een huishoudelijk reglement. De toestemming zou tevens op eerlijke wijze moeten zijn verkregen en met inachtneming van het eventuele aan de deelnemers meegedeelde doel.

2. Moreel element

Het misdrijf vereist uitdrukkelijk dat de dader opzettelijk, dat wil zeggen wetens en willens, handelt. De parlementaire werkzaamheden vermeldden duidelijk dat louter toeval of onbescheidenheid niet

van 17 januari 2017, blz. 2738. De parlementaire werkzaamheden verantwoordden deze wijziging als een terminologische aanpassing, rekening houdend met de wijzigingen in de artikelen 90*ter* e.v. van het Wetboek van strafvordering.

⁷² *Parl.St.*, Senaat, 1992-1993, nr. 843/1, blz. 6. De parlementaire werkzaamheden lichten ook toe dat het begrip "niet voor het publiek toegankelijke communicatie" betrekking heeft op communicatie of elektronische communicatie die zich in de privé sfeer afspeelt. Het is dus een overkoepelend begrip dat ook de vroegere termen "privécommunicatie of telecommunicatie" omvat: *Parl.St.*, Kamer, 2015-2015, nr. 1966/001, blz. 53.

⁷³ *Parl.St.*, Senaat, 1992-1993, nr. 843/1, p. 7. Commissie voor de bescherming van de persoonlijke levenssfeer, aanbeveling nr. 08/2012 van 2 mei 2012 betreffende de controle door de werkgever op het gebruik van elektronische communicatie-instrumenten op de werkvloer, www.privacycommission.be.

⁷⁴ *Parl.St.*, Senaat, 1992-1993, nr. 843/1, blz. 8 en nr. 843/2, blz. 10 en 36.

⁷⁵ In die zin: *Parl.St.*, Senaat, 1992-1993, nr. 843/1, blz. 7.

volstaat om van een misdrijf te spreken.⁷⁶ Bijgevolg is de louter toevallige ontdekking van niet voor het publiek toegankelijke communicatie niet strafbaar. Wie opzettelijk maar louter uit nieuwsgierigheid handelt, begaat evenwel een misdrijf.⁷⁷ Zo is bijvoorbeeld het toevallig kennismaken van de inhoud van communicatie door een technicus tijdens de controle van de goede werking van een informaticasysteem niet strafbaar, behalve indien hij opzettelijk uit nieuwsgierigheid heeft gehandeld.

Afdeling 2. Voorbereidende handelingen

1. Opstellen van een toestel

1.1. Materieel element

Het Strafwetboek stelt degene strafbaar die enig toestel opstelt of doet opstellen dat het ongeoorloofd onderscheppen, kennismaken of opnemen van communicatie mogelijk maakt.⁷⁸ Het toestel wordt immers niet noodzakelijk door of in opdracht van dezelfde personen geplaatst en gebruikt.⁷⁹

1.2. Moreel element

Het misdrijf vereist dat de dader handelt met het opzet een ongeoorloofde onderschepping, kennismaking of opname te plegen.

2. Ter beschikking stellen van een instrument

2.1. Materiële constitutieve elementen

De wetgever bestraft degene die, onrechtmatig, een instrument, met inbegrip van informaticagegevens, dat hoofdzakelijk is ontworpen of aangepast om het ongeoorloofd onderscheppen van communicatie mogelijk te maken, bezit, produceert, verkoopt, verkrijgt met het oog op het gebruik ervan, invoert, verspreidt of op enige andere manier ter beschikking stelt.⁸⁰

Onder het begrip “instrument” worden de toegangsmiddelen of andere tools verstaan die ontworpen zijn om bijvoorbeeld gegevens te wijzigen of te vernietigen, of om binnen te dringen in de werking van systemen, zoals virusprogramma’s, ofwel programma’s die ontworpen of aangepast zijn om binnen te dringen in informaticasystemen.⁸¹

⁷⁶ *Parl.St.*, Senaat, 1992-1993, nr. 843/1, blz. 6.

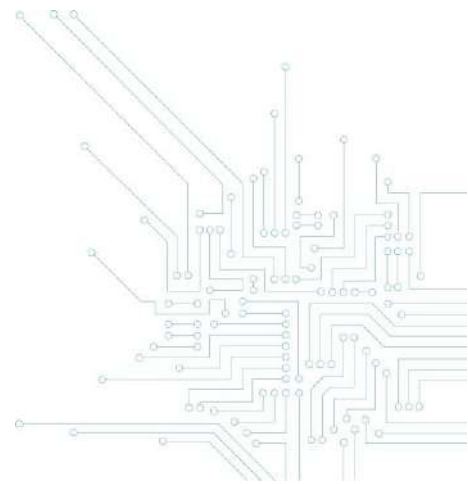
⁷⁷ *Parl.St.*, Senaat, 1992-1993, nr. 843/1, blz. 6.

⁷⁸ Art. 314bis, § 1, 2°, van het Strafwetboek.

⁷⁹ *Parl.St.*, Senaat, 1992-1993, nr. 843/1, blz. 9.

⁸⁰ Art. 314bis, §2bis, van het Strafwetboek.

⁸¹ *Parl.St.*, Kamer, 2003-2004, nr. 1284/001, blz. 6.



2.2. Moreel element

Zoals bij het ter beschikking stellen van middelen om een ongeoorloofde indringing mogelijk te maken, moet de dader wetens en willens een dergelijk instrument hebben ontwikkeld, in zijn bezit hebben gehad of ter beschikking hebben gesteld. Hij moet er dus van op de hoogte zijn geweest dat het strafbare instrument hoofdzakelijk werd ontworpen of aangepast om het ongeoorloofd onderscheppen, opnemen en kennismaken van communicatie mogelijk te maken.

De term “onrechtmatig” betekent niettemin dat het bezitten of ter beschikking stellen van een dergelijk instrument voor legitieme doeleinden, zoals wetenschappelijke of professionele doeleinden op het gebied van de beveiliging van communicatiesystemen, niet strafbaar is.

Afdeling 3. Helen van onrechtmatig verkregen communicatie

Het Strafwetboek bestraft degene die wetens de inhoud van niet voor het publiek toegankelijke communicatie of van gegevens van een informaticasysteem die onwettig onderscheept of opgenomen zijn of waarvan onwettig kennisgenomen is, onder zich houdt, aan een andere persoon onthult of verspreidt, of wetens enig gebruik maakt van een op die manier verkregen inlichting.⁸²

1. Materieel element

1.1. Inhoud van niet voor het publiek toegankelijke communicatie of van gegevens van een informaticasysteem die onwettig onderscheept of opgenomen zijn of waarvan onwettig kennisgenomen is

De persoon die bij vergissing of toevallig communicatie ontvangt die niet voor hem bestemd was, pleegt geen misdrijf.

1.2. Onder zich houden, aan een andere persoon onthullen of verspreiden of op enige manier gebruiken

Wat deze begrippen betreft, wordt verwezen naar de toelichting over het helen van onrechtmatig verkregen informaticagegevens.

2. Moreel element

Men moet “wetens” hebben gehandeld, dat wil zeggen opzettelijk en met kennis van zaken over de onwettigheid van de verkregen informatie.

⁸² Art. 314bis, § 2, van het Strafwetboek.



Afdeling 4. Poging

De poging tot het ongeoorloofd onderscheppen van niet voor het publiek toegankelijke communicatie wordt eveneens bestraft.⁸³

Hiervoor moet worden bewezen dat voorbereidende en uitvoerende handelingen zijn gesteld die geen twijfel laten over het misdadig opzet van de dader.

Afdeling 5. Geheimhouding van elektronische communicatie

Artikel 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie voorziet in strafrechtelijke sancties voor verschillende gedragingen die in strijd zijn met de geheimhouding van elektronische communicatie, die beschermd wordt door artikel 124 van dezelfde wet.

Deze verschillende sancties zijn gericht op het waarborgen van het vertrouwelijke karakter van de informatie die over een elektronische-communicatienetwerk wordt verzonden.⁸⁴

1. Materiële constitutieve elementen

1.1. Toestemming van de direct of indirect betrokken personen

Ondanks de in de wet gehanteerde ruime formulering, die doet veronderstellen dat alle personen die direct of indirect betrokken zijn bij de communicatie en de inhoud ervan hun toestemming zouden moeten geven⁸⁵, lijkt het niettemin redelijker ervan uit te gaan dat enkel de personen aan wie de communicatie rechtstreeks of onrechtstreeks gelinkt is, moeten instemmen met de kennisneming, namelijk de afzender en de ontvanger(s). Wat verbindingsgegevens of gegevens van geraadpleegde webpagina's betreft, volstaat het de toestemming van de betrokken gebruiker te verkrijgen.

1.2. Met opzet kennisnemen door iemand van het bestaan van informatie van alle aard die via elektronische weg is verstuurd en die niet persoonlijk voor hem bestemd is⁸⁶

1.2.1. Via elektronische weg verstuurde informatie

In de wet van 13 juni 2005 wordt het begrip "elektronische communicatie" onrechtstreeks gedefinieerd via de definitie van *elektronische-communicatiedienst*, zijnde "een gewoonlijk tegen vergoeding aangeboden dienst die geheel of hoofdzakelijk bestaat in het overbrengen, waaronder

⁸³ Art. 314bis, § 3, van het Strafwetboek. Zie Corr. Brussel, 8 januari 2008, *J.T.*, 2008, blz. 337, voor een voorbeeld van een poging tot het onderscheppen van communicatie d.m.v. een "keylogger", m.a.w. spyware die de activiteit (toetsaanslagen) van een computer registreert en doorstuurt naar een derde.

⁸⁴ *Parl.St.*, Senaat, 2004-2005, nr. 1425-1426/01, blz. 76.

⁸⁵ Commissie voor de bescherming van de persoonlijke levenssfeer, advies nr. 8/2004 van 14 juni 2004 over het voorontwerp van wet betreffende de elektronische communicatie, blz. 7, www.privacycommission.be: de CBPL vroeg zich af of een persoon die in het bericht zelf wordt vermeld volgens de wet als zijnde indirect betrokken bij de communicatie moest worden beschouwd, wat veel verder ging dan de Europese tekst.

⁸⁶ Art. 124, eerste lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie.



schakel- en routeringsverrichtingen, van signalen via elektronische-communicatienetwerken (...)" en van *elektronische-communicatienetwerk*, zijnde "de transmissiesystemen en, in voorkomend geval, de schakel- of routeringsapparatuur en andere middelen, waaronder netwerkelementen die niet actief zijn, die het mogelijk maken signalen over te brengen via draad, radiogolven, optische of andere elektromagnetische middelen (...)"⁸⁷. In het Wetboek van economisch recht wordt "elektronische post" gedefinieerd als een "tekst-, spraak-, geluids- of beeldbericht dat over een openbaar communicatienetwerk wordt verzonden en in het netwerk of in de eindapparatuur van de ontvanger kan worden opgeslagen tot het door de afnemer wordt opgehaald".⁸⁸

Het begrip "elektronische communicatie" omvat telefonische communicatie, e-mails, sms'en, berichten die worden verstuurd via een draadloos netwerk of de uitwisseling van cellulaire gegevens, verbindingen met een netwerk of met een informaticasysteem. Dit begrip omvat dus e-mails en internetverbindinggegevens die het mogelijk maken de geraadpleegde websites te identificeren.

De kennisneming betreft de informatie in haar geheel, met inbegrip van de inhoud van elektronische post.⁸⁹ De persoon die heeft kennisgenomen van het bestaan van elektronische post en er gebruik van heeft gemaakt, heeft immers noodzakelijkerwijs gelijktijdig kennisgenomen van de inhoud ervan. De kennisneming en het gebruik van de inhoud van een e-mail hangen samen met de kennisneming en het gebruik van het bestaan van die elektronische post.⁹⁰ We kunnen ervan uitgaan dat artikel 124 van de wet van 15 juni 2005 dus een belemmering vormt voor de kennisneming van de inhoud van elektronische communicatie.

1.2.2. Informatie van alle aard die niet persoonlijk voor hem bestemd is

De kennisneming van informatie van alle aard die persoonlijk bestemd is voor degene die ervan kennisneemt, vormt geen schending van artikel 124, eerste lid, van de wet van 13 juni 2005.

1.3. Met opzet identificeren van de personen die bij het versturen van de informatie en de inhoud ervan betrokken zijn

Artikel 124, tweede lid, verbiedt de identificatie van de personen die zowel bij het versturen van de informatie als bij de inhoud ervan betrokken zijn. Dit betreft zowel de identiteitsgegevens van de afzender, van de ontvanger(s) van de berichten als die van de bij de inhoud betrokken personen (bijvoorbeeld deze vermeld in de e-mail).

⁸⁷ Art. 2, 3° en 5°, van de wet van 13 juni 2005 betreffende de elektronische communicatie, *BS* van 20 juni 2005, blz. 28070.

⁸⁸ Wet van 15 december 2013 houdende invoeging van Boek XII, "Recht van de elektronische economie", in het Wetboek van economisch recht, en houdende invoeging van de definities eigen aan Boek XII en van de rechtshandhabingsbepalingen eigen aan Boek XII, in de Boeken I en XV van het Wetboek van economisch recht.

⁸⁹ Cass., 1 okt. 2009, C.08.0064.N, www.cass.be. De rechtsleer twijfelde of ervan moest worden uitgegaan dat artikel 124 niet alleen betrekking had op het bestaan van informatie, maar ook op de inhoud van de informatie zelf. Zie Commissie voor de bescherming van de persoonlijke levenssfeer, advies nr. 8/2004 van 14 juni 2004 over het voorontwerp van wet betreffende de elektronische communicatie, blz. 7, www.privacycommission.be: "Dit artikel heeft als doel de communicaties (zowel de inhoud als de verkeersgegevens) zodanig te beschermen dat er geen andere persoon kennis van kan nemen noch kan manipuleren dan de partijen die aan de communicatie hebben deelgenomen".

⁹⁰ *Ibidem*.

1.4. Met opzet kennisnemen van gegevens inzake elektronische communicatie en met betrekking tot een andere persoon⁹¹

Gegevens inzake elektronische communicatie zijn gegevens die via netwerken worden verzonden, zoals de e-mailadressen van afzender en ontvanger, het tijdstip van verzending en ontvangst, de routeringsgegevens, de grootte van het bericht, de aanwezigheid van bijlagen enz.⁹²

De kennisneming bestaat in het op de hoogte zijn van het bestaan en de inhoud van gegevens inzake elektronische communicatie tussen personen hoewel men niet de ontvanger van deze communicatie is.

1.5. Wijzigen, schrappen, kenbaar maken, opslaan of op enige wijze gebruikmaken van de informatie, identificatie of gegevens die met of zonder opzet werden verkregen⁹³

Het is verboden de informatie, de identificatie of de gegevens die met opzet maar ook toevallig werden verkregen te wijzigen, te schrappen, kenbaar te maken, op te slaan of er enig gebruik van te maken.

2. Moreel element

Deze bepaling houdt in dat de strafbaar gestelde handelingen met opzet moeten worden verricht door de dader van het misdrijf. Als wordt vastgesteld dat de kennisneming van elektronische communicatie toevallig heeft plaatsgevonden, ontbreekt het intentionele karakter van de ontdekking en is artikel 124 van de wet van 13 juni 2005 niet van toepassing.⁹⁴ Bijgevolg moet een onderscheid worden gemaakt tussen de actieve en de louter toevallige kennisneming van elektronische communicatie.

3. Uitzonderingen bepaald in artikel 125 van de wet

Artikel 125 van de wet van 13 juni 2005 betreffende de elektronische communicatie voorziet in een aantal uitzonderingen op de geheimhouding van communicatie bedoeld in artikel 124 van dezelfde wet en in artikel 314*bis* van het Strafwetboek. Deze bepaling maakt het onder andere⁹⁵ mogelijk om de in principe verboden handelingen te stellen wanneer ze nodig zijn om de goede werking van het netwerk na te gaan en om de goede uitvoering van een elektronische-communicatiedienst te garanderen. Door de algemene bewoordingen van de wet lijkt deze bepaling zowel toepasselijk te zijn op een openbaar elektronische-communicatienetwerk als op een privénetwerk.

⁹¹ Art. 124, derde lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie.

⁹² Arbh. Brussel, 10 februari 2004, R.G. 44002, www.juridat.be.

⁹³ Art. 124, vierde lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie.

⁹⁴ Arbh. Bergen, 8 dec. 2010, *JLMB*, 2011, blz. 715; *Chron. D.S.*, 2011, blz. 399; Arbh. Brussel, 4 december 2007, *J.T.T.*, 2008, blz. 179; Arbrb. Luik, 19 maart 2008, RG 360.454, www.juridat.be.

⁹⁵ Art. 125, § 1, 1°, van de wet van 13 juni 2005 betreffende de elektronische communicatie voorziet ook in de mogelijkheid van een afwijking wanneer de wet het stellen van de aangeklaagde handelingen toestaat of oplegt. Volgens de Privacycommissie zou artikel 16 van de wet van 3 juli 1978 betreffende de arbeidsovereenkomsten een wettelijke basis vormen mits bepaalde voorwaarden worden nageleefd.



Voor zover dit kan worden verantwoord door strikt technische maatregelen is het dus mogelijk om de handelingen bedoeld in artikel 124 te stellen. De informatie inzake elektronische communicatie die bij deze gelegenheid ontdekt wordt, mag echter niet voor andere doeleinden worden gebruikt dan het nagaan van de goede werking van het netwerk.

4. Bedrieglijke elektronische communicatie⁹⁶

1. Materiële constitutieve elementen

Het gaat om het op bedrieglijke wijze tot stand brengen van elektronische communicatie door middel van een elektronische-communicatienetwerk.

2. Moreel element

Naast het wetens en willens handelen impliceert dit misdrijf ook dat de dader een bijzonder opzet had, namelijk zichzelf of een andere persoon wederrechtelijk een voordeel verschaffen.

3. Poging en voorbereidende handelingen⁹⁷

De wet stelt ook de persoon strafbaar die op bedrieglijke wijze elektronische communicatie tot stand probeert te brengen of enig toestel opstelt dat bestemd is om dergelijke communicatie tot stand te brengen.

Net als de andere pogingen vereist ook deze poging dat wordt bewezen dat de dader voorbereidende en eenduidige uitvoerende handelingen heeft gesteld.

5. Ongeoorloofd gebruik van een elektronische-communicatienetwerk of -dienst⁹⁸

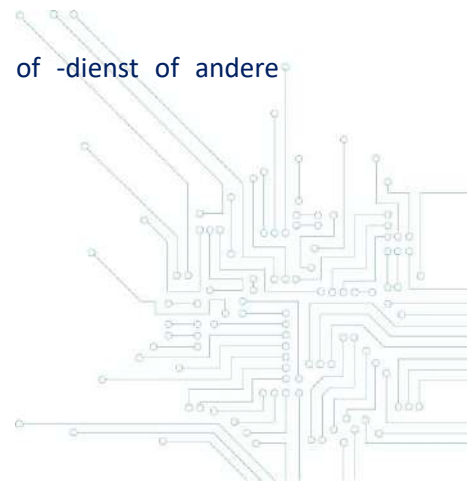
1. Materiële constitutieve elementen

De wet bestraft de persoon die een elektronische-communicatienetwerk of -dienst of andere elektronische communicatiemiddelen gebruikt met een ongeoorloofd doel.

⁹⁶ Art. 145, § 3, 1°, van de wet van 13 juni 2005 betreffende de elektronische communicatie.

⁹⁷ Art. 145, § 3, 3°, van de wet van 13 juni 2005 betreffende de elektronische communicatie.

⁹⁸ Art. 145, § 3bis, van de wet van 13 juni 2005 betreffende de elektronische communicatie.



2. Moreel element

Het misdrijf houdt in dat de dader overlast wil veroorzaken aan zijn correspondent of schade wil berokkenen.

3. Poging en voorbereidende handelingen

De wet stelt ook de persoon strafbaar die enig toestel opstelt dat bestemd is om ongeoorloofd gebruik te maken van een elektronische-communicatienetwerk of -dienst, alsook de poging hiertoe.

Voor de poging moet worden aangetoond dat de dader voorbereidende handelingen en eenduidige uitvoerende handelingen heeft gesteld.

Afdeling 6. Beleid voor de gecoördineerde bekendmaking van kwetsbaarheden en communicatie

Het is de deelnemer niet toegestaan opzettelijk, met enig toestel, niet voor het publiek toegankelijke communicatie te onderscheppen, ervan kennis te nemen of op te nemen.⁹⁹ Dit is overigens niet noodzakelijk bij de uitvoering van een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden.

Het onderscheppen, kennisnemen of opnemen van niet voor het publiek toegankelijke communicatie door de deelnemer is evenwel geen misdrijf als dit ofwel toevallig, ofwel met de toestemming van alle deelnemers aan de betrokken communicatie¹⁰⁰, ofwel met de deelname van de deelnemer zelf aan de communicatie gebeurt.

Ook kan een deelnemer, zonder een misdrijf te plegen, een toestel opstellen of doen opstellen dat het mogelijk maakt om niet voor het publiek toegankelijke communicatie te onderscheppen, ervan kennis te nemen of op te nemen voor zover hij handelt zonder de bedoeling om het betrokken toestel te gebruiken voor bovengenoemde doeleinden of met de toestemming van alle deelnemers, ofwel zelf deelneemt aan de communicatie.

Bovendien kan een deelnemer een instrument dat het onderscheppen, kennisnemen of opnemen van niet voor het publiek toegankelijke communicatie mogelijk maakt, uitwerken, bezitten of ter beschikking stellen van een andere deelnemer. Dit is evenwel alleen gewettigd in het kader van een

⁹⁹ Art. 314*bis* van het Strafwetboek.

¹⁰⁰ Hoewel dit in veel situaties niet vanzelfsprekend is, is het niet uitgesloten dat de deelnemer in het kader van het beleid voor gecoördineerde bekendmaking beschikt over de toestemming van de deelnemers aan de communicatie.

werkelijke deelname aan een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden. Dit instrument kan immers aantonen dat kwetsbaarheden in het informaticasysteem kunnen leiden tot een ongeoorloofde kennisneming van communicatie.

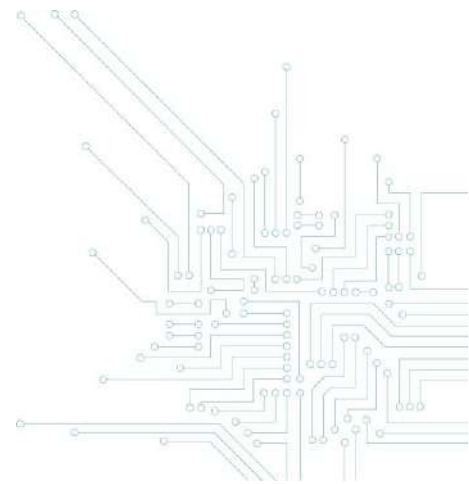
De opzettelijke poging om niet voor het publiek toegankelijke communicatie te onderscheppen, op te nemen of er kennis van te nemen is daarentegen slechts verantwoord zijn in het kader van de uitvoering van een beleid voor gecoördineerde bekendmaking als de deelnemer over de toestemming van alle deelnemers beschikt of zelf deelneemt aan de communicatie.

Als de deelnemer redelijkerwijs niet kon weten dat de inhoud van niet voor het publiek toegankelijke communicatie of van gegevens van een informaticasysteem onwettig werd verkregen, kan hij deze gebruiken, bijhouden, onthullen of verspreiden. Omgekeerd moet de deelnemer die weet dat dergelijke informatie onwettig werd verkregen, zich er strikt van onthouden deze te helen in het kader van zijn deelname aan een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden.

Gelet op de goede bedoelingen van de deelnemer moet deze in principe geen bedrieglijke elektronische communicatie tot stand brengen of een elektronische-communicatienetwerk of -dienst op ongeoorloofde wijze gebruiken.

Tot slot heeft een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden zeker niet tot doel om opzettelijk kennis te nemen van informatie, van de identiteit van communicerende personen of van gegevens inzake elektronische communicatie of deze te wijzigen. Als de deelnemer deze handelingen moet stellen, gebeurt dit toevallig of met de toestemming van alle betrokken deelnemers, ofwel is de communicatie persoonlijk voor hem bestemd. De uitvoering van een beleid voor gecoördineerde bekendmaking heeft daarentegen tot doel de vertrouwelijkheid van de door de verantwoordelijke organisatie uitgewisselde elektronische communicatie te bevorderen.

Volgens ons kan de deelnemer aan een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden zich eventueel beroepen op de toepassing van artikel 125 van de wet van 13 juni 2005 betreffende de elektronische communicatie, dat het mogelijk maakt af te wijken van de geheimhouding van elektronische communicatie. De handelingen die door een deelnemer worden gesteld in het kader van een beleid voor gecoördineerde bekendmaking kunnen tot doel hebben de goede werking van een elektronische-communicatienetwerk of -dienst na te gaan, met inbegrip van de veiligheid ervan.



G. Naleving van andere wettelijke bepalingen

Naast de bepalingen inzake cybercriminaliteit moeten de deelnemers aan een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden rekening houden met andere wettelijke bepalingen, waaronder de wetgeving betreffende de verwerking van persoonsgegevens.¹⁰¹

Een beleid voor gecoördineerde bekendmaking heeft niet tot doel om intentioneel persoonsgegevens te verwerken. De verantwoordelijke organisatie zal echter hoogstwaarschijnlijk persoonsgegevens moeten verwerken als verwerkingsverantwoordelijke of als verwerker. Het is dus mogelijk dat de deelnemer, zelfs toevallig, persoonsgegevens moet verwerken die worden opgeslagen, verwerkt of overgedragen in het betrokken informaticasysteem. Het kan ook nodig zijn dat een deelnemer, in het kader van zijn onderzoek naar kwetsbaarheden, persoonsgegevens verwerkt om het bestaan van een kwetsbaarheid aan te tonen.

Afdeling 1. Begrippen in verband met persoonsgegevens

1. Persoonsgegevens

De AVG verstaat onder persoonsgegevens alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Gegevens zijn identificeerbaar indien ze het mogelijk maken om een natuurlijke persoon direct of indirect te identificeren, met name aan de hand van een identicator zoals een naam, een identificatienummer, locatiegegevens, een online identicator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.¹⁰² 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 identicator, IP-adres of nog, locatiegegevens).

2. Verwerking

De verwerking van persoonsgegevens heeft een ruime betekenis en omvat “een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door

¹⁰¹ Europese verordening nr. 2016/679 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (Algemene verordening gegevensbescherming, hierna “AVG”) en tot intrekking van Richtlijn 95/46/EG, alsook de Belgische wetten in dit verband waaronder de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit, BS van 10 januari 2018, blz. 989.

¹⁰² Art. 4, 1), van de AVG.



middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligner of combineren, afschermen, wissen of vernietigen van gegevens”.¹⁰³ Kortom, het begrip “verwerking” omvat nagenoeg alle bewerkingen die betrekking kunnen hebben op persoonsgegevens.

Zo wordt het gewoon verzamelen of raadplegen van persoonsgegevens als een verwerking van deze gegevens beschouwd.¹⁰⁴

3. Verwerkingsverantwoordelijke

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 van persoonsgegevens vaststelt.¹⁰⁵

De hoedanigheid van verwerkingsverantwoordelijke vloeit dus voort uit de bevoegdheid om vast te stellen voor welke doeleinden persoonsgegevens worden verwerkt.

3.1. Bevoegdheid tot vaststelling

De bevoegdheid tot vaststelling betekent voor een entiteit dat ze ervoor kan kiezen persoonsgegevens te verwerken voor haar eigen doeleinden¹⁰⁶. Het begrip “verwerkingsverantwoordelijke” is een functioneel begrip, dat is bedoeld om verantwoordelijkheden toe te kennen aan personen die een feitelijke invloed uitoefenen. Het is dus meer op een feitelijke dan op een formele analyse gebaseerd.¹⁰⁷

In de praktijk dient dus te worden nagegaan waarom een verwerking plaatsvindt en wie concreet beslist heeft om deze uit te voeren.

¹⁰³ Art. 4, 2), van de AVG.

¹⁰⁴ C. DE TERWANGNE, *Vie privée et données à caractère personnel*, hoofdstuk 3.2 Analyse détaillée de la loi de protection des données et de son arrêté royal d'exécution, Brussel, Uitg. Politeia, blz. 23.

¹⁰⁵ Art. 4, 7), van de AVG: wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.

¹⁰⁶ C. DE TERWANGNE, *Vie privée et données à caractère personnel*, hoofdstuk 3.2 Analyse détaillée de la loi de protection des données et de son arrêté royal d'exécution, Brussel, Uitg. Politeia, blz. 26.

¹⁰⁷ Groep van artikel 29, advies 1/2010 over de begrippen “voor de verwerking verantwoordelijke” en “verwerker”, WP 169, blz. 10, (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_nl.pdf)



3.2. Vaststelling van het doel en de middelen

De verwerkingsdoeleinden zijn de doelstellingen van de verwerkingsacties. De middelen zijn de toegepaste technische en organisatorische methoden¹⁰⁸ om de verwerkingsdoeleinden te bereiken. In feite is het de bedoeling om het “waarom” en het “hoe” van de verwerkingsactiviteiten te bepalen.¹⁰⁹

Deze beide elementen moeten voorhanden zijn om als verwerkingsverantwoordelijke te worden beschouwd.

De vaststelling van de middelen moet betrekking hebben op de technische en organisatorische wezenlijke aspecten van de verwerking (bijvoorbeeld, de te verwerken gegevens, de verwerkingsduur of de personen die toegang mogen hebben tot de gegevens).¹¹⁰

4. Verwerker

De verwerker is een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.¹¹¹ De verwerker handelt ten behoeve van de verwerkingsverantwoordelijke door zijn instructies op te volgen, in ieder geval wat het doel van de verwerking en de wezenlijke aspecten van de middelen voor de verwerking betreft.

Afdeling 2. Juridische invulling van de rol van deelnemer

Het beleid voor verantwoorde bekendmaking is een vorm van toetredingsovereenkomst die de ethische hacker ten aanzien van de verwerkingsverantwoordelijke¹¹² bindt. Zo worden het doel van en de essentiële middelen voor de verwerking van persoonsgegevens, in principe, vastgesteld door de verantwoordelijke organisatie en niet door de deelnemer in het kader van een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden. In dat geval moet de deelnemer de wettelijke verplichtingen inzake bescherming van persoonsgegevens naleven in de hoedanigheid van verwerker van de verantwoordelijke organisatie.¹¹³

¹⁰⁸ C. DE TERWANGNE, *idem*, blz. 28.

¹⁰⁹ Groep van artikel 29, advies 1/2010 over de begrippen “voor de verwerking verantwoordelijke” en “verwerker”, WP 169, blz. 14, *idem*.

¹¹⁰ *Ibidem*.

¹¹¹ Art. 4, 8), van de AVG.

¹¹² of ten aanzien van de verwerker, indien de verantwoordelijke organisatie de hoedanigheid van verwerkingsverantwoordelijke heeft.

¹¹³ De verantwoordelijke organisatie kan een verantwoordelijke voor de verwerking van persoonsgegevens of zelf een verwerker van een verwerkingsverantwoordelijke zijn.

Volgens artikel 28, §3 (a) van de AVG moet de verwerker persoonsgegevens verwerken overeenkomstig de instructies van de verwerkingsverantwoordelijke. Algemeen wordt aangenomen dat de aan de verwerker toevertrouwde verwerking niettemin gepaard kan gaan met “een bepaalde handelingsvrijheid voor wat betreft de wijze waarop de belangen van de voor de verwerking verantwoordelijke het best kunnen worden gediend, zodat de verwerker de meest geschikte technische en organisatorische middelen kan kiezen”.¹¹⁴ Zo is het denkbaar dat de deelnemer een bepaalde keuzevrijheid geniet wat de door hem gebruikte middelen betreft om de beveiliging van de informatiesystemen van de verantwoordelijke organisatie na te gaan. De verantwoordelijke organisatie bepaalt welke systemen en diensten de deelnemer mag testen en tot welke hij geen toegang heeft.

Artikel 28, § 1, van de AVG bepaalt dat de verwerkingsverantwoordelijke procedures moet uitwerken voor de selectie van dienstverleners om zich ervan te vergewissen dat deze laatsten “afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen” bieden, met name op het gebied van deskundigheid, betrouwbaarheid en middelen. In het kader van een CVDP of van een beloningsprogramma voor het opsporen van kwetsbaarheden kan de verantwoordelijke organisatie de deelname immers beperken tot bepaalde ethische hackers of eisen dat de deelnemers de nodige deskundigheid en ervaring hebben om de systemen van de verantwoordelijke organisatie te testen, met inbegrip van haar eventuele persoonsgegevens.

De verwerkingsverantwoordelijke moet ook een zeker toezicht¹¹⁵ kunnen uitoefenen op de dienst die namens hem wordt uitgevoerd om na te gaan of dit gebeurt in overeenstemming met de overeenkomst die met de verwerker is gesloten en met de AVG. Zo moet de deelnemer samenwerken met de verantwoordelijke organisatie en, op haar verzoek, alle relevante informatie kunnen bezorgen.

De deelnemer kan evenwel als verwerkingsverantwoordelijke worden beschouwd wanneer de essentiële middelen voor de verwerking van persoonsgegevens onvoldoende zijn vastgesteld in de CVDP of wanneer de deelnemer de instructies van de verantwoordelijke organisatie niet opvolgt. De deelnemer die op ongeoorloofde wijze gegevens verwerkt (of gegevens verwerkt voor andere doeleinden dan het opsporen van kwetsbaarheden) moet immers als verwerkingsverantwoordelijke worden beschouwd aangezien hij zelf een ander verwerkingsdoel en/of (essentiële) verwerkingsmiddelen vaststelt.

¹¹⁴ Groep van artikel 29, advies 1/2010 over de begrippen “voor de verwerking verantwoordelijke” en “verwerker”, WP 169, blz. 27, *idem*.

¹¹⁵ Groep van artikel 29, advies 1/2010 over de begrippen “voor de verwerking verantwoordelijke” en “verwerker”, WP 169, blz.30.



Afdeling 3. Gevolgen voor de inhoud van het CVDP

Uit het voorgaande volgt dat het CVDP de verplichtingen van de partijen inzake de verwerking van persoonsgegevens, met name het doel van en de essentiële middelen voor eventuele verwerkingen, moet vermelden. Zo dient de inhoud van het beleid het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen, alsook de rechten en verplichtingen van de verwerkingsverantwoordelijke te omschrijven.

De verantwoordelijke organisatie moet in haar CVDP regels opnemen die de deelnemer verplichten afdoende garanties te bieden voor het toepassen van passende technische en organisatorische maatregelen voor de verwerking van persoonsgegevens.¹¹⁶ De deelnemer moet ervoor zorgen dat deze gegevens worden bijgehouden met waarborging van een op de risico's afgestemd beveiligingsniveau (bij voorkeur versleuteld) en dat ze onmiddellijk na afloop van de verwerking worden verwijderd.

Ook moet de verwerking van persoonsgegevens voor een ander doel dan het opsporen van kwetsbaarheden in de systemen, uitrusting of producten van de verantwoordelijke organisatie worden uitgesloten.

Voorts moet de deelnemer zich ertoe verbinden elk eventueel verlies van persoonsgegevens te melden aan de verantwoordelijke organisatie en/of aan de Gegevensbeschermingsautoriteit en dit zo snel mogelijk na kennisname ervan.

Het CVDP moet minstens de volgende verbintenissen van de deelnemer bevatten:¹¹⁷

- persoonsgegevens uitsluitend verwerken op basis van schriftelijke instructies van de verwerkingsverantwoordelijke;
- waarborgen dat de tot het verwerken van de persoonsgegevens gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen;
- ervoor zorgen dat natuurlijke personen die handelen onder het gezag van de verwerker en toegang hebben tot persoonsgegevens, deze slechts in opdracht van de verwerkingsverantwoordelijke mogen verwerken;¹¹⁸
- passende technische en organisatorische maatregelen 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

¹¹⁶ Art. 28, § 1, van de AVG.

¹¹⁷ Zie met name de voorwaarden vermeld in artikel 28, § 3, van de AVG.

¹¹⁸ Art. 32, § 4, van de AVG.



qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen;¹¹⁹

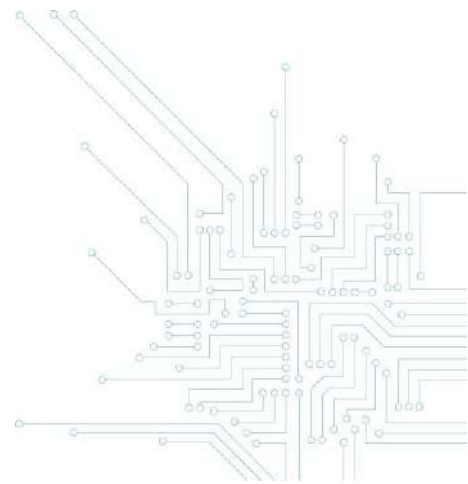
- de voorafgaande toestemming van de verwerkingsverantwoordelijke bekomen voor het in dienst nemen van een andere verwerker en deze laatste verplichten de inhoud van het bekendmakingsbeleid na te leven;
- de verwerkingsverantwoordelijke door middel van passende technische en organisatorische maatregelen, voor zover mogelijk, bijstand verlenen bij het vervullen van diens plicht om verzoeken om uitoefening van de rechten van de betrokkene te beantwoorden;
- de verwerkingsverantwoordelijke bijstand verlenen bij het doen nakomen van de verplichtingen vermeld in de artikelen 32 tot en met 36 van de AVG (beveiliging, melding van inbreuken, impactanalyse, voorafgaande raadpleging), rekening houdend met de aard van de verwerking en de informatie waarover de deelnemer beschikt;
- de verwerkingsverantwoordelijke onverwijld informeren zodra de deelnemer kennis heeft genomen van een inbreuk in verband met persoonsgegevens;¹²⁰
- na afloop van de deelname aan het beleid, alle persoonsgegevens wissen of deze terugbezorgen¹²¹ aan de verwerkingsverantwoordelijke, en bestaande kopieën verwijderen;
- de verwerkingsverantwoordelijke alle nodige informatie ter beschikking stellen om de nakoming van de verplichtingen aan te tonen, waaronder een register van alle categorieën van verwerkingsactiviteiten die hij namens de verwerkingsverantwoordelijke heeft uitgevoerd;¹²²
- het gebruik van persoonsgegevens voor een ander doel dan het opsporen van kwetsbaarheden in het systeem of het meedelen van deze gegevens aan derden uitsluiten.

¹¹⁹ Art. 32, § 1, van de AVG.

¹²⁰ Art. 33, § 2, van de AVG.

¹²¹ naargelang de keuze van de verwerkingsverantwoordelijke.

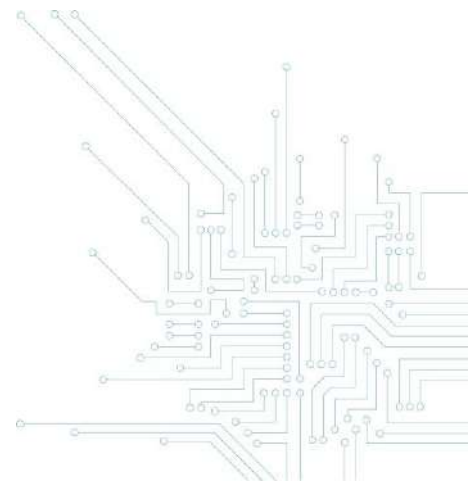
¹²² waarvan de inhoud vermeld is in art. 30, § 2, van de AVG.



H. Juridische referenties

- DE NAUW A. en KUTY F., *Manuel de droit pénal spécial*, Waterloo, Kluwer, 2014, blz. 1125-1145.
- DECHAMPS F. en LAMBILOT C., *Cybercriminalité: Etats des lieux*, Limal, Anthémis, 2016, blz. 26-46.
- DEHOUSSE F., VERBIEST T., ZGAJEWSKI T., "La criminalité dans la société de l'information" in *Introduction au droit de la société de l'information*, Brussel, Larcier, 2007.
- DE VILLENFAGNE F. en DUSOLLIER S., "La Belgique sort enfin ses armes contre la cybercriminalité : à propos de la loi du 28 novembre 2000 sur la criminalité informatique", *A.M.*, 2001, blz. 60-81.
- DOCQUIR B., "La loi du 15 mai 2006: nouvelles définitions des infractions en matière de criminalité informatique", *R.D.T.I.*, 2006, blz. 287-294.
- EVARD S., "La loi du 28 novembre 2000 relative à la criminalité informatique", *J.T.*, 2001, blz. 241-245.
- HENRION T., *Mémento Droit pénal*, Brussel, Kluwer, 2016.
- KUTY F., *Principes généraux du droit pénal*, t. 1, La loi pénale, Brussel, Larcier, 2009.
- K. ROSIER, "Le traitement de données dans le cadre des communications électroniques" in *X. Vie privée et données à caractère personnel*, Brussel, Politeia.
- LEROUX O., "La Criminalité informatique", *Les infractions contre les biens*, Brussel, Larcier, 2008, blz. 409-436.
- LEROUX O., in *X. Postal Mémoires. Lexique du droit pénal et des lois spéciales*, Brussel, Kluwer, 2014, blz. C 362/1-55.
- LORENT A., "Destructions et dégradations autres que par incendie ou explosion", *Droit pénal et procédure pénale (DPPP)*, Kluwer, 2006, blz. 119-136.
- MEUNIER C., "La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique", *Rev. dr. pén.*, 2001, blz. 611-690.
- MEUNIER C., "La loi du 28 novembre 2000 relative à la criminalité informatique" in *Actualités du droit des technologies de l'information et de la communication*, CUP, 2001, blz. 37-160.
- OMRANI F. en DUMORTIER F., "Chronique de jurisprudence 2009-2011. Criminalité informatique", *R.D.T.I.*, 2012, blz. 198-208.
- ROGER FRANCE E., "La criminalité informatique", *Actualités de droit pénal*, Brussel, Bruylant, 2005, blz. 101-133.
- TULKENS F., VAN DE KERCHOVE M., CARTUYVELS Y. en GUILLAIN C., *Introduction au droit pénal*, 9e uitg., Brussel, Kluwer, 2010.
- DE VILLENFAGNE F., "Chronique de jurisprudence 2002-2008. Criminalité informatique", *R.D.T.I.*, 2010, blz. 9-28.
- VANDER GEETEN V., "La criminalité informatique et les politiques de divulgation coordonnée des vulnérabilités" in *Les obligations légales de cybersécurité et de notifications d'incidents*, Politeia, Brussel, 2019, blz. 217 e.v.
- VANDERMEERSCH D., "Éléments de droit pénal et de procédure pénale", La Charte, Brussel, 2012.
- BAEYENS, E., "Informatica en recht: oude griffels - nieuwe leien", *T. Strafr.*, 2007, blz. 404-407.
- DEENE J. en NERINCKX G., "Computercriminaliteit" in *Praktijkboek recht en internet*, Titel II – Hoofdstuk 10, Brugge, Vanden Broele, 2007, blz. 3-43.

- DELBROUCK I., “Informatiacriminaliteit”, in X., *Postal Memorialis, Lexicon strafrecht, strafvordering en bijzondere wetten*, Antwerpen, Kluwer, 2007, I. 42/08-30.
- DE HERT, P., “De wet van 28 november 2000 inzake informatiacriminaliteit en het materieel strafrecht. Een wet die te laat komt of een wet die er nooit had moeten komen?”, *T. Strafr.*, 2001, blz. 286-334.
- J. DUMORTIER, *ICT-Recht, Acco*, Leuven, 1999, blz. 86 e.v.
- KERKHOFS J. en VAN LINTHOUT P., *Cybercrime 3.0*, Brussel, Politeia, 2019.
- KERKHOFS J. en VAN LINTHOUT P., *Cybercrime*, Brussel, Politeia, 2014.
- KERKHOFS J. en VAN LINTHOUT P., “Cybercriminaliteit doorgelicht”, *T. Strafr.*, 2010, blz. 179 e.v.
- KEUSTERMANS J., F. MOLS en T. DE MAERE, “Informatiacriminaliteit” in *Strafrecht en strafvordering. Commentaar met overzicht van rechtspraak en rechtsleer*, Mechelen, Kluwer, 2010, blz. 65-103.
- KEUSTERMANS J. en MOLS F., “De wet van 28 november 2000 inzake informatiacriminaliteit: eerste overzicht”, *R-W*, 2001-2002, blz. 721-732.
- KEUSTERMANS J. en DE MAERE T., “Tien jaar wet informatiacriminaliteit”, *R-W*, 2010-2011, blz. 562-568.
- VAN EECKE, P., “De Wet Informatiacriminaliteit”, in X., *Elektronische handel, juridische en praktische aspecten*, Heule, UGA, 2004, blz.369-385.
- VANSTEENHUYSE S. en T’JONCK P., “Cybercriminaliteit en privacy” in *Privacy en strafrecht, Nieuwe en grensoverschrijdende verkenningen*, Antwerpen, Maklu, 2007.



GIDS OVER HET BELEID VOOR DE GECOÖRDINEERDE BEKENDMAKING VAN KWETSBAARHEDEN DEEL I: WETTELIJKE ASPECTEN

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.

Alle teksten, lay-out, ontwerpen en overige elementen van welke aard ook in dit document zijn onderworpen aan de wetgeving op de auteursrechten. Uittreksels uit dit document mogen alleen voor niet-commerciële doeleinden en met bronvermelding worden gereproduceerd.

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/2020/14828/015

2020

