CEG Information Security

Responsible Disclosure

Modelbeleid en Procedure

Publicatie van de CIO Experience Group Information Security

CIO Platform Nederland, februari 2016

www.cio-platform.nl/publicaties

Inhoudsopgave

Definities

A. Responsible Disclosure is het op een verantwoorde wijze en in gezamenlijkheid tussen melder en organisatie openbaar maken van kwetsbaarheden op basis van een door organisaties hiervoor vastgesteld beleid voor Responsible Disclosure.
B. Een kwetsbaarheid is een (vermoedelijke) zwakte in, of inbreuk op, de beveiliging van de infrastructuur of ICT-systeem van <<*Organisatie*>>.
C. De melder is de persoon of instantie die die via Responsible Disclosure een kwetsbaarheid meldt.
D. De organisatie, <<*Organisatie*>>,is de eigenaar en/of beheerder van het systeem en de ontvanger van de Responsible Disclosure melding.
E. Het Responsible Disclosure beleid is het document waarin de spelregels zijn waaraan de melder en organisatie zich moeten houden. Zie hoofdstuk 5.
F. De Responsible Disclosure procedure is de procedure waarin de verantwoordelijkheden en operationele acties voor Responsible Disclosure zijn beschreven. Zie hoofdstuk 6.
G. Responsible Disclosure wordt ook wel genoemd Coordinated Vulnerability Disclosure.

1 Aanleiding

Uit voorbeelden uit de praktijk (zoals de zaak Henk Krol[1] en de melding over het netwerk van KPN door ethische hackers[2]) blijkt dat het belangrijk is voor organisaties om een Responsible Disclosure beleid uit te dragen. Voor zowel de organisatie als voor de melder schept het duidelijkheid in de verantwoordelijkheden die beide partijen hebben.

<<*Organisatie*>> heeft besloten om een Responsible Disclosure beleid en procedure te ontwerpen en deze toe te passen voor haar eigen organisatie.

[1] Rechtbank Oost-Brabant (2013), *Vonnis zaak Henk Krol*. Geraadpleegd via http://www.rechtspraak.nl

[2] KPN (2013), *Ethisch hackersbeleid helpt KPN*. Geraadpleegd via http://corporate.kpn.com/kpn-actueel/nieuwsberichten-1/ethisch-hackersbeleid-helpt-kpn.htm

2 Wetgeving

Het hacken van computersystemen kan zowel met goede als slechte bedoelingen worden gedaan. Om te bepalen of iemand heeft gehandeld in overeenstemming met de wet kan er een civiele of strafrechtelijke procedure worden gestart. In dit hoofdstuk wordt de Nederlandse wetgeving beschreven die relevant is voor Responsible Disclosure.

NB. Het is belangrijk om te melden dat elk land eigen regelgeving heeft of kan hebben om met inbreuken op computers en dergelijke om te gaan. Internationaal opererende organisaties zullen voor elk land waarin zij actief zijn moeten bepalen of Responsible Disclosure onder het daar geldende rechtssysteem mogelijk is.

2.1 Wetboek van Strafrecht

Met de komst van de wet Computercriminaliteit is hacken sinds 1993 strafbaar volgens het strafrecht. De strafbaarheid van hacken staat onder andere beschreven in artikel 138ab Sr (computervredebreuk) en 161 sexies Sr (beschadigen van systemen). De maximale gevangenisstraffen voor de strafbare feiten lopen respectievelijk van één tot vier jaar en van één tot vijftien jaar.

In de wetsartikelen 138ab en 161 sexies wordt geen onderscheid gemaakt tussen kwaadaardige hackers en ethische hackers. Er wordt in deze wetsartikelen dus geen direct onderscheid gemaakt tussen een kwaadaardige hacker die probeert in te breken of een website DDoSt en een ethische hacker die in het kader van maatschappelijk belang een kwetsbaarheid wil aantonen. De beslissing of een melder heeft gehandeld als een ethische hacker is aan het OM en de rechter.

2.2 Vervolging

Indien er volgens de wet sprake is van computervredebreuk dan kan dat gevolgen hebben voor een melder van een kwetsbaarheid. De melder kan hiervoor zowel civielrechtelijk als strafrechtelijk vervolgd worden (zie kader).

2.2.1 Civielrechtelijke vervolging

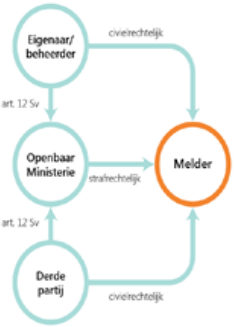
Naar aanleiding van een melding kan een beheerder/eigenaar van het systeem civielrechtelijke stappen ondernemen. Hij maakt de beslissing om al dan niet aangifte te doen en hij beslist of er een civiele rechtszaak gestart moet worden tegen de melder.

Vooraf kan een beheerder/eigenaar in een Responsible Disclosure beleid aangeven dat er onder bepaalde voorwaarden geen aangifte gedaan zal worden of een civiele zaak gestart zal worden. Als de melder zich houdt aan deze voorwaarden dient te worden afgezien van aangifte en civielrechtelijke vervolging.

Verschil civiel- en strafrecht

Het strafrecht regelt de verhouding tussen de Staat en de burger. In het Wetboek van Strafrecht is beschreven aan welke wetten de burgers zich moeten houden.

Het civiele recht regelt de verhoudingen tussen burgers en/of bedrijven onderling. In tegenstelling tot bij het strafrecht is er geen centrale instantie die de zaak voor de rechter brengt.



2.2.2 Strafrechtelijke vervolging

Het Openbaar Ministerie (OM) heeft de mogelijkheid om een strafrechtelijk onderzoek te starten alvorens tot strafrechtelijke vervolging over te gaan. Ook als een bedrijf eerder heeftaangegeven af te zien van vervolging, heeft het OM de mogelijkheid om een onderzoek te starten naar de handelingen van de melder.

Het OM kan na onderzoek ook afzien van vervolging volgens het zogenoemde opportuniteitsbeginsel[3]. De officier van justitie zal de verdachte in dat geval niet voor de rechter brengen op grond van algemeen belang.

Als het Openbaar Ministerie beslist om niet te vervolgen dan kan een derde partij die rechtstreeks belanghebbende is, bijvoorbeeld de beheerder/eigenaar, een

[3] Openbaar Ministerie (2013), *Begrippenlijst: Opportuniteitsbeginsel*. Geraadpleegd via https://www.om.nl/onderwerpen/begrippenlijst/opportuniteitsbeginsel

klant of een patiënt, op grond van artikel 12 Sr een klacht indienen met het verzoek aan het gerechtshof om alsnog over te gaan tot vervolging. Een melder kan dus zowel civiel- als strafrechtelijk worden vervolgd en beide vervolgingen kunnen los van elkaar worden gestart. Afzien van een civiele vervolging leidt dus niet direct tot afzien van een strafrechtelijke vervolging en vice versa.

2.3 Vrijheid van meningsuiting (Artikel 10 EVRM)

Om een zaak van zwaar maatschappelijk belang te onderzoeken kan het nodig zijn om de wet te overtreden. Artikel 10 van het Europees Verdrag van de Rechten voor de Mens (EVRM) geeft de burger de mogelijkheid om misstanden aan de kaak te stellen. Bij journalistieke waarde kan er vanwege het maatschappelijk belang voor gekozen worden om geen straf op te leggen, ondanks het feit dat een handeling op zichzelf staand strafbaar was. Niet alleen beroepsjournalisten, maar ook burgers kunnen journalistiek opereren en zich beroepen op artikel 10.

Belangrijk hierbij is wel dat er geen minder verstrekkende methodes voor handen zijn. Als er mogelijkheden zijn om hetzelfde aan te tonen met minder gevolgen, moet dat worden nagestreefd. Artikel 10 EVRM is bindend voor alle landen die lid zijn van de Raad van Europa en geldt dus voor Nederland.

Het komt voor dat ethische hackers hun melding doen via een journalist om hun anonimiteit te waarborgen. In Nederland heeft een journalist namelijk het recht om een bron geheim te houden. Dit beschermingsrecht komt voort uit artikel 10 EVRM. In een uitspraak van de Hoge Raad[4] is bepaald dat journalisten hun bron niet hoeven prijs te geven tijdens een getuigenverhoor, tenzij het openbaren van de bron noodzakelijk is voor een democratische samenleving. Er zal dan tegenover het ‘zéér zwaarwegende publieke belang’ van persvrijheid een nog ‘zwaarwegende belang’ moeten zijn om het bekendmaken van de bron te rechtvaardigen.

In de aanwijzing toepassing dwangmiddelen tegen journalisten staan de beleidsrichtlijnen van het OM ten opzichte van bronbescherming.

[4] Volkskrant (1996), *Hoge Raad gunt journalist bescherming van bronnen*. Geraadpleegd via http://www.volkskrant.nl/archief/hoge-raad-gunt-journalist-bescherming-van-bronnen~a426812/

In deze aanwijzing schrijft de landelijke leiding van het Openbaar Ministerie: "Omdat het recht op bronbescherming niet absoluut is, kan sprake zijn van het toepassen van strafvorderlijke dwangmiddelen tegen een journalist onder bijzondere omstandigheden: als dit het enige denkbare effectieve middel is om een zeer ernstig delict op te sporen en te voorkomen. Het moet gaan om die misdrijven waarbij het leven, veiligheid of de gezondheid van mensen ernstig kunnen worden geschaad of in gevaar kunnen worden gebracht."[5].

Daarnaast biedt bronbescherming voor de melder geen vrijwaring voor vervolging of absolute garantie voor anonimiteit. Een melder kan ook via andere kanalen worden opgespoord, zoals te zien was bij de melding van een zwakheid in systeem van het Groene Hart Ziekenhuis. De vermoedelijke hacker werd door de Nationale Recherche aangehouden na een onderzoek door het THCT (Team High Tech Crime)[6]. Dit onderzoek word geleid door het Landelijk Parket van het Openbaar Ministerie. Een publicatie via een journalist kon, in dit geval, niet voorkomen dat er in deze zaak een verdachte werd gearresteerd, doordat de vermoedelijke hacker via een andere wijze werd achterhaald.

2.4 Ontwikkelingen wetgeving

Er zijn ontwikkelingen te verwachten die in de toekomst van invloed kunnen zijn op de Responsible Disclosure. Voorbeelden hiervan zijn de Nederlandse Meldplicht datalekken en de Europese meldplicht datalekken.

Het belangrijkste effect van de meldplichten op Responsible Disclosure heeft betrekking op de doorlooptijd van een melding. De voorstellen voor de meldplichten geven aan dat de ontdekking van een lek binnen een bepaalde tijdsspanne gemeld moet worden. Dit betekent dat als er een Responsible Disclosure melding binnenkomt dit gevolgen kan hebben voor de resources die ingezet moeten worden om de melding op tijd te kunnen verwerken.

[5] College van procureurs-generaal (2013), *Aanwijzing toepassing dwangmiddelen tegen journalisten*. Geraadpleegd via https://zoek.officielebekendmakingen.nl/stcrt-2012-3656.html
[6] Landelijke Parket Openbaar Ministerie (2013), *Verdachte aangehouden voor inbraak computer Groene Hart Ziekenhuis*. Geraadpleegd via https://www.om.nl/vaste-onderdelen/zoeken/@30198/verdachte/

3 Standaarden

Sinds de komst van de "Leidraad om te komen tot een praktijk van Responsible Disclosure" van het Nationaal Cyber Security Center (NCSC) wordt Responsible Disclosure door steeds meer Nederlandse organisaties gehanteerd. Naast de leidraad van het NCSC zijn er sinds begin 2014 ook een tweetal internationale ISO standaarden beschikbaar. In de hoofdstuk worden zowel de leidraad als de ISO standaarden toegelicht.

3.1 Leidraad Responsible Disclosure

Naar aanleiding van een motie van Tweede Kamerlid Hachchi (D66) tijdens het AO Cyber Security en Veiligheid van Overheidswebsites op 10 april 2012 heeft minister Opstelten van Veiligheid en Justitie toegezegd om te komen met een kader voor Responsible Disclosure. Dit kader is aangegeven in de 'Leidraad om te komen tot een praktijk van Responsible Disclosure'. De leidraad richt zich zowel tot de organisatie die eigenaar/beheerder is van een informatiesysteem als tot de melder van een kwetsbaarheid. Om te komen tot de leidraad zijn onder andere welwillende hackers uit de community geraadpleegd[7] en zijn ook best practices zoals de policy van Marktplaats.nl meegenomen.

Het NCSC hanteert in haar leidraad de volgende definitie voor Responsible Disclosure: "Responsible Disclosure binnen de ICT-wereld is het op een verantwoorde wijze en in gezamenlijkheid tussen melder en organisatie openbaar maken van ICT kwetsbaarheden op basis van een door organisaties hiervoor vastgesteld beleid voor Responsible Disclosure."[8]

De definitie bevat twee belangrijke elementen die het standpunt van het NCSC typeren. Allereerst zijn er primair twee partijen betrokken bij Responsible Disclosure: de melder en de organisatie. Ten tweede gaat het NCSC uit van een door de organisatie (vooraf) vastgesteld beleid voor Responsible Disclosure.

[7] NCSC (2013), *Kamerbrief Responsible Disclosure*. Geraadpleegd via https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/responsible-disclosure-leidraad/2/Kamerbrief%2BResponsible%2BDisclosure.pdf
[8] NCSC (2013), *Responsible Disclosure*. Geraadpleegd via https://www.ncsc.nl/security

Het NCSC verwijst naar meerdere Responsible Disclosure policies die kunnen dienen als voorbeeld. Deze voorbeelden zijn onder andere afkomstig van Floor Terra, Marktplaats.nl, Fox-IT en grote Nederlandse telecomproviders.

In de leidraad wordt uitgelegd hoe een melder zou kunnen handelen in het geval dat een eigenaar/beheerder geen vastgesteld beleid heeft voor Responsible Disclosure. De melder wordt in dat geval geacht om direct contact op te nemen met de eigenaar/beheerder. Geeft dit niet het gewenste effect dan kan een melder beslissen om een intermediair in te schakelen. In de leidraad wordt het NCSC aangewezen als intermediair en ook in het Responsible Disclosure beleid van het NCSC wordt op haar website aangegeven dat het NCSC bij het niet of niet goed reageren door een derde partij kan "optreden als intermediair"[9].

De leidraad heeft geen invloed op strafrechtelijke kaders. Het volgen van de richtlijnen garandeert de melder dus op geen enkele wijze dat hij is gevrijwaard van een strafrechtelijk procedure. Een civielrechtelijke procedure kan eventueel wel door een melder worden voorkomen door met de eigenaar/beheerder overeen te komen dat er geen aangifte wordt gedaan of civielrechtelijke stappen worden ondernomen.

3.2 ISO standaarden

De Internationale Organisatie voor Standaardisatie (ISO) heeft diverse standaarden uitgebracht rondom het inrichten van veiligheid in een organisatie. Vertrekpunt hierbij vormt de standaard 27002, die best practices en beheersmaatregelen biedt voor informatiebeveiliging. Een Responsible Disclosure beleid moet aansluiten op de processen die zijn ingericht op basis van ISO 27002, of een vergelijkbare standaard.

Daarnaast heeft ISO twee standaarden uitgebracht over het openbaren van kwetsbaarheden en de afhandeling van meldingen van kwetsbaarheden. Beide standaarden zijn toegepast bij de inrichting van een Responsible Disclosure procedure voor het modelbeleid.

[9] NCSC (2013), *Responsible Disclosure*. Geraadpleegd via https://www.ncsc.nl/security

3.2.1 ISO 29147

De NEN-ISO 29147 geeft richtlijnen voor de openbaarmaking van potentiële kwetsbaarheden. In de internationale norm worden methoden beschreven die een organisatie kan gebruiken om problemen bij de openbaarmaking van een kwetsbaarheid op te pakken. De norm beschrijft vier richtlijnen:

- Ontvangst van meldingen mogelijke kwetsbaarheden
- Verspreiding van informatie over kwetsbaarheden in hun producten en online diensten
- Informatiestromen bij openbaar maken van een kwetsbaarheid
- Voorbeelden van gestructureerde informatie-uitwisseling

3.2.2 ISO 30111

De NEN-ISO 30111 geeft richtlijnen voor de manier waarop mogelijk informatie over kwetsbaarheden verwerkt moet worden en hoe de kwetsbaarheid opgelost kan worden in een product of online dienst. De norm beschrijft drie richtlijnen:

- Een gestructureerd proces en organisatiestructuur om onderzoek en het verhelpen van kwetsbaarheden te ondersteunen
- De stappen om een kwetsbaarheid te verifiëren
- Het proces om een kwetsbaarheid te behandelen

4 Doel Responsible Disclosure

Het kan natuurlijk gebeuren dat een zwakheid in een product of dienst over het hoofd gezien wordt door de organisatie, die door iemand anders wel wordt opgemerkt. <<*Organisatie*>> vindt het daarom belangrijk om meldingen van kwetsbaarheden aan te nemen en samen te werken (eventueel met de melder) om die kwetsbaarheden te verhelpen. Op deze wijze kan het niveau van informatiebeveiliging verhoogd worden en kan schade worden voorkomen.

Veiligheid en het voorkomen van schade staat voorop. Daarom wil <<*Organisatie*>> de kwetsbaarheid oplossen voordat deze extern bekend wordt gemaakt. De melder moet <<*Organisatie*>> dus voldoende tijd geven om het lek te dichten voordat de kwetsbaarheid eventueel openbaar kan worden.

Door het opstellen van een beleid voor Responsible Disclosure kan een deel van de onduidelijkheid omtrent vervolging weggenomen worden. Het Responsible Disclosure beleid zorgt ervoor dat er spelregels zijn voor de melder en voor <<*Organisatie*>>. Hierbij is het wel van belang om te melden dat het OM en een eventuele betrokken derde partij (zoals een webhoster) altijd zelfstandig over kan gaan tot juridische stappen, ongeacht de inhoud van het beleid van de organisatie.

5 Beleid Responsible Disclosure

Het Responsible Disclosure beleid geeft de spelregels aan voor de melder en geeft aan wat er van de organisatie verwacht kan worden. Om de melder en het publiek de juiste verwachtingen te geven wordt het beleid gepubliceerd op de website. Het beleid hangt samen met de Responsible Disclosure procedure. De procedure is te vinden in hoofdstuk 6.

Het beleid is gebaseerd op het voorbeeldbeleid van Floor Terra.

---------- Beleid zoals te publiceren op website ----------

Bij <<Organisatie>> vinden wij de veiligheid van onze systemen erg belangrijk. Ondanks onze zorg voor de beveiliging van onze systemen kan het voorkomen dat er toch een zwakke plek is.

Als u een zwakke plek in één van onze systemen heeft gevonden, dan horen wij dit graag zodat er zo snel mogelijk maatregelen kunnen treffen. Wij willen graag met u samenwerken om onze gebruikers en onze systemen beter te kunnen beschermen.

Ons beleid voor Responsible Disclosure is geen uitnodiging om ons bedrijfsnetwerk uitgebreid actief te scannen om zwakke plekken te ontdekken. Wij monitoren ons bedrijfsnetwerk. Hierdoor is de kans groot dat een scan wordt opgepikt, dat er door onze CERT of dienstverlener onderzoek wordt gedaan en er mogelijk onnodige kosten worden gemaakt.

Er bestaat een kans dat u tijdens uw onderzoek handelingen uitvoert die volgens het strafrecht strafbaar zijn. Als u zich aan de onderstaande voorwaarden heeft gehouden zullen wij geen juridische stappen tegen u ondernemen betreffende de melding. Het Openbaar Ministerie behoudt altijd het recht zelf te beslissen of u strafrechtelijk vervolgd wordt. Het Openbaar Ministerie heeft hierover beleidsbrief(https://www.om.nl/publish/pages/22742/03_18_13_beleidsbrief_college_responsible_disclosure.pdf) gepubliceerd.

Wij vragen u:

- Uw bevindingen zo snel mogelijk te mailen naar <<*vul in een mailadres specifiek voor het melden van security incidentten, bijvoorbeeld security@<<organisatie>>.nl*>> .Versleutel uw bevindingen met onze PGP key <<*fingerprint invullen*>> om te voorkomen dat de informatie in verkeerde handen valt.

- De zwakheid niet te misbruiken door bijvoorbeeld meer data te downloaden dan nodig is om het lek aan te tonen of door het veranderen of verwijderen van gegevens en extra terughoudendheid te betrachten bij persoonsgegevens.

- De zwakheid niet met anderen te delen totdat het is opgelost. Geen gebruik te maken van aanvallen op fysieke beveiliging of applicaties van derden, van social engineering, distributed denial-of-service, of spam.

- Voldoende informatie te geven om de zwakheid te reproduceren zodat wij het zo snel mogelijk kunnen oplossen. Meestal is het IP-adres of de URL van het getroffen systeem, een omschrijving van de kwetsbaarheid en de uitgevoerde handelingen voldoende, maar bij complexere kwetsbaarheden kan meer nodig zijn.

Wat wij beloven:

- Wij reageren binnen 3 werkdagen op uw melding met onze beoordeling van de melding en een verwachte datum voor een oplossing.

- Wij behandelen uw melding vertrouwelijk en zullen uw persoonlijke gegevens niet zonder uw toestemming met derden delen tenzij dat noodzakelijk is om een wettelijke verplichting na te komen.

- Wij houden u op de hoogte van de voortgang van het oplossen van de zwakheid.

- Anoniem of onder pseudoniem melden is mogelijk. Het is voor u goed om te weten dat dit wel betekent dat wij dan geen contact kunnen opnemen over bijvoorbeeld de vervolgstappen, voortgang van het dichten van het lek, publicatie of de eventuele beloning voor de melding.

- In berichtgeving over de gemelde zwakheid zullen wij, indien u dit wenst, uw naam vermelden als de ontdekker van de kwetsbaarheid.

Wij kunnen u een beloning geven voor uw onderzoek. Wij zijn daartoe echter niet verplicht. U heeft dus niet zonder meer recht op een vergoediing. De vorm van deze beloning staat niet van tevoren vast en zal door ons per geval worden bepaald. Of we een beloning geven en vorm van de beloning hangt af van de zorgvuldigheid van uw onderzoek, de kwaliteit van de melding en ernst van het lek.

Wij streven er naar om alle problemen zo snel mogelijk op te lossen, alle betrokken partijen op de hoogte te houden en wij worden graag betrokken bij een eventuele publicatie over de zwakheid nadat het is opgelost.

Ons beleid valt onder een Creative Commons Naamsvermelding 3.0 licentie. Het beleid is gebaseerd op het voorbeeldbeleid van Floor Terra (Responsible Disclosure.nl)

---------- Einde beleid ----------

6 Procedure Responsible Disclosure

Het Responsible Disclosure beleid hangt samen met de Responsible Disclosure procedure. Het beleid is te vinden in hoofdstuk 5. De stroomdiagram van deze procedure is te vinden in bijlage A.

6.1 Uitgangspunten

A. <<*Organisatie*>> stelt een beleid en procedure voor Responsible Disclosure vast en publiceert beleid en procedure op haar website. Beleid en procedure zijn te bereiken via <<*vul in een mailadres specifiek voor het melden van security incidenten, bijvoorbeeld security@organisatie.nl*>>.
B. De organisatie reserveert capaciteit om adequaat op meldingen te kunnen reageren. Met name incidentafhandeling en mandaat van de procesverantwoordelijke vergen extra aandacht.
C. De informatiebeveiliging die wordt toegepast op de meldingen is gelijk aan de standaard die wordt gehanteerd bij vertrouwelijke informatie, tenzij dit niet noodzakelijk blijkt na inschaling van de melding.
D. Wederzijds vertrouwen is de basis van Responsible Disclosure, vooral in het geval van een langlopende behandeling van de kwetsbaarheid. De organisatie moet de melder en overige betrokkenen met regelmaat op de hoogte houden van de voortgang van het proces. Grote wijzigingen in de voortgang moeten aan de melder worden aangegeven omdat deze impact kunnen hebben op de publicatie van de melder.
E. Als de melder zich houdt aan de spelregels zoals gesteld in het Responsible Disclosure beleid worden er door <<*Organisatie*>> geen juridische (vervolg)stappen ondernomen. Als blijkt dat de melder zich niet conform de spelregels heeft gehandeld, kunnen er alsnog juridische vervolgstappen worden ondernomen.
F. Responsible Disclosure en het niet naleven van de spelregels van Responsible Disclosure kunnen vergaande juridische implicaties hebben voor de organisatie en melder. Tijdige juridische consultatie door een bedrijfsjurist bij civielrechtelijke, strafrechtelijke en privacyvraagstukken is daarom essentieel.
G. Responsible Disclosure is primair een zaak tussen de melder en de eigenaar/beheerder van het systeem. Meldingen over een systeem van derden kunnen niet behandeld worden door <<*Organisatie*>>.

H. Indien mogelijk moeten er afspraken gemaakt worden met leveranciers van goederen en diensten waarop de Responsible Disclosure procedure eventueel betrekking tot heeft.

6.2 Rollen en verantwoordelijkheden

A. De incidenten afhandelende medewerker of CERT van <<*Organisatie*>> is verantwoordelijk voor het doorzetten van meldingen van kwetsbaarheden naar de juiste Information Security Officer van de werkmaatschappij. De incidenten afhandelende medewerker of CERT van <<*Organisatie*>> kan advies bieden bij het oplossen van de kwetsbaarheid en kan betrokken partijen informeren over een kwetsbaarheid.
B. De Information Security Officer van de werkmaatschappij waar de kwetsbaarheid zich bevindt is verantwoordelijk voor het bewaken van de procesvoortgang en het onderzoeken en verhelpen van de kwetsbaarheid. Daarnaast onderhoudt de Information Security Officer het contact met de melder.
C. De communicatieafdeling kan de Information Security Officer steunen bij de communicatie met de melder en wordt betrokken bij publicatie van een kwetsbaarheid.
D. De centrale telefoniste en ICT-helpdesk van de werkmaatschappij moeten op de hoogte zijn van de Responsible Disclosure procedure en moeten een melder kunnen verwijzen naar de incidenten afhandelende medewerker of CERT van <<*Organisatie*>> in het geval een melding binnenkomt bij de centrale telefoniste of ICT-helpdesk.
E. De melder is verantwoordelijk voor het eigen handelen en heeft zich te houden aan de spelregels zoals die zijn gesteld in het Responsible Disclosure beleid van de organisatie.

6.3 Ontvangen melding

A. Een melding over een kwetsbaarheid komt binnen via e-mail. Meldingen via e-mail komen binnen op *<<vul in een mailadres specifiek voor het melden van security incidenten, bijvoorbeeld security@organisatie.nl>>* en dienen te worden versleuteld met de bijbehorende openbare PGP sleutel.
B. De melding kan anoniem, onder een pseudoniem of via een tussen-/vertrouwenspersoon gedaan worden. Dit kan betekenen dat er geen communicatie mogelijk is met de melder.
C. Er wordt door de incidenten afhandelende medewerker of CERT van

<<*Organisatie*>> een ontvangstbevestiging van de melding gestuurd naar de melder. Dit is geen bevestiging van de validiteit van het lek maar bevestiging van de start van het onderzoek.

D. De incidenten afhandelende medewerker of CERT van <<*Organisatie*>> zorgt er voor dat de melding zo snel mogelijk terecht komt bij de afdeling die de melding het beste kan beoordelen en in behandeling kan nemen en er wordt bij de incidenten afhandelende medewerker of CERT van <<*Organisatie*>> een ticket aangemaakt.

6.4 Identificatie kwetsbaarheid

A. Binnen drie werkdagen stuurt de Information Security Officer een digitaal ondertekende ontvangstbevestiging van de melding van de kwetsbaarheid. In de e-mail staat minimaal:
   a) De bevestiging van de melding
   b) Een eerste inschatting van legitimiteit en ernst van de gemelde kwetsbaarheid
      - Er dient een inschatting te worden gemaakt van de legitimiteit en ernst van de gemelde kwetsbaarheid. Daaruit komt een termijn waarop de kwetsbaarheid verholpen wordt. Standaardtermijnen voor kwetsbaarheden zijn 60 dagen in configuratie en software en 6 maanden in hardware.
   c) Eventuele vervolgstappen voor het traject.
   d) Eventuele behandeltermijn voor het oplossen van het lek.

B. De Information Security Officer probeert de mogelijke kwetsbaarheid te verifiëren. Als er sprake is van een melding van een kwetsbaarheid in niet meer ondersteunde software, service of website, moet er worden vastgesteld of deze kwetsbaarheid zich niet ook bevindt in andere, wél ondersteunde producten of diensten. Daarnaast zal een inschatting gemaakt moeten worden of deze zelfde kwetsbaarheid ook bij andere organisaties, binnen of buiten de sector, zou kunnen voorkomen en dienen betrokkenen via de daartoe geëigende kanalen te worden ingelicht.

C. De prioritering moet worden vastgesteld. Deze wordt herleid uit een tweetal factoren: urgentie en impact. De prioritering die moet worden gevolgd is de incident prioritering uit het '*Draaiboek informatiebeveiligingsincidenten*'. Bij een prioriteringsklasse van medium of hoger moet de Corporate Information Security Officer worden betrokken bij het onderzoek.

D. Er moet een eerste inschatting gemaakt worden of de melder zich heeft gehouden aan de spelregels uit het beleid. Als er mogelijk sprake is van overtreding van de spelregels moet de Corporate Privacy Officer worden ingeschakeld voor een juridische beoordeling.
E. Bij het bepalen van een prioritering van de melding moet rekening worden gehouden met de informatie die op dat moment beschikbaar is. Hieronder kunnen de volgende aspecten worden overwogen:
   a) **De agenda van de melder**: De melder kan van plan zijn om de kwetsbaarheid openbaar te maken via een bijvoorbeeld een onderzoeksverslag of een presentatie tijdens een conferentie. De organisatie moet de kwetsbaarheid openbaar maken voor of direct na de openbaarmaking door de melder. De organisatie moet dus op de hoogte zijn van de gewenste publicatiedatum van de melder.
   b) **Algemene kennis over de kwetsbaarheid**: Als de kwetsbaarheid algemeen bekend is de kans groter dat de kwetsbaarheid uitgebuit zal worden.
   c) **Het karakter van mogelijke aanvallen**: De kosten en de slaagkans van een aanval hangen af van de kwetsbaarheid die moet worden uitgebuit. Kwetsbaarheden met lage aanvalskosten en hoge slaagkans moeten snel worden opgelost.
   d) **Het bestaan en volwassenheid van aanvalsmiddelen**: Wanneer er goedwerkende methodes beschikbaar zijn om gebruik te maken van de kwetsbaarheid, kunnen er aanvalstools ontwikkeld worden.
   e) **Het karakter van potentiële schade**: Het karakter van het product en de potentiële schade bepalen de ernst voor de gebruikers. Een kwetsbaarheid in een intranet kan bijvoorbeeld grote impact hebben door het lekken van persoonlijke informatie.
   f) **Bewijzen van aanvallen (incidenten)**: Incidenten waarbij de kwetsbaarheid wordt uitgebuit kunnen wijzen op een vergroot risico voor de gebruikers. Afhankelijk van de beschikbare informatie kan er een tijdelijke oplossing worden ontwikkeld, ook als er nog geen complete oplossing beschikbaar is.

6.5 Beëindiging onderzoek

Er zijn verschillende mogelijkheden waarop een onderzoek kan worden afgerond. De melder moet op de hoogte worden gesteld waarom het onderzoek wordt gestaakt.

A. Dubbele melding: Het probleem is al eerder gemeld en wordt al

behandeld via een Responsible Disclosure procedure, via een andere incident afhandelingsprocedure, via gepland onderhoud, of is al verholpen.

B. Verouderd product: De kwetsbaarheid is alleen aanwezig in een product of dienst die niet meer wordt ondersteund door de organisatie.
C. Non-security kwetsbaarheid: De kwetsbaarheid die is gemeld heeft geen implicaties voor de informatiebeveiliging of is niet te misbruiken door middel van bestaande technieken.
D. Kwetsbaarheid bij derde partij: De kwetsbaarheid is aanwezig in een product of dienst van een derde partij. Er kan in overleg met de melder contact worden gezocht met de derde partij.

6.6 Bevestigen validiteit

A. Nadat de verificatie van de kwetsbaarheid is afgerond moet de melder geïnformeerd worden over de bevindingen en de vervolgstappen van het onderzoek.
B. Mogelijk kan de organisatie de kwetsbaarheid niet reproduceren op basis van de informatie uit de melding. De organisatie moet dan de melder vragen om meer bewijs om aan te tonen dat het daadwerkelijk om een informatiebeveiligingsprobleem gaat.

6.7 Schade indamming en beoordeling blootstelling

A. Start een grondige beoordeling van de aard en omvang van het incident, stel vast wat de schade is en stel bewijsmateriaal veilig.
B. Aanvulling: De melder moet op de hoogte worden gesteld van de voortgang van het onderzoek. Indien mogelijk wordt de melder een globale planning voor remediatie en herstel gestuurd.

6.8 Remediatie en herstel

A. Neem maatregelen om de oorzaak van het incident te blokkeren of te verwijderen, verminder de impact door verdere blootstelling van de gevoelige gegevens te voorkomen, maak een start om de bedrijfsprocessen te herstarten als deze gestopt waren als gevolg van het incident en zorg ervoor dat risico's die verband houden met dit incident worden gemitigeerd.

6.9 Openbaar maken

A. Als er een update beschikbaar is voor de kwetsbaarheid in een online

omgeving, moet deze update geïmplementeerd worden.

B. De melder maakt de kwetsbaarheid pas openbaar als de melder en organisatie zijn overeengekomen dat de kwetsbaarheid openbaar wordt gemaakt, alle betrokken organisaties goed zijn geïnformeerd en de organisatie heeft aangegeven dat de kwetsbaarheid is opgelost conform de gemaakte afspraken.
C. Als een kwetsbaarheid niet of moeilijk op te lossen is, of indien er hoge kosten mee gemoeid zijn, kan <<*Organisatie*>> in overleg met de melder afspreken om de kwetsbaarheid niet openbaar te maken.
D. Zodra de organisatie tevreden is met de effectiviteit van de update moeten medewerkers, gebruikers en klanten via een beveiligingsadvies (zie bijlage C) worden geïnformeerd. De oplossing moet beschikbaar worden gesteld via de website van de organisatie.
E. Nadat er een beveiligingsadvies is gepubliceerd kunnen er verdere aanpassingen noodzakelijk zijn. Deze aanpassingen moeten duidelijk worden bijgehouden.
F. Indien er een ticket bij de incidenten afhandelende medewerker of CERT van <<*Organisatie*>> is aangemaakt moet er worden aangegeven dat deze is afgehandeld.

6.10 Informeren betrokkenen

A. Indien de kwetsbaarheid mogelijk ook op andere plaatsen aanwezig is, kan de Information Security Officer met de melder afspreken om via de incidenten afhandelende medewerker of CERT van <<*Organisatie*>> een bredere ICT-community of het algemene publiek te informeren over de kwetsbaarheid.

6.11 Belonen melder

A. De organisatie bepaalt zelfstandig per geval of er een beloning wordt toegekend en welke vorm de beloning heeft. Een toegekende beloning wordt uitgekeerd zodra met voldoende zekerheid is vastgesteld dat de melder zich heeft gehouden aan de voorwaarden uit het Responsible Disclosure beleid en de Responsible Disclosure procedure.

6.12 Publiceren

A. Er worden met de melder afspraken gemaakt over hoe de publiciteit wordt gezocht. De communicatieafdeling wordt betrokken in de besluitvoering omtrent een publicatie.
B. In overleg met de melder kan er toe besloten worden om tezamen

naar buiten te treden. Te denken valt aan een gezamenlijke presentatie op een beveiligingscongres of een publicatie op een blog van <<*Organisatie*>>.

C. Indien de melder de kwetsbaarheid niet zelf wil publiceren wordt de melder via een e-mail op de hoogte gesteld van de afronding, de eventuele beloning en bedankt voor zijn melding en inzet.

6.13 Rapportage en evalueren

A. Evaluatie wordt uitgevoerd zoals beschreven in het *'Draaiboek informatiebeveiligingsincidenten'*.

B. Resultaten van de Responsible Disclosure procedure en de oorzaken van de kwetsbaarheid worden geëvalueerd door het <<*Organisatie*>> Security Kernteam.

7 Bronnen

7.1 Beleid

Floor Terra (2013), *Responsible Disclosure voorbeeld tekst*. Geraadpleegd via www.responsibledisclosure.nl

NCSC (2013), Leidraad om te komen tot een praktijk van Responsible Disclosure. Geraadpleegd via https://www.ncsc.nl/actueel/nieuwsberichten/leidraad-responsible-disclosure.html

Nederland ICT (2013), *Gedragscode Responsible Disclosure*. Geraadpleegd via http://www.nederlandict.nl/Files/TER/Gedragscode_responsible_disclosure_2013.pdf

SURFnet (2014), *modelbeleid en procedure Responsible Disclosure Hoger Onderwijs*

7.2 Procedure

NEN-ISO/IEC (2014), *NEN-ISO/IEC 29147:2014 Vulnerability disclosure*. Genève: ISO/IEC

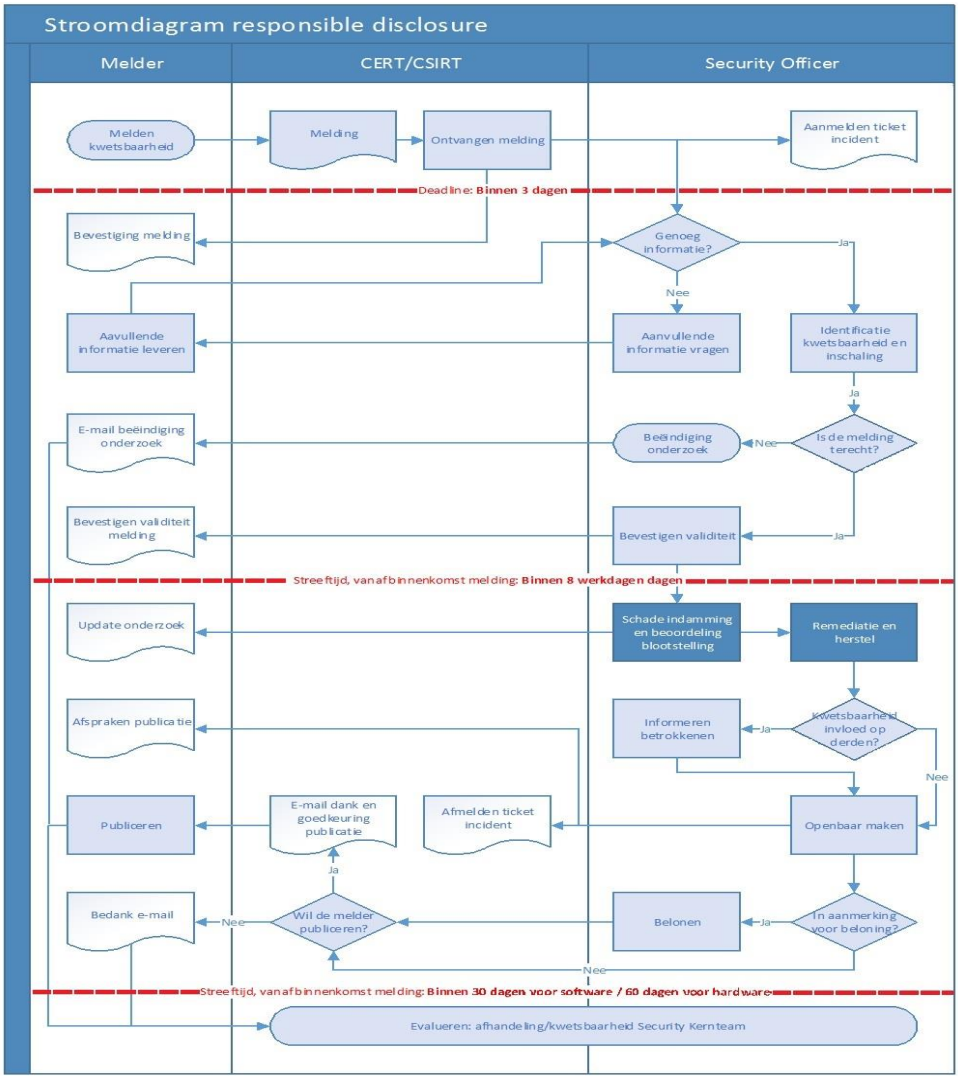
NEN-ISO/IEC (2013), *NEN-ISO/IEC 30111:2013 Vulnerability handling processes*. Genève: ISO/IEC

7.3 Dankbetuiging

Onze speciale dank gaat uit naar de opstellers van de documenten waarop deze publicatie is gebaseerd. In het bijzonder willen we hierbij noemen de Coöperatie SURF, het Nationaal Cyber Security Centrum en Floor Terra. Door hun voorzet was het voor ons gemakkelijker om een handreiking te doen aan alle organisaties die Responsible Disclosure willen inrichten. Door samen te werken maken we de digitale wereld veiliger.

Bijlage A: Flowchart proces Responsible Disclosure

Deze flowchart geeft de volgorde aan waarop de verschillende stappen van de Responsible Disclosure.



Bijlage B: Formulier

Voorbeelden voor de inhoud voor formulier melding kwetsbaarheid zijn te vinden in ISO 29147; Annex A of https://forms.cert.org/VulReport/. Een voorbeeld van een formulier:

Dit formulier is alleen bedoeld voor het melden van beveiligingslekken. Graag zo compleet mogelijk invullen.

- Naam
- E-mail
- Public key
- Telefoonnummer
- Wil je publiceren over de kwetsbaarheid (ja/nee)
- Beschrijving kwetsbaarheid en de uitgevoerde handelingen
- Selecteer bestand

Bijlage C: Beveiligingsadvies

Voorbeelden voor beveiligingsadviezen (advisories) zijn te vinden in ISO/IEC 29147:2014; Annex A of https://www.ncsc.nl/dienstverlening/response-op-dreigingen-en-incidenten/beveiligingsadviezen-toelichting.html.

Het NCSC hanteert de volgende opbouw voor een beveiligingsadvies:

- Titel
- Advisory-ID
- Versie
- Kans
- CVE-ID
- Schade
- Uitgiftedatum
- Toepassing
- Versie(s)
- Platform
- Update
- Samenvatting
- Gevolgen
- Beschrijving
- Mogelijke oplossingen
- Links

“De vereniging van ICT eindverantwoordelijken in grote organisaties van de vraagzijde”

www.cio-platform.nl