Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Coordinated Vulnerability Disclosure: de Leidraad

Voorwoord

Nog tot aan het begin van dit decennium werden meldingen over digitale kwetsbaarheden lang niet altijd met open armen ontvangen. Gaten in ICT-systemen werden dan simpelweg niet gedicht. Cybercriminelen maakten hier dankbaar gebruik van om publieke en private organisaties aan te vallen. Hoe anders is de praktijk anno 2018!

Het Nationaal Cyber Security Centrum (NCSC) stimuleert het proces van Coordinated Vulnerability Disclosure (CVD) actief sinds de publicatie in 2013 van de 'leidraad om te komen tot een praktijk van responsible disclosure'. De honderden meldingen die het NCSC sindsdien heeft ontvangen, illustreren het vertrouwen en de samenwerking tussen de ICT-community, overheden, het bedrijfsleven en het NCSC voor een CVD-proces voor het afhandelen en oplossen van kwetsbaarheden in hard- en software.

Ik ben trots dat ik het herziene product van deze vruchtbare samenwerking mag introduceren. Een product waarin de mens centraal staat, want dat is waar het bij CVD om draait. 'Coordinated Vulnerability Disclosure: de leidraad' is een aanscherping van het proces met de belangrijkste lessen van de afgelopen 5 jaar uit de praktijk. Een praktijk die ook internationaal actief wordt gedeeld en uitgedragen.

Met de presentatie van deze leidraad zetten we opnieuw een stap naar een veiliger digitaal Nederland.

Hans de Vries
Directeur NCSC

Rickey Gevers

1. Inleiding

Digitalisering heeft zich doordrongen in de maatschappij. Bijna alle processen hebben op enig moment te maken met computers, uiteenlopend van mobiele telefoons tot en met specialistische software. Dit zorgt voor veel nieuwe mogelijkheden, maar maakt ook dat kwetsbaarheden in ICT-systemen een grote impact kunnen hebben. Het is daarom van belang dat er op effectieve wijze omgegaan wordt met kennis over deze kwetsbaarheden.

Begin 2013 is een aantal organisaties begonnen met het publiceren van beleid omtrent het melden van kwetsbaarheden. Het Nationaal Cyber Security Centrum (NCSC) heeft na overleg met deze partijen de ontwikkelingen samengevat in "leidraad om te komen tot een praktijk van Responsible Disclosure" (de "Leidraad"). Met dit beleid geven bedrijven aan open te staan voor meldingen van kwetsbaarheden van buitenaf, beschrijven ze de randvoorwaarden en geven ze beloftes. Voor melders schiep dit duidelijkheid en creëerde een enigszins veilige omgeving om onderzoek te doen en kwetsbaarheden te melden, zonder direct een strafbaar feit te plegen.
In 2016 hebben tijdens de '*EU high-level meeting on cybersecurity*' 29 organisaties het belang van een beleid voor het omgaan met kwetsbaarheden nogmaals onderstreept door het tekenen van het Coordinated Vulnerability Disclosure Manifesto[1] geïnitieerd door het CIO Platform Nederland en de Rabobank in samenwerking met het NCSC.

Voor publieke en private partijen is er een groot belang gebleken van Coordinated Vulnerability Disclosure (CVD). In de dagelijkse praktijk zijn zij in sterke mate afhankelijk van het ongestoord functioneren van informatiesystemen. Meldingen van kwetsbaarheden in hun systemen hebben de afgelopen jaren geholpen om de veiligheid en continuïteit van systemen te verbeteren. Enerzijds door kwetsbaarheden te verhelpen, anderzijds doordat het bijgedragen heeft aan het algemene ICT-veiligheidsbewustzijn bij bedrijven Nederland.

De afgelopen jaren is gebleken dat melders bereid zijn om te werken binnen de randvoorwaarden van het door organisaties opgestelde CVD-beleid. Meldingen worden door melders direct of indirect bij organisaties gedaan. Uit de praktijk van responsible disclosure is gebleken dat goedwillende melders en kwetsbare organisaties elkaar konden vinden en hiermee een stap verder konden zetten in het verhogen van de beveiliging van netwerk- en informatiesystemen.

Voor deze herziening is opnieuw gesproken met een brede en diverse groep van melders, private en publieke partijen, als ook met het Openbaar Ministerie en de Nationale Politie. Vanuit die praktijk is bevestiging gekomen voor de huidige aanpak en daarnaast zijn er aanvullingen en aanscherpingen gekomen. Het belangrijkste aandachtspunt blijkt communicatie te zijn, zowel tussen melder en organisatie, als ook met andere partijen na het verhelpen van een kwetsbaarheid.

In de volgende hoofdstukken wordt ingegaan op de definitie van CVD, de bouwstenen voor een CVD-beleid en het communicatieproces.

De vorige Leidraad gebruikte de term "responsible disclosure", dat toen de gangbare term was voor die praktijk. In de tussentijd is gebleken dat die term nog te veel nadruk legt op de verantwoordelijkheid van de melder, terwijl het uitgangspunt is dat er een gelijkwaardig gesprek ontstaat tussen melder en mogelijk kwetsbare organisatie. Dit sentiment wordt beter gevat in de huidig gangbare term "coordinated vulnerability disclosure" (CVD). Deze naam wordt ook gebruikt in de ISO-standaarden over dit proces, ISO 29147 en ISO 30111.

1 https://www.thegfce.com/initiatives/r/responsible-disclosure-initiative-ethical-hacking/manifesto

Melanie Rieback

2. Coordinated Vulnerability Disclosure

In de afgelopen 30 jaar zijn er verschillende methoden gebruikt om kwetsbaarheden in ICT-systemen bekend te maken. Voorbeelden hiervan zijn:

- ***'full disclosure'* – het volledig publiek maken van een kwetsbaarheid,**
- ***'non disclosure'* – het verkopen of zelf gebruik maken van een kwetsbaarheid, of**
- ***'coordinated vulnerability disclosure'* (CVD) – het op een gecoördineerde wijze bekend maken van een kwetsbaarheid.**

Deze laatste praktijk heeft nadrukkelijk de voorkeur.

Het is gebleken dat binnen de ICT-gemeenschap er een grote bereidheid is om kennis en ervaringen te delen. De samenwerking opzoeken met deze gemeenschap kan daarom helpen om de algehele beveiliging van systemen te verbeteren.

Doel van Coordinated Vulnerability Disclosure

Het doel van CVD is om bij te dragen aan de veiligheid van ICT-systemen door kennis over kwetsbaarheden te delen. In deze praktijk wordt de kennis gedeeld met een of meer mogelijk kwetsbare organisaties om zo in samenwerking met de melder te komen tot een gezamenlijke oplossing van de gevonden kwetsbaarheid. Om schade zoveel mogelijk te beperken of te voorkomen is het hierbij van belang dat de getroffen organisaties voldoende tijd hebben om kwetsbaarheden te verhelpen of systemen te beschermen. Openbaarmaking van kennis over de kwetsbaarheden na het verhelpen is het uitgangspunt van het proces.

Bij CVD staat voorop dat partijen zich over en weer houden aan afspraken over het melden van de kwetsbaarheid en de omgang hiermee. Het helpt hierbij dat een organisatie randvoorwaarden vooraf publiceert, zoals over welke systemen meldingen gedaan kunnen worden en wat voor soort onderzoek uitgevoerd kan worden. Belangrijk uitgangspunt bij deze randvoorwaarden is dat de organisatie in principe geen aangifte doet of andere juridische stappen onderneemt als er binnen de gestelde voorwaarden onderzocht en gemeld wordt. Deze Leidraad geeft organisaties houvast bij het opstellen van een eigen beleid om recht te doen aan de uitgangspunten van CVD.

Zoals de naam aangeeft staat centraal bij CVD dat de organisatie en de melder met elkaar afstemmen. Het is daarbij van belang om zo min mogelijk schakels te hebben tussen de persoon die de kwetsbaarheid meldt en de persoon binnen de organisatie die verantwoordelijk is voor het oplossen van het probleem.

Bij een kwetsbaarheid die veel systemen raakt kan het van belang zijn om meerdere partijen tegelijk in te lichten. Het NCSC of andere partijen binnen de *security-community* kunnen in dat geval vanuit een coördinerende rol ondersteunen met het CVD-proces.

Mischa R. van Geelen

3. Verantwoordelijkheden

Met het voeren van een CVD-beleid wordt beoogd dat melders en de organisatie met elkaar samenwerken om zo kwetsbaarheden in ICT-systemen te verminderen. Het voeren van dit beleid moet worden gezien als een aanvulling op bestaande maatregelen rondom informatiebeveiliging. De verschillende actoren hebben allemaal een eigen rol. Hieronder worden de belangrijkste verantwoordelijkheden van elke actor nader toegelicht.

De organisatie die eigenaar/beheerder is van een systeem

De organisatie die eigenaar/beheerder of leverancier is van een systeem, is primair verantwoordelijk voor de beveiliging van dit systeem. Daarmee is de organisatie ook verantwoordelijk voor de wijze waarop gevolg wordt gegeven aan de melding van de kwetsbaarheid.

De organisatie kan ervoor kiezen om aan de hand van deze Leidraad een eigen CVD-beleid op te stellen en dit uit te dragen naar mogelijke melders. Organisaties tonen met het publiceren van een CVD-beleid bereidheid om informatie over kwetsbaarheden te ontvangen. Een partij die een CVD-beleid vaststelt kan zich binden aan het principe om geen aangifte te doen als aan de volgens het beleid geldende spelregels wordt voldaan.

Na het melden van een kwetsbaarheid geeft een melder de bal uit handen aan de organisatie. Het is belangrijk te beseffen dat de melder vaak iemand van buiten de organisatie is. De melder heeft geen direct zicht op interne processen die gaan lopen na de melding van een kwetsbaarheid. Melders zullen het daarom op prijs stellen om op de hoogte gehouden te worden van de ontwikkelingen rondom het verhelpen van de kwetsbaarheid. Dit is ook van belang om de juiste verwachtingen ten aanzien van opvolging en tijdigheid van de oplossing te scheppen.

De melder van een kwetsbaarheid

De melder heeft op enigerlei wijze een kwetsbaarheid weten te constateren en wil bijdragen aan de veiligheid van ICT-systemen door deze kwetsbaarheid te laten verhelpen en eventueel later openbaar te maken. De melder kan iets ontdekt hebben door passieve observatie, of door actief testen uit te voeren op het ICT-systeem. De melder is uiteraard verantwoordelijk voor het eigen handelen en de wijze waarop de kwetsbaarheid ontdekt is. Het is de eigen verantwoordelijkheid van de melder om op de hoogte te zijn van de randvoorwaarden die een organisatie stelt in het CVD-beleid. De meeste overheden en bedrijven hebben hun CVD-beleid gepubliceerd op de website.

Het vinden van kwetsbaarheden kan niettemin gepaard gaan met het overtreden van de wet. Organisatie en melder kunnen in het kader van CVD overeenkomen dat van eventueel strafrechtelijk handelen geen aangifte zal worden gedaan. Het gepubliceerde CVD-beleid van de organisatie is daarbij leidend. Eveneens kan worden afgesproken dat er geen civielrechtelijke stappen worden ondernomen.

Als de indruk bestaat dat de wet overtreden is door de melder, kan een CVD-beleid allereerst helpen om aangifte tegen de melder te doen voorkomen. Dit valt of staat met de randvoorwaarden uit het beleid waar een organisatie vraagt een melder zich aan te houden, met daaraan mogelijk een gekoppelde belofte om geen aangifte te doen, zolang de melder binnen de randvoorwaarden van dit beleid opereert. Indien er wel aangifte wordt gedaan, is in Nederland het bestaan en naleven van CVD-beleid een relevante omstandigheid die de officier van justitie zal meenemen in zijn beslissing om al dan niet een strafrechtelijk onderzoek in te laten stellen en/of te vervolgen. In principe stellen Politie en Openbaar Ministerie (OM) geen strafrechtelijk onderzoek in, indien de melder zich klaarblijkelijk aan de regels uit het CVD-beleid van de betreffende organisatie heeft gehouden. Het OM en de Politie zullen de zaak wel nader onderzoeken als er aanwijzingen zijn dat de melder in het handelen

bewust dan wel onbewust te ver is gegaan en/of zich niet aan het CVD-beleid heeft gehouden. Op basis van dit onderzoek kan het OM besluiten om wel of niet tot vervolging over te gaan.

Het Openbaar Ministerie heeft een beleidsbrief gepubliceerd waarin het meer specifiek ingaat op aspecten die van belang zijn bij de onderzoeks- en vervolgingsbeslissing. Denk daarbij aan de vraag of het handelen van de melder een zwaarwegend algemeen belang diende, evenals de vraag of de melder niet onevenredig heeft gehandeld en of de melder niet op een andere minder ingrijpende manier had kunnen handelen. In de betreffende beleidsbrief worden deze aspecten nader uitgewerkt.[2] Relevante jurisprudentie sinds 2013[3] laat zien dat deze aspecten voor de rechter ook meewegen als een organisatie niet actief een CVD-beleid voert.

2 https://www.om.nl/@32028/beleid-ethische/

3 Zie: http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBOBR:2013:BZ1157 en http://deeplink.rechtspraak.nluitspraak?id=ECLI:NL:RBDHA:2014:15611

Victor Gevers

4. Bouwstenen voor het CVD-proces

Hieronder zijn bouwstenen voor het vormgeven van het CVD-proces weergegeven voor de organisatie, de melder en het NCSC.

4.1 De organisatie

Het uitdragen van CVD begint bij een organisatie die eigenaar is van ICT-systemen of leverancier van een ICT-product/systeem. Deze organisatie is immers primair verantwoordelijk voor de informatiebeveiliging van deze ICT-systemen. Om op een effectieve wijze samen te werken met verschillende partijen aan het oplossen van kwetsbaarheden kan een organisatie besluiten een CVD-beleid op te stellen en te publiceren. Door het opstellen van een eigen CVD-beleid maakt de organisatie duidelijk op welke wijze zij omgaat met meldingen van kwetsbaarheden. Hierdoor kan een organisatie zelf ook richting geven aan de manier waarop zij meldingen wenst te ontvangen. Dit kan als volgt werken:

- De organisatie stelt een CVD-beleid vast en publiceert dit.
- In dit beleid geeft de organisatie duidelijke spelregels aan voor het onderzoek dat melders kunnen uitvoeren, zoals welke technieken toegestaan zijn, welke systemen wel en niet binnen de scope vallen.
- De organisatie maakt het laagdrempelig voor een melder om een melding te doen. Dit kan door een gestandaardiseerde wijze – bijvoorbeeld een specifiek mailadres of online formulier – te gebruiken voor het doen van meldingen. Hierbij kan de organisatie de afweging maken om anonieme meldingen in ontvangst te nemen.
- De organisatie reserveert interne capaciteit en richt een proces in om adequaat op meldingen te kunnen reageren. Het verdient de aanbeveling een proces in te richten waarmee gevonden kwetsbaarheden adequaat verholpen kunnen worden. De herkomst van de melding doet hierbij niet ter zake. De kwetsbaarheid kan ook door een interne medewerker zijn geconstateerd of bijvoorbeeld bij een test.
- Ervaring uit de praktijk leert dat er na het initieel publiceren van het CVD-beleid er een verhoogde interesse ontstaat voor het melden van kwetsbaarheden bij de organisatie. De organisatie houdt hier rekening mee door het inplannen van (extra) capaciteit.
- De organisatie neemt de melding van de kwetsbaarheid in ontvangst en zorgt ervoor dat deze zo snel mogelijk terecht komt bij de afdeling die de melding het beste kan beoordelen en in behandeling kan nemen.
- De organisatie stuurt een ontvangstbevestiging van de melding, bij voorkeur digitaal ondertekend om de prioriteit te benadrukken, aan de melder.
- De organisatie treedt in overleg met de melder om de termijn vast te stellen waarop eventuele bekendmaking zal plaatsvinden. Deze termijn zal sterk afhangen van de aard van de kwetsbaarheid en het type systeem.
  - Als richtlijn wordt vaak een termijn van ongeveer 60 dagen gebruikt voor software kwetsbaarheden. Het verhelpen van kwetsbaarheden in hardware is lastiger te realiseren, hierbij kan een richtlijn van 6 maanden worden gehanteerd.
- In overleg kan het wenselijk zijn om deze termijn uit te breiden of in te korten, indien veel of juist weinig ICT-systemen afhankelijk zijn van het systeem ten aanzien waarvan de kwetsbaarheid gemeld wordt, of de kwetsbaarheid makkelijker of moeilijker blijkt om op te lossen.
- Het kan voorkomen dat een kwetsbaarheid niet of moeilijk op te lossen is, of dat er hoge kosten gemoeid zijn met het verhelpen ervan. In deze gevallen kan de organisatie, eventueel in overleg met de melder, overeenkomen de kwetsbaarheid als geaccepteerd risico te beschouwen en niet te verhelpen.
- De organisatie houdt de melder op de hoogte van de voortgang van het proces.

- De organisatie kan aanbieden dat de melder publiekelijk wordt bedankt bij publicatie van de kwetsbaarheid. Ook kan er voor gekozen worden gezamenlijk naar buiten te treden.
- Het verdient de voorkeur de melder een beloning/waardering te geven voor het melden van kwetsbaarheden in systemen, indien de melder zich aan de in het CVD-beleid opgenomen spelregels heeft gehouden. De hoogte van de beloning kan afhankelijk zijn van de kwaliteit van de melding. Door een beloning/waardering te geven kan er een betere relatie ontstaan tussen melder en organisatie en vergroot de bereidheid om ook nieuwe meldingen conform het CVD-beleid te melden.
- De organisatie kan in overleg met de melder afspreken om de bredere ICT-gemeenschap te informeren over de kwetsbaarheid indien het aannemelijk is dat de kwetsbaarheid ook op andere plaatsen aanwezig is.
- De organisatie kan zich in het CVD-beleid binden aan het principe om geen aangifte te doen als aan de spelregels wordt voldaan.

4.2 De melder

De melder is de spil bij het kunnen voeren van een succesvol CVD-proces. De melder heeft op enigerlei wijze een kwetsbaarheid weten te constateren en wil bijdragen aan de veiligheid van ICT-systemen door deze kwetsbaarheid bij een organisatie te laten verhelpen en openbaar te maken. Melders erkennen hiermee dat zij een belangrijke maatschappelijke bijdrage kunnen leveren door kwetsbaarheden op gecoördineerde wijze te openbaren. Om tot een succesvol CVD-proces te komen zijn voor de melder de volgende bouwstenen van belang:

- De melder is verantwoordelijk voor het eigen handelen en zal bij het onderzoeken en melden van kwetsbaarheden proportionaliteit en subsidiariteit in acht nemen. Dat wil zeggen dat de melder in ieder geval niet verder gaat dan noodzakelijk om de kwetsbaarheid aan te tonen, en in eerste instantie de kwetsbaarheid meldt bij de (systeem/informatie) eigenaar.
- De melder zal een melding zo snel als mogelijk doen om te voorkomen dat kwaadwillenden de kwetsbaarheid ook vinden en er misbruik van maken.
- De melder zal de melding op een vertrouwelijke manier bij de organisatie doen om te voorkomen dat anderen ook toegang kunnen krijgen tot deze informatie.
- De melder mag het doen van een melding of verdere verstrekking van informatie niet afhankelijk maken van de beloning. Het initiatief voor het geven van een beloning bij een melding ligt bij de ontvangende organisatie, die kan hierover randvoorwaarden schetsen in het gepubliceerde beleid.
- Melder en de organisatie maken duidelijke afspraken over openbaarmaking van de kwetsbaarheid. Mochten er meerdere organisaties betrokken zijn, dan is het uitgangspunt dat pas gepubliceerd kan worden als alle organisaties het hiermee eens zijn. Het is hierbij aan te raden deze afspraken al in een vroeg stadium te maken.
- De melder en de betrokken organisatie kunnen afspraken maken over het informeren van de bredere ICT-gemeenschap. Dit kan bijvoorbeeld het geval zijn bij een (nog niet bekende) kwetsbaarheid waarvan bekend is dat die op meer plaatsen aanwezig kan zijn. Het Nationaal Cyber Security Centrum (NCSC) kan hierbij betrokken worden om de doelgroepen Rijksoverheid en vitale infrastructuur te bedienen of om bij een kwetsbaarheid die veel systemen raakt meerdere partijen in te lichten.

4.3 Het NCSC

Primair is het CVD-proces een aangelegenheid die organisaties en melder aangaat. Het NCSC zal desalniettemin het gebruikmaken van een CVD-proces stimuleren. Ook kan het NCSC in samenspraak tussen melder en organisatie betrokken worden om informatie over de kwetsbaarheid met haar doelgroepen te delen om daarmee verdere veiligheidsrisico's die voortvloeien uit de kwetsbaarheid te beperken.

Mocht het melden van de kwetsbaarheid niet gaan zoals de melder hoopt of wanneer de melder liever niet rechtstreeks bij de organisatie melding maken van de kwetsbaarheid, dan kan er contact worden opgenomen met het NCSC[4]. Het NCSC zal dan waar nodig als intermediair optreden.

Op elk moment is de eigenaar van het ICT-systeem verantwoordelijk voor de beveiliging ervan. Het NCSC kan de eigenaar van het systeem niet dwingen een kwetsbaarheid te verhelpen en kan ook niet garanderen dat een eigenaar geen juridische stappen onderneemt tegen de melder. De melder dient daarom bij het zoeken en melden van een kwetsbaarheid rekening te houden met de eerdergenoemde bouwstenen voor organisaties en melders. Van het NCSC mag een melder verwachten dat het haar best doet om de kwetsbaarheid te laten verhelpen en dat ze de melding vertrouwelijk behandelt. Het NCSC deelt geen persoonlijke gegevens tenzij het hiertoe wettelijk verplicht is.

Het NCSC zal, indien mogelijk, de verkregen informatie over kwetsbaarheden in samenspraak tussen organisaties en melders gebruiken om de kennis verder te delen met de ICT-gemeenschap. Dit kan bijvoorbeeld door het openbaar maken van een deel van informatie, het schrijven of bijwerken van een factsheet of whitepaper of het gericht informeren van organisaties.

4 Zie https://www.ncsc.nl/incident-response/responsible-disclosure-melding.html

- Het NCSC zal afhankelijk van de betreffende organisatie en de aard van de geconstateerde kwetsbaarheid zich inzetten om de kwetsbaarheid onder de aandacht van de betreffende organisatie te brengen. De eigenaar van het betreffende systeem blijft echter zelf verantwoordelijk voor het ICT-systeem.
- Het NCSC zal waar mogelijk en nodig de betreffende organisatie voorzien van advies over het verhelpen van de kwetsbaarheid.
- Het NCSC zal meldingen vertrouwelijk behandelen en persoonlijke gegevens van melder of ontvangende organisatie niet delen zonder toestemming, tenzij dat voortvloeit uit een wettelijke verplichting.
- Het NCSC zal de melder zoveel mogelijk op de hoogte houden van de voortgang van het contact met de organisatie en het verhelpen van de kwetsbaarheid.
- Het NCSC zal, in gevallen dat een melding wordt gedaan bij het NCSC, trachten de (potentiële) melder en de organisatie met elkaar in contact te brengen.

Als een melder een kwetsbaarheid heeft gevonden in bijvoorbeeld een softwareproduct of een kwetsbaarheid die veel verschillende systemen raakt, dan kan de melder het NCSC vragen het verhelpen van de kwetsbaarheid en het in de openbaarheid brengen van de kwetsbaarheid te coördineren. Het NCSC zal dan samen met melder, partners, (software)ontwikkelaars en andere security teams helpen bij het analyseren, (laten) verhelpen, coördineren en gecontroleerd in de openbaarheid brengen van de kwetsbaarheid. Dit alles in goed overleg met de melder die de kwetsbaarheid heeft gevonden.

Met een CVD-beleid wordt geprobeerd een balans te vinden tussen het belang om kwetsbaarheden zo snel mogelijk bekend te maken, zodat men maatregelen kan treffen, en het belang van ontwikkelaars en leveranciers om voldoende tijd te hebben de kwetsbaarheid te verhelpen. Het NCSC hanteert voor dit proces een standaardtermijn van 60 dagen tussen melding en publieke bekendmaking. Er kunnen echter omstandigheden zijn waardoor besloten wordt deze termijn te verlengen of in te korten.

Het delen van informatie over de kwetsbaarheid met derden doet het NCSC altijd in overleg met de melder. Hierbij is het van belang dat voor het op een gecoördineerde manier in de openbaarheid brengen van een kwetsbaarheid het NCSC altijd samen moeten werken en dus ook informatie over de kwetsbaarheid moeten delen met belanghebbenden. Hiermee zorgt het NCSC ervoor dat de juiste partijen kunnen werken aan het verhelpen van de kwetsbaarheid, mee kunnen helpen om eventuele schade te beperken en kunnen helpen om de gevonden kwetsbaarheid onder de aandacht te krijgen.

Edwin van Andel

5. Communicatie en het disclosure proces

Vijf jaar praktijkervaring leert dat duidelijke communicatie aan de basis staat van een succesvol CVD-proces. Er zijn aandachtspunten over, tijdens en na het CVD-proces.

Communicatie over het disclosure proces

Het publiceren van een CVD-beleid is een eerste stap in communicatie over het proces. Door een beleid publiek te publiceren wordt er een uitnodiging gedaan aan melders om gevonden kwetsbaarheden te melden bij de organisatie. De organisatie kan randvoorwaarden opstellen voor het onderzoek dat gedaan wordt om kwetsbaarheden te ontdekken en de manier waarop contact gezocht wordt. Daartegenover kan de organisatie zich binden aan het principe om geen aangifte te doen als aan de spelregels van het beleid wordt voldaan. Op die manier wordt de positie van de melder beschermd.

Het CVD-beleid kan op een later moment veranderd of bijgewerkt worden. Hierbij is het van belang om duidelijk te zijn over de wijzigingen. Het is voor melders van belang om te weten wanneer en wat gewijzigd is. Het duidelijk maken van wijzigingen kan bijvoorbeeld door een datum van publicatie op te nemen aan het begin van het CVD-beleid, door een samenvatting van wijzigingen te beschrijven onder het CVD-beleid, of door een archief bij te houden van oude versies van het CVD-beleid.

Het CVD-beleid kan richtlijnen geven over hoe er gecommuniceerd zal worden tijdens het proces, bijvoorbeeld door aan te geven reguliere updates via email of een webportaal. In het CVD-beleid kan worden beschreven hoe een melder bedankt kan worden door vermelding bij een update, opname in een hall of fame, of een andere vorm van beloning.

Communicatie tijdens het disclosure proces

Een melder neemt initiatief tot CVD door een bericht te sturen aan de organisatie. De melder geeft in dit bericht een duidelijke omschrijving van de gevonden kwetsbaarheid. Belangrijke onderdelen daarbij zijn het IP-adres of de URL van het getroffen systeem en de benodigde stappen om een kwetsbaarheid te reproduceren.

Voor de organisatie is het van belang om duidelijk naar de melder te communiceren zodat verwachtingen rondom het proces helder zijn. Dit kan al beginnen door een (automatische) ontvangstbevestiging te sturen, met daarin een indicatie voor de termijn waarop een (eerste) inhoudelijk reactie gestuurd zal worden. In een CVD-beleid kan een indicatie gegeven worden van een oplossingstermijn. Het is ook mogelijk om dit open te laten en een eerste indicatie van de termijn te geven na inhoudelijke beoordeling van de melding. Het is aan te raden om snel duidelijk te zijn over de termijn waarop een oplossing verwacht kan worden. Op die manier weet de melder wat de verwachting kan zijn voor een oplossing.

In sommige gevallen kan het mogelijk zijn dat er voor de melder al een publicatiedatum duidelijk is, bijvoorbeeld door presentatie op een conferentie, of omdat een melder zelf een vaste termijn hanteert. Ook in dit geval is het van belang dat de melder hier duidelijk over communiceert en deze tijdslijn in een zo vroeg mogelijk stadium uitspreekt en duidelijk is over de (on)mogelijkheden om deze datum op te schuiven.

Een melder is vaak iemand die buiten de organisatie staat en geen enkel zicht heeft op de interne processen die in gang gezet worden door een melding. Organisaties kunnen met regelmatige updates de melder op de hoogte houden over de voortgang van het proces. Daarmee blijft voor een melder duidelijk dat er gewerkt wordt aan een oplossing. Indien nodig kan een organisatie tijdens het proces om verduidelijking of testen van een oplossing vragen.

Mocht een organisatie de initiële oplossingstermijn niet kunnen halen, kan overlegd worden met de melder om dit op te schuiven. Regelmatige communicatie kan dit mogelijk in een vroeger stadium duidelijk maken aan een melder.

Hoewel de belangrijkste intentie van CVD is om in samenspraak de kwetsbaarheid op te lossen om daarna mogelijk te publiceren, is het publiek maken van de kwetsbaarheid ('full disclosure') voor een melder altijd een mogelijkheid indien het proces volgens de melder te lang duurt. Dit is de spreekwoordelijke stok achter de deur waar de melder de beschikking over heeft. Deze situatie moet uiteraard zoveel mogelijk voorkomen worden.

Communicatie na afloop van het CVD-proces

Er zijn vele mogelijke redenen waarom melders op zoek gaan naar kwetsbaarheden en die vervolgens via het CVD-proces melden bij organisaties. Een belangrijke reden voor een groot deel van de melders is (publieke) erkenning.

Een dankmelding aan de melder bij een update of opname in een *hall of fame* geeft een melder publieke erkenning. De behoefte aan publieke erkenning geldt echter niet voor alle melders, er zijn ook melders die juist niet publiek bekend willen worden. Bij communicatie door de organisatie is het daarom aan te raden om toestemming te vragen aan de melder voor het noemen van de melder.

Melders kunnen ook zelf besluiten te communiceren over een melding na het afsluiten van het CVD-proces. De melder kan een beschrijving doen van het ontdekkingsproces, anderen waarschuwen over de kwetsbaarheid, enzovoort. Een melder kan besluiten de publicatie ter informatie aan een organisatie voor te leggen. Het CVD-proces is met het wegnemen van de kwetsbaarheid in principe afgerond en het staat de melder dan vrij om hierover te communiceren, tenzij er aanvullende afspraken gemaakt worden in het beleid of tijdens het proces.

Communicatie over het disclosure proces

- Publicatie van CVD-beleid op website
- Duidelijkheid geven over randvoorwaarden (zie ook Hfd 6 voor diverse benaderingen)
  - Beperkingen in onderzoeksmethode
  - Afspraken over communicatie
  - Afspraken over een (eventuele) beloning; Hall of Fame, financiele vergoeding, t-shirt, etc
- Eventuele aanpassingen in het CVD-beleid helder aangeven, inclusief wijzigingsdatum

Communicatie tijdens het disclosure proces

- Melder neemt contact op met de organisatie over een gevonden kwetsbaarheid
- Organisatie maakt verwachtingen helder, zoals de reactietermijn voor een eerste (inhoudelijke) reactie
- Organisatie en melder geven elkaar een indicatie van de (verwachte/gewenste) oplossingstermijn
- Organisatie geeft regelmatig een (proces)update
- Indien nodig bespreken melder en organisatie het inlichten van mogelijk ander geraakte organisaties

Communicatie na afloop van het disclosure proces

- Afspraken over (publieke) erkenning en beloning van de melder
- Communicatieafspraken over publicatie van de gevonden kwetsbaarheid, zoals het ontdekkingsproces en het informeren van andere organisaties

Zawadi Done

6. Voorbeelden Coordinated Vulnerability Disclosure beleid

Er zijn veel verschillende vormen van Coordinated Vulnerability Disclosure beleidsteksten. Het gepubliceerde CVD-beleid fungeert als een uithangbord richting potentiele melders, zorg daarom dat de vorm van dit beleid aansluit bij het beleid en strategie van de organisatie.

Belangrijke elementen in een CVD-beleid zijn:
- Contactmethode voor veilige communicatie
- Randvoorwaarden voor de melder
- Duidelijke verwachtingen voor de afhandeling van een melding
- De manier van belonen voor meldingen
- Versienummer en datum van laatste herziening

Hieronder drie voorbeelden: Veel organisaties in Nederland hebben geput uit het basisvoorbeeld van ResponsibleDisclosure.nl. Andere organisaties nemen meer randvoorwaarden op, zie het voorbeeld van Fox IT. Er zijn ook organisaties die een vrijere vorm nemen om beter aan te sluiten bij hun doelgroep, zie het beleid van Bits of Freedom.

Responsible Disclosure.nl[5]

Bij Acme Corporation 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 horen wij dit graag zodat we zo snel mogelijk maatregelen kunnen treffen. Wij willen graag met u samenwerken om onze klanten en onze systemen beter te kunnen beschermen.

Wij vragen u:

- Uw bevindingen te mailen naar cert@example.com. Versleutel uw bevindingen met onze PGP key om te voorkomen dat de informatie in verkeerde handen valt,
- Het probleem niet te misbruiken door bijvoorbeeld meer data te downloaden dan nodig is om het lek aan te tonen of gegevens van derden in te kijken, verwijderen of aanpassen,
- Het probleem niet met anderen te delen totdat het is opgelost en alle vertrouwelijke gegevens die zijn verkregen via het lek direct na het dichten van het lek te wissen,
- Geen gebruik te maken van aanvallen op fysieke beveiliging, social engineering, distributed denial of service, spam of applicaties van derden, en
- Voldoende informatie te geven om het probleem te reproduceren zodat wij het zo snel mogelijk kunnen oplossen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende, maar bij complexere kwetsbaarheden kan meer nodig zijn.

Wat wij beloven:

- Wij reageren binnen 3 dagen op uw melding met onze beoordeling van de melding en een verwachte datum voor een oplossing,
- Als u zich aan bovenstaande voorwaarden heeft gehouden zullen wij geen juridische stappen tegen u ondernemen betreffende de melding,
- 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. Melden onder een pseudoniem is mogelijk,
- Wij houden u op de hoogte van de voortgang van het oplossen van het probleem,
- In berichtgeving over het gemelde probleem zullen wij, indien u dit wenst, uw naam vermelden als de ontdekker, en
- Als dank voor uw hulp bieden wij een beloning aan voor elke melding van een ons nog onbekend beveiligingsprobleem. De grootte van de beloning bepalen wij aan de hand van de ernst van het lek en de kwaliteit van de melding met een minimum van een waardebon van €50,-.

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

5 Deze tekst is geschreven door Floor Terra en is gepubliceerd onder een Creative Commons Naamsvermelding 3.0 licentie.

Fox-IT

Bij Fox-IT vinden wij de veiligheid van onze systemen, ons netwerk en onze producten erg belangrijk. Ondanks dat wij heel veel zorg besteden aan security, kan het voorkomen dat een zwakke plek wordt ontdekt. Indien dat het geval is, dan horen wij dit graag zo snel mogelijk, zodat we snel maatregelen kunnen treffen.

Zwakke plekken kunnen op twee manieren worden ontdekt: je loopt ergens per ongeluk tegenaan bij normaal gebruik van een digitale omgeving, of je doet expliciet je best om een zwakke plek te vinden.

Ons responsible disclosure-beleid is geen uitnodiging om ons bedrijfsnetwerk uitgebreid actief te scannen op zwakke plekken. Wij monitoren ons netwerk zelf. Hierdoor is de kans groot dat een scan wordt opgepikt, dat ons Security Operation Centre (SOC) hier onderzoek naar gaat doen en er mogelijk onnodige kosten worden gemaakt.

Voor wat betreft onze producten bent u van harte uitgenodigd om in een offline en non-productie omgeving actief op zoek te gaan naar kwetsbaarheden en uw bevindingen aan ons te melden. Uit verantwoording naar onze klanten willen we niet oproepen tot hack-pogingen op hun infrastructuur. Echter, ook hiervoor geldt dat we zo snel mogelijk van u willen vernemen zodra er kwetsbaarheden worden gevonden, zodat wij deze adequaat kunnen verhelpen.

Wij willen graag met u samenwerken om onze klanten en onze systemen beter te kunnen beschermen.

Wij vragen u:

- Uw bevindingen zo snel mogelijk te mailen naar security-alert@fox-it.com.
- Misbruik de zwakheid niet door bijvoorbeeld het downloaden, veranderen of verwijderen van gegevens. Wij nemen uw melding altijd serieus en gaan elk vermoeden van een kwetsbaarheid uitzoeken, ook zonder ‘bewijs’.
- Deel het probleem niet met anderen totdat het is opgelost.
- Maak geen gebruik van aanvallen op fysieke beveiliging, van social engineering of hacking tools, zoals vulnerability scanners.
- Geef ons voldoende informatie om het probleem te reproduceren, zodat wij het zo snel mogelijk kunnen oplossen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende, maar bij complexere kwetsbaarheden kan meer nodig zijn.

Wat wij beloven:

- Wij reageren binnen drie 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. Een uitzondering hierop is politie en justitie, in geval van aangifte of indien gegevens worden opgeëist.
- Wij houden u op de hoogte van de voortgang van het oplossen van het probleem.
- In berichtgeving over het gemelde probleem zullen wij, indien u dit wenst, uw naam vermelden als de ontdekker.
- Het is helaas niet mogelijk bij voorbaat juridische stappen tegen u uit te sluiten. We willen elke situatie apart kunnen afwegen. We achten ons zelf moreel verplicht om aangifte te doen op moment dat we het vermoeden hebben dat de zwakheid of gegevens misbruikt worden, of dat u kennis over de zwakheid met anderen heeft gedeeld. U kunt er op rekenen dat een toevallige ontdekking in onze online-omgeving niet tot aangifte zal leiden.
- Als dank voor uw hulp bieden wij een beloning voor elke melding van een ons nog onbekend beveiligingsprobleem. De grootte van de beloning bepalen wij aan de hand van de ernst van het lek en de kwaliteit van de melding.

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 het probleem, nadat het is opgelost.

Met dank aan Floor Terra voor zijn voorbeeldtekst op http://responsible-disclosure.nl

Bits of Freedom

Onze afhankelijkheid van onze digitale infrastructuur wordt alleen maar groter. Dat geldt voor de maatschappij als geheel, maar ook voor onszelf. We vinden daarom dat overheden en organisaties (en wijzelf dus ook) sterk moeten inzetten op de beveiliging van onze digitale infrastructuur. We realiseren ons ook dat het, ondanks de beste bedoelingen en zorg, kan gebeuren dat er in de beveiliging van systemen een kwetsbaarheid voorkomt. Als jij een zwakke plek in één van onze systemen vindt, dan horen we dat heel graag. Wij kunnen dan de kwetsbaarheid oplossen.

Wat wij van jou verwachten:

- Als je een kwetsbaarheid in een van onze systemen onderzoekt, hou je rekening met proportionaliteit van de aanval. Je hoeft niet aan te tonen dat als je de grootste DDoS-aanval uit de historie van het internet op onze website uitvoert, we even niet meer bereikbaar zijn. Dat weten we. Ook begrijpen we dat als je met een shovel ons kantoor inrijdt, je waarschijnlijk wel een laptop buit kunt maken.
- Die proportionaliteit speelt ook een rol bij het aantonen van de kwetsbaarheid zelf. Je bekijkt of verandert niet meer gegevens dan strikt noodzakelijk om de kwetsbaarheid aan te tonen. Als je bijvoorbeeld onze voorpagina kunt aanpassen, voeg je ergens een non-controversieel woord toe, in plaats van de volledige pagina over te nemen. Als je toegang weet te krijgen tot een database, volstaat een lijstje van de tabellen of de eerste regel uit één van die tabellen.
- Een kwetsbaarheid in een van onze systemen meld je zo spoedig mogelijk door een e-mail te sturen aan security@bof.nl. Bij voorkeur verstuur je de melding versleuteld met OpenPGP. Je voorziet de melding van voldoende informatie waarmee wij het probleem kunnen reproduceren en onderzoeken.
- Je deelt de kennis over de kwetsbaarheid niet met anderen zolang wij de kwetsbaarheid nog niet hebben opgelost en de redelijke oplossingstermijn niet al ruimschoots is verstreken.
- Je verwijdert alle vertrouwelijke gegevens die je hebt verkregen in je onderzoek direct nadat wij de kwetsbaarheid hebben opgelost.

Wat je van ons mag verwachten:

- We reageren binnen drie dagen inhoudelijk op je melding, inclusief de verwachte oplossingstermijn. Uiteraard houden we je ook daarna regelmatig op de hoogte van de voortgang van het oplossen van het probleem.
- We lossen de kwetsbaarheid zo snel mogelijk op. Ook hier speelt proportionaliteit een belangrijke rol: de termijn voor het oplossen van een kwetsbaarheid is afhankelijk van verschillende factoren, waaronder de ernst en de complexiteit van de kwetsbaarheid.
- Als je je aan bovenstaande verwachtingen houdt, zullen wij geen juridische stappen tegen je ondernemen ten aanzien van je melding.
- We vinden het belangrijk om je de credits te geven die je toekomen – en die je wenst. We zullen je naam bij een publicatie over de kwetsbaarheid alleen vermelden als je daarmee instemt.
- Als dank voor je hulp in het beter beschermen van onze systemen, belonen we je graag voor de melding van een tot dan toe ons nog onbekende kwetsbaarheid. De beloning is afhankelijk van de ernst van de kwetsbaarheid en de kwaliteit van de melding.
- Mocht je een kwetsbaarheid vinden in software die wij gebruiken maar die door een andere partij gemaakt wordt en die kwetsbaarheid valt onder een bug bounty program, dan is een eventuele bounty uiteraard voor jou.

Versie 1.0 van 23 juni 2017.

Uitgave
Nationaal Cyber
Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

Fotografie
Tobias Groenland |
hackershandshake.com

oktober 2018