CEG Information Security

Responsible Disclosure

Implementatiehandleiding

Publicatie van de CIO Experience Group Information Security

CIO Platform Nederland, februari 2016

www.cio-platform.nl/publicaties

Inhoudsopgave

1 Inleiding

Het voeren van een Responsible Disclosure beleid kan grote impact hebben op de bedrijfsvoering van een organisatie. Het is daarom van belang dat de invulling van het Responsible Disclosure beleid en de procedure zorgvuldig worden afgewogen.

Het CIO Platform Nederland heeft een Responsible Disclosure modelbeleid en een operationele procedure voor Responsible Disclosure opgesteld voor bedrijven en organisaties. Deze handleiding is ontwikkeld als handvat voor een gedegen invulling van het beleid en de procedure.

Deze implementatiehandleiding is bestemd voor de verantwoordelijke voor het formuleren van het informatiebeveiligingsbeleid van een organisatie. De implementatiehandleiding is een middel om te komen tot een gedegen invulling van het Responsible Disclosure beleid.

Er zijn voorbeelden uit de praktijk bekend waar een ongewenst resultaat de uitkomst is van een onjuist opgesteld beleid en procedure. Zo kan een niet goed geformuleerde beloningsstructuur er toe leiden dat er (professionele) premiejagers worden aangetrokken die met grote regelmaat een melding doen met als reden zo veel mogelijk beloningen te innen. Ook kunnen spelregels die de eisen omtrent publicatie niet goed beschrijven, grote irritatie opwekken bij de melder van een kwetsbaarheid die zijn bevindingen bijvoorbeeld wil presenteren op een beveiligingsconferentie.

Het doel van Responsible Disclosure omvat het volgende:

a) Draagt ertoe bij dat kwetsbaarheden die door externe personen worden geïdentificeerd, bekend worden gemaakt aan jouw organisatie
b) Draagt ertoe bij dat een kwetsbaarheid kan worden geadresseerd voordat deze wordt geëxploiteerd en publiek bekend wordt gemaakt
c) Geeft invulling aan de verantwoordelijkheid van jouw organisatie om goed om te gaan met persoonlijke informatie van klanten e.a.
d) Geeft inzicht en richting aan de juridische- en communicatie stappen die jouw organisatie zal nemen rond melding van kwetsbaarheden.

1.1 Definitie Responsible Disclosure

Er worden uiteenlopende definities gebruikt voor Responsible Disclosure. De definitie die gebruikt is bij het opstellen van dit document, is de definitie van het Nationaal Cyber Security Center (NCSC): “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”. Uit de definitie van het NCSC blijkt dat er pas sprake is van Responsible Disclosure als een organisatie een beleid heeft. [https://www.ncsc.nl/actueel/Responsible+Disclosure+Leidraad]

1.2 Leeswijzer

In hoofdstuk 2 zijn de argumenten voor het inzetten van Responsible Disclosure beschreven. Vervolgens is de positionering van het modelbeleid en de procedure aangeven in hoofdstuk 3. In hoofdstuk 4 wordt nader ingegaan op de afstemming met betrokken partijen. In hoofdstuk 5 zijn de beslissingspunten voor Responsible Disclosure beschreven en wordt per beslissing een overweging beschreven die meegenomen kan worden in de besluitvorming door de organisatie. In hoofdstuk 6 staat een stappenplan die gebruikt kan worden om de implementatie van Responsible Disclosure te plannen.

1.3 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.

2 Argumenten voor Responsible Disclosure beleid

ICT speelt bij alle organisaties een steeds belangrijker rol en steeds meer dienstverlening verloopt via Internet. Een organisatie wordt geacht om informatie op een betrouwbare manier te beheren. Om het belang van Responsible Disclosure voor organisaties aan te geven zijn er hieronder een aantal argumenten opgesomd:

2.1 Verlagen drempel melder

Een organisatie kan de drempel tot melden van kwetsbaarheden voor haar doelgroep verlagen.

2.2 Spelregels vastleggen

De handelingen die een onderzoeker uitvoert om kwetsbaarheden aan te tonen kunnen volgens het Nederlandse strafrecht[1] te ver gaan, maar vanwege maatschappelijke belangen toch verantwoord zijn. De organisatie kan aangeven hoe ver een melder mag gaan bij het uitvoeren van zijn onderzoek door in een Responsible Disclosure beleid aan te geven wat de organisatie verwacht van de melder. Op deze manier wordt er duidelijkheid verschaft in het “grijze gebied” van de wetgeving met betrekking tot Responsible Disclosure.

2.3 Vertrouwen

Een organisatie verwerkt veel gegevens van klanten. Daarmee moet zorgvuldig worden omgegaan. Elke bijdrage aan het vergroten van de veiligheid van deze gegevens is relevant en draagt bij aan het vertrouwen van de klant.

2.4 Gemeenschappelijk belang

ICT heeft groeiende invloed op de maatschappij. De potentiële impact van kwetsbaarheden op gebruikers is groot. Een belangrijke drijfveer voor melders is het aan de kaak stellen van kwetsbaarheden en risico’s vanwege het maatschappelijk belang. Responsible Disclosure is een oplossing om op een

[1] In deze publicatie wordt uitgegaan van het Nederlandse recht. Check in elk land waarin je dit beleid wil toepassen op specifieke wetten en regelgeving, want dat kan anders zijn.

maatschappelijk verantwoorde en effectieve wijze om te gaan met kwetsbaarheden.

2.5 Verhogen informatiebeveiligingsniveau

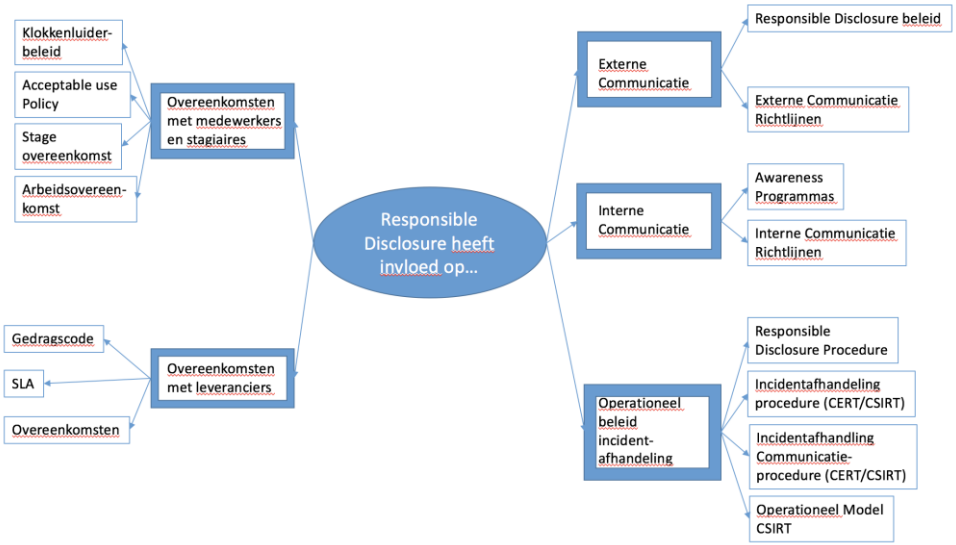
Een organisatie heeft nooit alle kennis in huis. Responsible Disclosure kan ingezet worden om gebruik te maken van kennis over kwetsbaarheden die buiten de organisatie aanwezig is. Door de mogelijkheid te bieden om op verantwoorde wijze een kwetsbaarheid te melden wordt het voor goedwillende beveiligingsonderzoekers mogelijk een bijdrage te leveren aan het verhogen van het informatiebeveiligingsniveau van de organisatie.

2.6 Trend

Responsible Disclosure wordt steeds meer branche breed in Nederland gehanteerd. Voorbeelden waarbij Responsible Disclosure branche breed wordt gestimuleerd zijn de Nederlandse rijksoverheid, de grote Nederlandse telecomproviders, de Nederlandse banken en de Dutch Hosting Provider Association. Ook buiten Nederland groeit de interesse in deze vorm van kennisdelen.

3 Positionering

Responsible Disclosure kan een grote invloed hebben op de bedrijfsvoering van een organisatie. Om ervoor te zorgen alle betrokkenen op de juiste manier op de hoogte worden gesteld en mee kunnen werken aan een Responsible Disclosure melding moet Responsible Disclosure beleid aansluiten op bestaande beleidstukken, procedures en overeenkomsten. In figuur 1 is de positionering van het Responsible Disclosure beleid grafisch weergegeven. [NB. Niet elke organisatie heeft al deze elementen, aanpassen naar eigen organisatie en omgeving]



Figuur 1

3.1 Intern

3.1.1 Operationele beleidsstukken voor incidentmanagement

Een Responsible Disclosure beleid heeft veel overeenkomsten met incidentmanagement. Voor een groot deel kunnen beide beleidstukken zelfs gelijk zijn. Het grootste verschil met een normale incidentprocedure zijn de extensieve communicatie met melder en de afhandeling van openbaring en

beloning. Door de onderdelen schade indamming, beoordeling van de blootstelling en remediatie en herstel van het Responsible Disclosure beleid af te stemmen op het incidentmanagement wordt voorkomen dat er grote overlap tussen het beleid ontstaat.

3.1.2 Afspraken over communicatie

De organisatie wordt geacht de melder en overige betrokkenen op de hoogte te houden van de voortgang van het proces. De belangen van de melder kunnen soms in strijd zijn met de belangen van de organisatie. Daarnaast kunnen meldingen van sterk technische aard zijn waardoor het noodzakelijk is om de communicatie direct via technisch operationeel personeel te laten verlopen. Het is daarom van groot belang om beleidsregels vast te stellen met betrekking tot de communicatie van de melder.

3.1.3 Klokkenluidersregeling

Meldingen over organisatorische misstanden kunnen eventueel afgedekt zijn via een klokkenluidersregeling, meldingen over een (technische) kwetsbaarheid in de systemen van de organisatie vallen hier vaak niet onder. Het model voor een klokkenluidersregeling van de rijksoverheid en de verklaring van de Stichting van de Arbeid zijn voorbeelden van een klokkenluidersregeling. Beide modellen voorzien niet in de bescherming van medewerkers in het geval van een Responsible Disclosure melding door een medewerker.

3.2 Extern

3.2.1 Afspraken met leveranciers

Naast de betrokkenheid van de melder kunnen er ook andere derden betrokken zijn bij een melding van een kwetsbaarheid. Te denken valt aan een hostingprovider waarop de kwetsbare website draait of een fabrikant van een kwetsbaar netwerkelement. De handelingen van een melder kunnen impact hebben op de betrouwbaarheid van een systeem van een derde partij. Door vooraf afspraken te maken met leveranciers, aan de hand van inkoopvoorwaarden met betrekking tot Responsible Disclosure, weet een leverancier dat de organisatie een Responsible Disclosure beleid hanteert en kan de leverancier daar zijn beleid en organisatie op afstemmen. Dit voorkomt eventuele problemen bij de gewenste snelle aanpak van een kwetsbaarheid of

civiele stappen van de leverancier richting de melder.

3.2.2 Afspraken met gebruikers

Een organisatie is verantwoordelijk voor het beheer van gevoelige informatie van klanten en medewerkers, zoals salarisstroken, personeelsdossiers e.d. Afspraken met de medewerkers, en eventueel met klanten over de omgang met deze informatie, en de rechten en plichten kunnen onder andere worden vastgelegd in een arbeidsovereenkomst, overeenkomsten met leveranciers en klanten of eventueel een Acceptable Use Policy (gebruiksreglement voor informatievoorzieningen voor werknemers en gebruikers). Aangezien de melder van een kwetsbaarheid zichzelf mogelijk ook toegang verschaft tot informatie over klanten of medewerkers is het belangrijk om deze partijen te informeren over de eventuele impact van Responsible Disclosure. Daarnaast kan er voor worden gekozen om Responsible Disclosure terug te laten komen in deze documenten om discussie of een civiele zaak tussen klant/medewerker en de melder te voorkomen.

3.2.3 Externe communicatie

Responsible Disclosure is een middel om de drempel tot melden van een kwetsbaarheid te verlagen en spelregels vast te stellen voor het onderzoeken van kwetsbaarheden. De melder moet op de hoogte gesteld worden dat de organisatie een Responsible Disclosure beleid hanteert. Daartoe zal het Responsible Disclosure beleid vindbaar op de website worden gepubliceerd.

Bovendien is het voor de organisatie relevant om een goede relatie te onderhouden met de melder van een kwetsbaarheid. Daartoe is externe communicatie ook van belang.

4 Afstemming betrokken partijen

Bij het opstellen van Responsible Disclosure beleid moet er rekening worden gehouden met meerdere factoren en er moeten afspraken worden vastgelegd. Dit hoofdstuk beschrijft de ketenstructuur van het Responsible Disclosure proces, de verantwoordelijkheden die moeten worden belegd en welke beslissingen er gemaakt moeten worden.

4.1 Ketenstructuur

De implementatie van Responsible Disclosure stopt niet bij de organisatie zelf. Een melding over een kwetsbaarheid heeft vaak niet alleen betrekking op de organisatie, maar ook op partijen waarmee de organisatie te maken heeft. Voordat een Responsible Disclosure beleid wordt geïmplementeerd is het goed om na te denken over afstemming met deze partijen. Hierbij valt te denken aan:

- Leveranciers van webhosting, clouddiensten, netwerkapparatuur, softwarelicenties, etc.
- Medewerkers via bijvoorbeeld een ondernemingsraad

4.2 Afstemming interne stakeholders

Het is van belang dat er afstemming met stakeholders plaatsvindt om het Responsible Disclosure proces zo adequaat mogelijk in te richten. Voor het vaststellen van beleid en procedure moeten er in ieder geval de volgende groepen worden geraadpleegd, dit kan per bedrijf verschillen.

Wie	Waarom
Verantwoordelijke voor de afhandeling van ICT-incidenten ((bijvoorbeeld CERT/CSIRT)	De procedure voor Responsible Disclosure hangt nauw samen met de afhandeling van ICT-incidenten. Vaak zal het voornaamste deel van de afhandeling van een Responsible Disclosure melding afgehandeld worden door deze partij
Juridische afdeling	Responsible Disclosure heeft vaak juridische implicaties tussen de organisatie en de melder. Door de juridische afdeling in het proces te betrekken, kan voorkomen worden dat een melding grote gevolgen heeft voor de organisatie of melder.
Eindverantwoordelijke informatiebeveiliging (CISO)	De eindverantwoordelijke voor informatiebeveiliging is vaak ook de verantwoordelijke voor het Responsible Disclosure proces.
ICT-helpdesk	Een helpdesk of servicedesk is vaak het eerste aanspreekpunt voor klanten en medewerkers als er problemen zijn met geautomatiseerde werken.
Bestuur	Net als bij incidentafhandeling speelt het hebben van mandaat een grote rol. Er moet een handelsbevoegdheid zijn om bijvoorbeeld op de juiste manier te kunnen ingrijpen of de melder te belonen.
Communicatieafdeling	Communicatie speelt een grote rol bij Responsible Disclosure en kan van invloed zijn op het imago van de organisatie. Niet alleen de communicatie tussen melder en organisatie, maar ook de communicatie naar de gebruikers, medewerkers, ICT community en buitenwereld moet goed worden afgestemd.

5 Invulling Responsible Disclosure beleid

Bij de implementatie van Responsible Disclosure moet voor de organisatie worden bepaald welke exacte invulling voor het beleid en de procedure gewenst is. Om de afwegingen die moeten worden gemaakt concreet te maken zijn er een breed aantal stappen geformuleerd. Aan de hand van de invullingen binnen de organisatie kunnen de stappen worden aangepast.

5.1 Beleggen verantwoordelijkheden

Net zoals bij elk beleid is het ook voor Responsible Disclosure van belang om verantwoordelijkheden vast te leggen.

Een aantal verantwoordelijkheden moeten in ieder geval belegd worden om Responsible Disclosure tot een succes te maken:

- In eerste instantie bepalen van de ernst en validiteit van de melding
- Bepalen van het verdere verloop van de melding als de melding ernstig blijkt (bijvoorbeeld een lek van persoonsgegevens)
- Toezien op de kwaliteit van de afhandeling van de melding
- Toezien op het tijdspad van de afhandeling van de melding
- Communicatie met de melder
- Bepalen van de termijn waarop bekendmaking van (individuele) melding plaatsvind
- Toekennen van de beloning
- Akkoord geven voor publicatie
- De eindverantwoordelijkheid voor het Responsible Disclosure proces

Bij het beleggen van de verantwoordelijkheden dient extra aandacht te worden besteed aan de communicatie tussen de verschillende organisatorische lagen. In de praktijk is het voorgekomen dat een melder na het doen van een Responsible Disclosure melding alsnog de pers opzoekt om de kwetsbaarheid openbaar te maken omdat de communicatie tussen verschillende afdelingen niet goed was afgestemd. Hierdoor was het mogelijk dat het voor de organisatie niet duidelijk was waar de melding was opgepakt en hoe de voortgang van de behandeling van de melding verliep.

5.2 Scope Responsible Disclosure beleid

Bepaal op welke producten en diensten het beleid betrekking heeft in jouw

organisatie.

Overweging(en):

Wanneer alle applicaties en de infrastructuur worden meegenomen in de scope, kan dit leiden tot veel meldingen. Bij beperkingen, bijvoorbeeld alleen webapplicaties, kunnen belangrijke bevindingen op bijvoorbeeld een offline applicatie verloren gaan.

5.3 Manier van melden

5.3.1 Wijze van ontvangst

Bepaal op welke wijze jouw organisatie meldingen wil ontvangen.

Denk hierbij aan:

- E-mail
- Post
- Digitaal formulier (al dan niet via SSH)
- Telefoon

Overweging(en):

Bij het melden via een digitaal formulier kan bij de melder worden afgedwongen dat bepaalde zaken worden vermeld, zoals contactgegevens.

De drempel kan hierdoor hoger zijn om een melding daadwerkelijk te doen. Dit is bij het melden via e-mail en telefoon minder aan de orde. Wanneer versleuteling bij e-mail noodzakelijk wordt geacht wordt deze drempel voor sommige melders wel weer hoger.

Meldingen met betrekking tot kwetsbaarheden in systemen met vertrouwelijke informatie moeten vertrouwelijk behandeld worden. Vaak is versleuteling van de informatie-uitwisseling volgens het informatiebeveiligingsbeleid dan noodzakelijk.

5.3.2 Anoniem of niet?

Bepaal of er anoniem gemeld mag worden.

Je kan hierin een keuze maken:

- De melding kan zowel anoniem, onder een pseudoniem of via een tussen-/vertrouwenspersoon gedaan worden
- Meldingen onder een pseudoniem, anoniem of via een tussen-/vertrouwenspersoon worden niet aangenomen
- Meldingen kunnen zowel anoniem als onder een pseudoniem gemeld worden Meldingen via een tussen-/vertrouwenspersoon zijn niet toegestaan en worden niet behandeld
- Meldingen worden alleen aangenomen wanneer contact mogelijk blijft, dus onder een pseudoniem of geheel bekend

Overweging(en):

Anoniem melden kan communicatie verhinderen en daarmee afstemming, beloning en eventuele informatie uitwisseling i.h.g.v. onduidelijkheden onmogelijk maken. Daarnaast verhindert of bemoeilijkt het de opsporingsmogelijkheden bij het mogelijk overtreden van de spelregels van het Responsible Disclosure beleid. Tot slot geeft een anonieme melding mogelijk geen goed beeld van de persoon die achter de melding zit en daarmee is mogelijk de intentie van de melder minder zichtbaar.

Een voordeel van anoniem melden is dat de drempel voor de melder laag is. Hiermee wordt voorkomen dat een melder die liever anoniem wil blijven besluit om naar de pers te stappen of kiest voor full disclosure.

5.3.3 Snelheid van bevestigen

Bepaal hoe snel jouw organisatie een bevestiging van ontvangst van de melding moet sturen aan de melder.

Je kan hierin een keuze maken:

- Binnen 1 werkdag
- Binnen 2 werkdagen
- Binnen 3 werkdagen
- Binnen een week

Overweging(en):

Een snelle reactie naar de melder geeft de indruk dat de melding serieus genomen wordt. Door als organisatie de verplichting te stellen dat er snel een reactie verstuurd moet worden naar de melder kan een snellere verwerking van meldingen gestimuleerd worden. Doordat de melder het gevoel heeft dat hij serieus genomen wordt, kan voorkomen worden dat de melder alsnog naar de pers wordt stapt of gebruik maakt van full disclosure.

5.4 Afzien van vervolging

Bepaal voor jouw organisatie of je afziet van vervolging wanneer de melder de spelregels uit het Responsible Disclosure beleid heeft nageleefd.

Je kan hierin een keuze maken:

- Ja of Nee

Overweging(en):

Wanneer er expliciet in het beleid wordt vermeld dat er wordt afgezien van vervolging kan dit de melder gerust stellen en is de kans groter dat een melding wordt gedaan. Echter is het wel van belang om duidelijk te vermelden dat het altijd mogelijk is dat er voor de organisatie wettelijke verplichtingen zijn om juridische stappen te nemen.

Als het niet expliciet wordt vermeld verminderd dit mogelijk risico tot verplichte juridische stappen en het in strijd zijn met het Responsible Disclosure beleid.

Uitgangspunt binnen de organisatie dient bij het volgen van de spelregels wel het afzien van vervolging te zijn.

5.5 Meldingen met impact op derden

Bepaal voor jouw organisatie hoe er gehandeld moet worden in het geval dat er een melding wordt gedaan over jouw systeem die ook impact heeft op een systeem van derden, waarbij de derde partij *geen* Responsible Disclosure beleid hanteert.

Je kan hierin een handelingskeuze maken:

- Er wordt overlegd met de melder wat er moet gebeuren
- Jouw organisatie bemiddelt tussen de melder en de mogelijk getroffen partij
- De melding moet door jouw organisatie worden doorgegeven aan de mogelijk getroffen partij

Overweging(en):

Wanneer de melder wordt betrokken bij het besluit voor vervolgstappen blijft de verantwoordelijkheid bij de melder en is aan hem/haar de keuze om contact op te nemen met de derde partij.

Bemiddeling tussen organisatie en mogelijk getroffen partij draagt bij een maatschappelijke verantwoording aan de melder dat het eventuele probleem wordt opgelost en aan de derde partij dat het probleem, wat zij mogelijk heeft, wordt gemeld.

Indien de melding wordt doorgegeven aan de mogelijk getroffen partij kan het probleem snel worden opgelost. Echter moet nog wel de keuze gemaakt worden om de melder anoniem te houden.

Bepaal hoe jouw organisatie handelt in het geval dat de melder van een kwetsbaarheid vindt in een systeem van een derde partij en dit meldt aan jouw organisatie? Betekent dit dat het Responsible Disclosure proces wordt beëindigd omdat de melding niet van toepassing is op de systemen van jouw organisatie?

Je kan hierin een handelingskeuze maken:

- Er wordt overlegd met de melder wat er moet gebeuren
- Jouw organisatie bemiddelt tussen de melder en de mogelijk getroffen partij
- De melding moet door jouw organisatie worden doorgegeven aan de mogelijk getroffen partij

Overweging(en):

Wanneer de melder wordt betrokken bij het besluit voor vervolgstappen blijft de verantwoordelijkheid bij de melder en is aan hem/haar de keuze om contact op te nemen met de derde partij.

Bemiddeling tussen organisatie en mogelijk getroffen partij draagt bij een maatschappelijke verantwoording aan de melder dat het eventuele probleem wordt opgelost en aan de derde partij dat het probleem, wat zij mogelijk heeft, wordt gemeld.

Indien de melding wordt doorgegeven aan de mogelijk getroffen partij kan het probleem snel worden opgelost. Echter moet nog wel de keuze gemaakt worden om de melder anoniem te houden.

5.6 Opleggen beperkingen

Bepaal hoe ver de melder mag gaan in zijn onderzoek.

Je kan hierin een handelingskeuze maken:

- Je vermeldt expliciet wat wel en niet is toegestaan
- Je geeft een duidelijke lijn aan waar de melder zich aan moet houden
- Je geeft geen richtlijn mee

Overweging(en):

Wanneer expliciete regels worden vermeld wat wel en niet mag kan dit tegenwerken voor de melder. De melder kan zich beperkt voelen en wanneer de melder een stap heeft genomen die niet toegestaan is volgens de regels maar hier geen schade mee heeft aangericht, kan de melder besluiten geen melding te doen in verband met eventuele vervolging. Echter creëert dit wel duidelijke, meetbare regels en draagt bij aan verwachtingsmanagement.

Duidelijkheid kan ook worden geboden door een lijn aan te geven waaraan de melder zich moet houden. Hierin worden geen strenge regels opgelegd maar bijvoorbeeld wel van de melder gevraagd geen data te wijzigen of verwijderen en kunnen er enkele beperkingen worden opgelegd.

Bij het geheel vrijlaten kan misverstand ontstaan over wat billijk is. Echter kan de melder wel alle kwetsbaarheden aantonen en melden.

5.7 Belonen melder

Bepaal of de melder beloond moet worden.

Keuzes varieren van:

- Ja, door middel van een geldelijke beloning of in de vorm van waardebonnen
- Ja, in natura zoals een t-shirt, rondleiding, seminar of een uitnodiging voor een presentatie
- Ja, door een plek op de Hall of Fame van de organisatie
- Nee, geen beloning
- Etc….

Overweging(en):

Er moet overwogen worden wat de eventuele financiële mogelijkheden zijn voor de organisatie.

Bij het uitkeren van een geldelijke beloning is de kans op melders die handelen vanuit financieel oogpunt groter. Dit betekent meer meldingen wat ook meer geld en tijd kost voor de organisatie. De kans op nuttige meldingen van hoge kwaliteit wordt echter wel vergroot.

Ethische melders handelen echter vaak vanuit maatschappelijk belang of voor het opbouwen van een goede reputatie. Hieruit zou geconcludeerd kunnen worden dat het geven van een niet geldelijke beloning de kans op alleen ethische melder wordt vergroot.

5.7.1 Persoonsgegevens

Bepaal hoe om moet worden gegaan met meldingen van kwetsbaarheden waarbij persoonsgegevens verkregen zijn.

Wanneer expliciet wordt vermeld dat het niet is toegestaan dat er persoonsgegevens worden verkregen kan dit een melder afhouden om een melding te doen als de melder niet opzettelijk persoonsgegevens heeft verkregen bij het vinden van een lek.

Welke keuzes kan jouw organisatie daarin maken?

- Jouw organisatie kan dit te allen tijde niet toestaan. Als er toch persoonsgegevens worden bemachtigd wordt er aangifte gedaan tegen de melder
- De melding behandelen als een normale melding, met in achtneming van wettelijke meldingsplichten
- Het per geval bekijken, als er bijvoorbeeld geen sprake is van braak maar slecht geïmplementeerde software kan dit niet te wijten zijn aan de melder

Overweging(en):

Wanneer expliciet wordt vermeld dat het niet is toegestaan als er persoonsgegevens worden verkregen kan dit een melder afhouden om een melding te doen als de melder niet opzettelijk persoonsgegevens heeft verkregen bij het vinden van een lek.

5.7.2 Afspraken met derden

Bepaal of er afspraken gemaakt moeten worden met leveranciers en/of gebruikers met betrekking tot Responsible Disclosure.

Overweging(en):

Ondersteuning van leveranciers kan nodig zijn bij het oplossen van een kwetsbaarheid. Daarnaast kan een kwetsbaarheid worden gemeld van een systeem van een leverancier. Het is daarom nuttig om van te voren afspraken te maken met leveranciers over bijvoorbeeld oplostijd van kwetsbaarheden.

Melders kunnen tijdens het doen van onderzoek naar de kwetsbaarheid mogelijk toegang krijgen tot gegevens van gebruikers van de systemen zoals eigen medewerkers. Het kan daarom nuttig zijn om afspraken te maken of in ieder geval de gebruikers op hoogte te stellen van het Responsible Disclosure beleid wat wordt gehanteerd.

6 Stappenplan implementatie Responsible Disclosure

In globale stappen uitgelegd hoe een implementatie traject voor een organisatie er uit zou kunnen zien.

1. **Vaststellen gereedheid organisatie**
   Responsible Disclosure is alleen succesvol als een organisatie adequaat kan reageren op de melding van een kwetsbaarheid. Het ontbreken van een ICT-incidentprocedure of ontbreken van mandaat voor het afsluiten van producten of diensten kunnen tekenen zijn dat een organisatie nog niet klaar is voor Responsible Disclosure. Als een organisatie de meldingen niet adequaat kan oppakken, kan dit betekenen dat een melder er voor kiest om de kwetsbaarheid alsnog kenbaar te maken via de media of full disclosure.
2. **Bepalen beslissingspunten**
   De invulling van een Responsible Disclosure beleid kan invloed hebben op het imago van de organisatie. Aan de hand van hoofdstuk 5 van dit document kan een organisatie de belangrijkste beslissingspunten bepalen, zoals scope, toegestane aanvalstechnieken en beloning melder.
3. **Overeenstemming bereiken met betrokkenen (leveranciers, medewerkers/gebruikers, legal, communicatie, etc.)**
   Het invoeren van een Responsible Disclosure beleid heeft invloed op de organisatie, degenen waarop de gegevens betrekking heeft en de betrokken leveranciers van diensten, hardware en software. Het is goed om de invoering van Responsible Disclosure, vanwege de eventuele impact, met deze partijen af te stemmen.
4. **Opstellen Responsible Disclosure beleid en procedure**
   De organisatie kan aan de hand van het “Modelbeleid en Procedure Responsible Disclosure” een beleid en procedure opstellen.
5. **Voorleggen aan bestuur van de organisatie**
   Responsible Disclosure kan van invloed zijn op de organisatorische inrichting van een organisatie. Daarnaast is het belangrijk dat er mandaat wordt gegeven aan degene die is belast met de uitvoering van Responsible Disclosure om adequaat handelen te stimuleren. In bijlage A staat een managementsamenvatting die gebruikt kan worden om Responsible Disclosure voor te leggen aan het bestuur van de organisatie.

6. **Intern communicatie beleid en procedure**
   Omdat er bij Responsible Disclosure verschillende interne partijen betrokken kunnen zijn, zoals de ICT afdeling, juridische afdeling en communicatie, moet duidelijk worden gemaakt welke verantwoordelijkheden zijn belegd en hoe er gehandeld dient te worden. Het benoemen van Responsible Disclosure tijdens een awareness training voor personeel kan nuttig zijn aangezien men meer bewust wordt van informatiebeveiliging en mogelijk kwetsbaarheden sneller herkent.
7. **Oefenmelding sturen**
   Met behulp van een oefenmelding kunnen aspecten zoals mandaat, tijdige afhandeling, communicatie en de samenwerking tussen de verschillende actoren worden gemeten.
8. **Evalueren**
   Aan de hand van de resultaten van de oefenmelding kunnen er eventueel aanpassingen worden gemaakt in het beleid en de procedure.
9. **Publiceren Responsible Disclosure beleid**
   Het Responsible Disclosure beleid moet duidelijk zichtbaar zijn voor melders. Hierbij kan gedacht worden aan een extra link op de contactpagina of een verwijzing op de security pagina van een website.

Bijlage A: Template aanbiedingsbrief

De basis voor het Responsible Disclosure beleid is de “Leidraad om te komen tot een praktijk van Responsible Disclosure” van het Nationaal Cyber Security Centrum (NCSC) uit 2013. Daarnaast is er gebruik gemaakt van best practices van de overheid, de financiële sector en de telecommunicatiesector.

Wat is een Responsible Disclosure beleid?

Er bestaan voor melders van ICT-kwetsbaarheden meerdere manieren om kwetsbaarheden bekend te maken. Een kwetsbaarheid kan direct aan het publiek bekend gemaakt worden (full disclosure) of het kan op een meer besloten en verantwoorde manier gebeuren (Responsible Disclosure). Responsible Disclosure is een strategie gericht op het oplossen en verhelpen van een kwetsbaarheid en gericht op het voorkomen van uitbuiting van de kwetsbaarheid. Dit kan verankerd worden in beleid.

Door, als organisatie, beleid op te stellen met betrekking tot het verantwoord melden van ICT-kwetsbaarheden wordt er duidelijkheid verschaft in wat er van de melder en organisatie verwacht wordt. In het beleid wordt aangegeven hoe ver de melder mag gaan bij het onderzoeken van een kwetsbaarheid en wordt er aangegeven dat de organisatie afziet van juridische stappen als er wordt gehandeld in overeenstemming met de spelregels uit het beleid. De melder weet dus wat hij aan de organisatie heeft en vice versa.

Waarom een Responsible Disclosure beleid?

Bij het onderzoeken van een kwetsbaarheid handelt een ethische hacker al snel in strijd met de Wet Computercriminaliteit. In deze wet wordt echter geen rekening gehouden met het ethisch motief van de melder en is voor de melder vaak niet duidelijk hoe ver hij mag gaan. Hierdoor ontstaat er voor de melder een drempel om een kwetsbaarheid bij een organisatie te melden. Melders kunnen er dan voor kiezen om een kwetsbaarheid anoniem via de pers te melden om op deze manier bronbescherming te genieten. Een melding via de pers kan er voor zorgen dat de kwetsbaarheid uitgebuit wordt of dat er imagoschade ontstaat voor de organisatie.

Eind 2012 heeft de minister van Veiligheid en Justitie ‘een leidraad om te komen

tot een praktijk van Responsible Disclosure' opgesteld. Deze leidraad geeft richtlijnen voor het vaststellen van een beleid voor het op verantwoorde wijze openbaar maken van ICT-kwetsbaarheden. Het ministerie van Veiligheid en Justitie geeft aan dat Responsible Disclosure primair een aangelegenheid is tussen de melder en de betrokken organisatie. Het Openbaar Ministerie heeft daarnaast een intern beleidsstuk gepubliceerd dat in lijn is met de leidraad Responsible Disclosure. Er is geen wetgeving die direct voorziet in Responsible Disclosure. Organisatie worden dus geacht zelf beleid op te stellen ten aanzien van Responsible Disclosure. Dit voorstel voorziet in de implementatie van een dergelijk beleid.

Een korte samenvatting van de procedure die onderdeel is van het Responsible Disclosure beleid:

Meldingen van ICT-kwetsbaarheden komen binnen bij het <<*CERT*>> en worden vervolgens doorgezet naar de <<*Security Officer*>>. De <<*Security Officer*>> beoordeelt de melding en lost de kwetsbaarheid op, eventueel in samenspraak met de melder. In het geval van een ernstige kwetsbaarheid of een lek van persoonsgegevens wordt de <<*Corporate Security Officer*>> betrokken bij het proces. Eventuele overtreding van de spelregels wordt juridisch beoordeeld. Tijdens het onderzoek wordt de melder met regelmaat op de hoogte gehouden van de voortgang. <<*Organisatie*>> besluit of de melder in aanmerking komt voor een (geldelijke) beloning. Daarna wordt, in samenspraak met de melder, besloten of de kwetsbaarheid publiek gemaakt wordt.

Naast de eerder genoemde argumenten voor de implementatie van een Responsible Disclosure beleid voor <<*Organisatie*>>, kan het volgende worden overwogen:

Verlagen drempel melder
Een organisatie kan de drempel tot melden van kwetsbaarheden voor haar doelgroep verlagen. Het is aannemelijk dat onderzoekers een ICT-kwetsbaarheid herkennen en deze verantwoord willen melden zonder juridische complicaties.

Transparantie
Een transparante houding van <<*Organisatie*>> is in lijn met haar maatschappelijke rol. Door publicatie van een Responsible Disclosure beleid

geeft <<*Organisatie*>> aan welk standpunt zij inneemt in deze kwestie.

Gemeenschappelijk belang

ICT heeft groeiende invloed op de maatschappij. De potentiële impact van kwetsbaarheden op gebruikers is groot. Een belangrijke drijfveer voor melders is het aan de kaak stellen van kwetsbaarheden en risico's vanwege het maatschappelijk belang. Responsible Disclosure is oplossing om op een maatschappelijk verantwoorde en effectieve wijze om te gaan met ICT-kwetsbaarheden.

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

www.cio-platform.nl