Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

» ***Leidraad*** *om te komen tot een praktijk van Responsible Disclosure* »

Inhoudsopgave

Inleiding

Informatie en communicatietechnologie (ICT) zijn doorgedrongen in de haarvaten van de maatschappij. Enerzijds zorgt ICT voor enorme gebruiksmogelijkheden. Anderzijds zorgt de wijde toepassing van ICT en de omvang hiervan ook dat de potentiële impact van kwetsbaarheden is vergroot. Daarmee is het gemeenschappelijke belang van het op effectieve wijze omgaan met ICT-kwetsbaarheden sterk gestegen.

De ICT-security-community bestaat uit een diversiteit van spelers, die op uiteenlopende wijze kennis verkrijgen over kwetsbaarheden in systemen. Een voorname drijfveer bij de white-hat hackers en beveiligingsonderzoekers is het leveren van een bijdrage aan de veiligheid van ICT-systemen door kwetsbaarheden en risico's aan de kaak te stellen. Hiermee kunnen goedwillende hackers en beveiligingsonderzoekers een belangrijke rol vervullen naar partijen die kwetsbare systemen bezitten.

Voor publieke en private partijen schuilt er een groot belang in. In de dagelijkse praktijk zijn zij in sterke mate afhankelijk van het ongestoord functioneren van informatiesystemen. Het verkrijgen van kennis over de kwetsbaarheden in de eigen systemen en de beveiliging hiervan verbeteren is daarmee noodzakelijk voor de dagelijkse bedrijfsvoering.

Momenteel bestaat er bij beveiligingsonderzoekers angst om deze kwetsbaarheid rechtstreeks bij een bedrijf te melden. Hierdoor wordt een kwetsbaarheid bijvoorbeeld indirect en via de media naar buiten gebracht. Dit is een onwenselijke situatie aangezien in dat geval de kwetsbaarheid nog steeds bestaat. Sterker nog, in sommige gevallen is er zelfs sprake van specifieke aanvalssoftware om de kwetsbaarheid uit te buiten. In veel gevallen leidt dit tot een incident waarbij zowel de goedwillende partij in een kwaad daglicht wordt gesteld en waarbij de kwetsbare organisatie niet gelijk een stap kan zetten in het verder verhogen van de beveiliging.

Dit laat zien dat het van groot belang is om deze partijen bij elkaar te brengen. Deze leidraad beoogt er toe bij te dragen dat melders die kennis hebben van kwetsbaarheden en deze verholpen willen zien en de organisaties die hiermee te maken hebben en afhankelijk zijn van deze kwetsbare systemen bij elkaar komen.

Ruim een derde van de kwetsbaarheden leidt potentieel tot volledige inbreuk op beveiligingsaspecten[1]

Succesvolle uitbuiting leidt bij ruim een derde van de bekende kwetsbaarheden tot volledige inbreuk op beveiligingsaspecten. Kwaadwillenden kunnen in dit geval:
- het systeem volledig onbeschikbaar maken (beschikbaarheid);
- elk bestand op het systeem aanpassen (integriteit);
- toegang verkrijgen tot alle bestanden op het systeem (vertrouwelijkheid).

Te verwachten is dat zelfs met een afnemend aantal bekende kwetsbaarheden deze een belangrijke bron blijven voor toekomstige incidenten. Belangrijkste reden is dat deze niet door organisaties verholpen worden of verholpen kunnen worden.

Om partijen bij elkaar te brengen is het goed om samen te werken op basis van afspraken. Met goede afspraken hebben alle partijen meer zekerheid over hun positie en kan een bijdrage worden geleverd aan het gezamenlijke doel; het verhogen van de veiligheid van informatiesystemen. Deze leidraad biedt organisaties inzicht in de wijze waarop vorm kan worden gegeven aan het vaststellen van een eigen beleid inzake responsible disclosure, om zo te bevorderen dat zij in goede samenwerking met de ICT-security-community kwetsbaarheden gemeld krijgen. Voor hackers en onderzoekers is het een van waarborgen voorziene handelwijze.

De geldende strafrechtelijke kaders worden niet aangetast, de leidraad beoogt wel een handreiking te bieden aan organisaties om door middel van een eigen beleid constructief te kunnen samenwerken met alle partijen die de veiligheid van ICT-systemen hoog in het vaandel hebben staan. Hiermee wordt actief bijgedragen aan het verminderen van de veiligheidsrisico's die kwetsbaarheden opleveren en de mogelijke negatieve maatschappelijke, economische en financiële gevolgen die uit deze kwetsbaarheden kunnen voortvloeien.

Bij de totstandkoming is gesproken met een brede en diverse groep van potentiële melders, private partijen en publieke partijen. Deze gesprekken hebben de basis gelegd voor de in deze leidraad genoemde bouwstenen. Deze bouwstenen kunnen de basis vormen voor organisaties die zelf een beleid ten aanzien van responsible disclosure willen vaststellen om een dergelijke vorm van openbaarmaking te bevorderen. Meerdere partijen hebben de afgelopen maanden reeds initiatieven genomen om een beleid voor responsible disclosure uit te dragen. Deze initiatieven zijn dan ook nadrukkelijk meegenomen in de uitwerking van deze leidraad.

In de volgende hoofdstukken wordt respectievelijk ingegaan op: kwetsbaarheden, de definitie van responsible disclosure en de bouwstenen voor responsible disclosure.

[1] Zie voor meer informatie het Cyber Security Beeld Nederland 2 (CSBN-2)

Hoofdstuk 1

Wat is een kwetsbaarheid

Kwetsbaarheden in ICT komen op diverse plaatsen in hard- en software voor en kennen vele gradaties. Gemeenschappelijke deler is dat het uitbuiten van de kwetsbaarheid kan leiden tot mogelijke veiligheidsrisico's.

De kwetsbaarheid is een eigenschap van een samenleving, organisatie of informatiesysteem of een onderdeel daarvan die afbreuk doet aan de weerbaarheid van deze entiteit. Een kwetsbaarheid biedt een kwaadwillende partij de kans om schade toe te brengen omdat de bescherming tegen schade te wensen overlaat. Zo kan een kwaadwillende partij bijvoorbeeld de legitieme toegang tot informatie of functionaliteit verhinderen en beïnvloeden dan wel ongeautoriseerd benaderen.
Kwetsbaarheden vormen de 'toegangspoorten' waarlangs dreigingen kunnen leiden tot incidenten. Het verhelpen van kwetsbaarheden is een directe manier om dreigingen af te laten nemen en de kans op incidenten te verkleinen.

Systemen kunnen door kwetsbaarheden mogelijkerwijs uitvallen (beschikbaarheid), data binnen het systeem kunnen gewijzigd worden (integriteit) en data kunnen toegankelijk worden voor personen die daar niet toe gemachtigd zijn (vertrouwelijkheid).

ICT-kwetsbaarheden kunnen, juist voor organisaties die in sterke mate afhankelijk zijn van ICT, ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid grote gevolgen hebben, zeker indien deze kwetsbaarheden bij de betrokken organisatie nog niet bekend zijn.

Hoofdstuk 2
Responsible Disclosure

In de ICT-wereld bestaan meerdere praktijken om kwetsbaarheden in ICT bekend te maken. Voorbeelden hiervan zijn de zogeheten 'full disclosure', oftewel het volledig publiekelijk bekendmaken van een kwetsbaarheid en een verantwoorde wijze van responsible disclosure. Bij het volledig publiek maken van een kwetsbaarheid is deze nog steeds aanwezig en kan een veiligheidsrisico ontstaan. De praktijk van responsible disclosure heeft dan ook nadrukkelijk de voorkeur.

Binnen de ICT-community is veel kennis en de wil om deze te delen met betrekking tot kwetsbaarheden in ICT alsmede de wijze waarop deze verholpen kunnen worden. De samenwerking met de ICT-community is daarmee van het grootste belang in het kader van het gezamenlijke streven naar cyber security.

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

Doel van responsible disclosure

Het doel van responsible disclosure is het bijdragen aan de veiligheid van ICT systemen en het beheersen van de kwetsbaarheid van ICT-systemen door kwetsbaarheden op verantwoorde wijze te melden en deze meldingen zorgvuldig af te handelen, zodat schade zo veel als mogelijk kan worden voorkomen of beperkt. Hierbij dient dan voldoende tijd voor herstel beschikbaar te zijn alvorens tot openbaarmaking wordt overgegaan.

Centraal bij het werken met responsible disclosure staat het verhelpen van de kwetsbaarheid en het verhogen van de veiligheid van informatiesystemen.

Bij responsible disclosure staat voorop dat partijen zich over en weer houden aan afspraken over het melden van de kwetsbaarheid en de omgang hiermee. Een partij die een responsible disclosure policy vaststelt kan zich bijvoorbeeld binden aan het principe om geen aangifte te doen als aan de volgens het beleid geldende spelregels wordt voldaan.

Bij de praktijk van responsible disclosure zijn primair de melder en de organisatie, die eigenaar/beheerder van het systeem is, betrokken. Het is van belang om zo min mogelijk schakels te hebben tussen de persoon die de kwetsbaarheid meldt en de organisatie die verantwoordelijk is voor het oplossen van het probleem. De melder en de organisatie kunnen echter gezamenlijk besluiten om het Nationaal Cyber Security Centrum (NCSC) of andere partijen binnen de ICT-security-community in te lichten over de kwetsbaarheid, zeker bij een nog niet bekende kwetsbaarheid, om ook elders (vervolg)schade te voorkomen of te beperken.

In hoofdstuk 3 wordt nader ingegaan op de respectievelijke verantwoordelijkheden van partijen. In hoofdstuk 4 wordt ingegaan op de bouwstenen voor responsible disclosure.

Hoofdstuk 3
Verantwoordelijkheden

Met het voeren van een beleid voor responsible disclosure wordt beoogd dat in gezamenlijkheid door melder en organisatie een bijdrage wordt geleverd aan het verminderen van kwetsbaarheden in informatiesystemen. Het werken met responsible disclosure laat echter de bestaande verantwoordelijkheden en verplichtingen onverlet. De verschillende actoren die betrokken zijn bij responsible disclosure hebben allemaal een eigen rol. Hieronder staan beknopt de respectievelijke verantwoordelijkheden.

De organisatie die eigenaar/beheerder is van een informatiesysteem
De organisatie, die eigenaar/beheerder of leverancier is van een informatiesysteem, is primair verantwoordelijk voor de beveiliging van dit systeem. Daarmee is de organisatie ook verantwoordelijk voor de wijze waarop een vervolg wordt gegeven aan de melding van een kwetsbaarheid. De organisatie kan ervoor kiezen om aan de hand van deze leidraad een openlijk uit te dragen beleid voor responsible disclosure vast te stellen.

De melder van een kwetsbaarheid

De spil in het kunnen voeren van een praktijk van responsible disclosure is de melder. De melder heeft op enigerlei wijze een kwetsbaarheid weten te constateren en wil bijdragen aan de veiligheid van informatiesystemen door deze kwetsbaarheid openbaar te maken en de kwetsbaarheid bij een organisatie te laten verhelpen. De melder van een kwetsbaarheid is verantwoordelijk voor het eigen handelen en de wijze waarop hij/zij de kwetsbaarheid ontdekt heeft. Het melden van de kwetsbaarheid vrijwaart de melder, indien hij bij het aantonen van de kwetsbaarheid een strafbaar feit heeft gepleegd, niet van de mogelijkheid van een strafrechtelijk onderzoek en vervolging. Organisatie en melder kunnen in het kader van responsible disclosure wel overeenkomen dat ten aanzien van eventueel strafrechtelijk handelen geen aangifte zal worden gedaan. Eveneens kan worden afgesproken dat er geen civielrechtelijke stappen worden ondernomen.

Het NCSC

Responsible disclosure is primair een aangelegenheid die organisatie en melder aangaat en waartoe een organisatie een beleid kan vaststellen. Dit neemt echter niet weg dat het NCSC een rol heeft in het stimuleren van het voeren van een beleid van responsible disclosure. Tevens heeft het NCSC een rol in het uitdragen van kennis over kwetsbaarheden in ICT aan de overheid en de vitale sectoren. Het NCSC kan door organisaties worden betrokken bij het zo nodig over geconstateerde kwetsbaarheden informeren van andere organisaties. Het NCSC zal, indien een melding direct bij het NCSC wordt gedaan, trachten de melder in contact te brengen met de betrokken organisatie.

Hoofdstuk 4

Bouwstenen voor Responsible Disclosure

Hieronder zijn de bouwstenen voor responsible disclosure weergegeven. Deze bouwstenen zien toe op de organisatie, de melder en het NCSC.

4.1 De organisatie

Het uitdragen van responsible disclosure begint bij een organisatie die eigenaar is van informatiesystemen of leverancier van een product. De eigenaar/leverancier is immers primair verantwoordelijk voor de informatiebeveiliging van deze systemen of producten. Belangrijk hierin is dat de organisatie de keuze heeft om een beleid voor responsible disclosure vast te stellen en te voeren. Op deze wijze kan op effectieve wijze gewerkt worden aan het oplossen van kwetsbaarheden.

Door het opstellen van een eigen beleid voor responsible disclosure maakt de organisatie duidelijk op welke wijze zij wil omgaan met meldingen van kwetsbaarheden. Dit wordt reeds door diverse partijen gedaan en kan als volgt werken:
De organisatie stelt een beleid voor responsible disclosure vast en maakt het beleid voor responsible disclosure publiekelijk kenbaar.

De organisatie maakt het laagdrempelig voor een melder om een melding te doen. Dit kan door een gestandaardiseerde wijze, bijvoorbeeld een 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 capaciteit om adequaat op meldingen te kunnen reageren.

- De organisatie neemt de melding over een 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. Hierna treden de organisatie en de melder in contact over het verdere proces.

- De organisatie bepaalt in overleg met de melder de termijn waarop eventuele bekendmaking zal plaatsvinden. Een redelijke standaardtermijn die kan worden gehanteerd voor kwetsbaarheden in software is 60 dagen. Het verhelpen van kwetsbaarheden in hardware is lastiger te realiseren, hierbij kan een redelijke standaardtermijn 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 systemen afhankelijk zijn van het systeem ten aanzien waarvan de kwetsbaarheid gemeld wordt.

- Als een kwetsbaarheid niet of moeilijk op te lossen is, of indien er hoge kosten mee gemoeid zijn, kunnen melder en organisatie afspreken om de kwetsbaarheid niet openbaar te maken.

- De organisatie houdt de melder en overige betrokkenen op de hoogte van de voortgang van het proces.

- De organisatie kan uitdragen dat de organisatie de melder credits zal geven, als de melder dat wenst, voor het doen van de melding.

- De organisatie kan ervoor kiezen om een melder een beloning/waardering te geven voor het melden van kwetsbaarheden in ICT-producten of -diensten, indien de melder zich aan de in het beleid opgenomen spelregels heeft gehouden. De hoogte van de beloning kan afhankelijk zijn van de kwaliteit van de melding.

- De organisatie kan in overleg met de melder afspreken om de bredere ICT-community te informeren over de kwetsbaarheid indien het aannemelijk is dat de kwetsbaarheid ook op andere plaatsen aanwezig is.

- De organisatie spreekt zich in het vastgestelde beleid uit over het niet ondernemen van juridische vervolgstappen indien conform het beleid wordt gehandeld.

4.2 De melder

De spil in het kunnen voeren van een praktijk van responsible disclosure is de melder. De melder heeft op enigerlei wijze een kwetsbaarheid weten te constateren en wil bijdragen aan de veiligheid van informatiesystemen door deze kwetsbaarheid openbaar te maken en de kwetsbaarheid bij een organisatie te laten verhelpen. Melders erkennen hiermee dat zij een belangrijke maatschappelijke verantwoordelijkheid hebben en nemen die door kwetsbaarheden op verantwoorde wijze te openbaren. Om tot een succesvolle praktijk van responsible disclosure te komen, gelden voor de melder de volgende bouwstenen:

- De melder is verantwoordelijk voor het eigen handelen en zorgt ervoor dat de melding primair bij de (systeem/informatie)eigenaar wordt gedaan.

- 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 zal niet op onevenredige wijze handelen:
  - door gebruik te maken van social engineering om zich op die wijze toegang te verschaffen tot het systeem.
  - door een eigen backdoor in een informatiesysteem plaatsen om vervolgens daarmee de kwetsbaarheid aan te tonen, aangezien daarmee aanvullende schade kan worden aangericht en onnodige veiligheidsrisico's worden gelopen.
  - door een kwetsbaarheid verder uit te nutten dan noodzakelijk is om de kwetsbaarheid vast te stellen.
  - door gegevens van het system te kopiëren, te wijzigen of te verwijderen. Een alternatief hiervoor is het maken van een directory listing van een systeem.
  - door veranderingen in het systeem aan te brengen.
  - door herhaaldelijk toegang tot het systeem te verkrijgen of de toegang te delen met anderen.
  - door gebruik te maken van het zogeheten "bruteforcen" van toegang tot systemen, daarbij is immers geen sprake van een kwetsbaarheid, maar alleen van het herhaaldelijk proberen van wachtwoorden.

- Als melder en organisatie overeen komen dat de kwetsbaarheid openbaar wordt gemaakt dan maakt een melder het pas openbaar als alle betrokken organisaties goed zijn geïnformeerd en zij aangegeven hebben dat de kwetsbaarheid is opgelost, conform de gemaakte afspraken.

- Tot slot kunnen de melder en de betrokken organisatie afspraken maken over het informeren van de bredere ICT-community. Dit kan bijvoorbeeld het geval zijn bij een (nog niet bekende) kwetsbaarheid waarvan bekend is dat die op meer plaatsen aanwezig kan zijn. Het NCSC kan hierbij betrokken worden om de doelgroepen Rijksoverheid en vitaal te bedienen.

4.3 Het NCSC

Primair is responsible disclosure een aangelegenheid die organisaties en melder aangaat. Het NCSC zal echter het gebruikmaken van een beleid van responsible disclosure stimuleren. Tevens kan het NCSC in samenspraak tussen melder en organisatie betrokken worden om informatie over de kwetsbaarheid met de doelgroep te delen om daarmee verdere veiligheidsrisico's, die voortvloeien uit de kwetsbaarheid, te beperken. Indien een (potentiële) melder direct in contact treedt met het NCSC, zal het NCSC trachten de melder met de organisatie in contact te brengen.

Het NCSC zal, indien mogelijk, de verkregen informatie over technische kwetsbaarheden in samenspraak tussen organisaties en melders gebruiken om de kennis verder te delen met de ICT-community. 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.

- 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.

- Het NCSC zal, als zij geïnformeerd wordt over een kwetsbaarheid, andere partijen binnen de doelgroep van Rijksoverheid en vitale sectoren informeren.

Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Nationaal Cyber Security Centrum

Wilhelmina van Pruisenweg 104 | 2595 AN | Den Haag
Postbus 117 | 2501 CC| Den Haag

T 070 888 75 55
F 070 888 75 50

info@ncsc.nl
www.ncsc.nl