Bachelorscriptie
Informatica / Informatiekunde

Radboud Universiteit

Responsible Disclosure: een kritische beschouwing

Auteur:
Nicky van Rijsbergen
S4062833
n.vanrijsbergen@student.ru.nl

Inhoudelijk begeleider:
prof. dr. B.P.F. (Bart) Jacobs

Inhoudsopgave

Inleiding

Op 3 Januari 2013 heeft minister van Veiligheid en Justitie, Ivo Opstelten, een brief naar de tweede kamer gestuurd. In deze brief presenteert de minister een leidraad voor de totstandkoming van een praktijk van wat hij noemt 'Responsible Disclosure'[1]. In het vervolg van dit document zullen we spreken over de leidraad, als we het hebben over de leidraad voor Responsible Disclosure die is opgesteld door de minister. De leidraad heeft als doel om kwetsbaarheden op een verantwoorde wijze bekend te maken en op te lossen. Dit doel wil de leidraad bereiken door de samenwerking tussen ethische hackers en kwetsbare systeemeigenaren te stimuleren en te bevorderen. Voorheen was het probleem vaak dat deze samenwerking niet goed verliep, als überhaupt al gesproken kon worden van samenwerken.

De eerste versie van de leidraad is al in gebruik, maar er is behoorlijk wat kritiek op deze versie[2][3][4][5]. Deze scriptie zal één van de eerste analyses van de leidraad voor Responsible Disclosure zijn. Deze analyse zal gedaan worden aan de hand van de volgende onderzoeksvraag:

Bereikt de leidraad voor Responsible Disclosure in de huidige staat haar doel, namelijk het op een verantwoorde manier bekendmaken en oplossen van kwetsbaarheden?

De opbouw van deze scriptie is als volgt: de terminologie, een aantal inleidende hoofdstukken, een informele analyse van Resonsible Disclosure en een hoofdstuk waarin wordt uitgelegd hoe het met het recht en Responsible Disclosure zit. Hierna volgt een hoofdstuk waarin de hoofdproblemen van de leidraad worden uitgelegd. Gevolgd door het hoofdonderdeel van deze scriptie, namelijk een precieze analyse van de leidraad. Tot slot een conclusie waarin een mogelijk antwoord op de onderzoeksvraag gegeven wordt.

Terminologie

Systeemeigenaar zal in dit document gebruikt worden om één of meer mensen aan te geven die gebruik maken van een ICT-systeem. Voorbeelden van systeemeigenaren zijn een bedrijf, een organisatie of een overheidsinstelling. De minister gebruikt vaak het woord organisatie om een systeemeigenaar aan te geven.

Kwetsbaarheid ook wel ICT-kwetsbaarheid. Dit is een zwakke plek in een ICT-systeem. Via een zwakke plek kan een aanvaller in het systeem binnendringen en schade aan het ICT-systeem aanbrengen.

Kwetsbare systeemeigenaar is een systeemeigenaar met één of meer kwetsbaarheden in het door de systeemeigenaar gebruikte ICT-systeem.

Ethische hacker ook wel white-hat hacker, goedwillende hacker of beveiligingsonderzoeker. Dit zijn hackers die bewust of onbewust een kwetsbaarheid in een systeem vinden en deze graag verholpen willen zien in plaats van uitgebuit. Zij willen de ICT-wereld verbeteren.

Melder is een persoon die een eventuele kwetsbaarheid meldt. De melder kan dit doen bij de kwetsbare systeemeigenaar zelf, maar ook elders, bijvoorbeeld bij de media.

Ontdekker ook wel vinder. Dit is de persoon die een kwetsbaarheid ontdekt.

Vondst ook wel ontdekking. In dit document betekent een vondst een gevonden kwetsbaarheid in een ICT-systeem.

Full Disclosure is het bekendmaken van alle details van een gevonden kwetsbaarheid. Mogelijk zelfs inclusief software om de kwetsbaarheid uit te buiten. Dit wordt gedaan ongeacht of de kwetsbare systeemeigenaar de kwetsbaarheid heeft verholpen.

Responsible Disclosure is het op een verantwoorde wijze bekendmaken van een kwetsbaarheid. Responsible Disclosure is een strategie gericht op het oplossen/verhelpen van een kwetsbaarheid en gericht op het minimaliseren van het risico op uitbuiting van de kwetsbaarheid.

Responsible Repair is onderdeel van Responsible Disclosure. Het beschrijft het proces dat de kwetsbare systeemeigenaar uitvoert wanneer een melding van een kwetsbaarheid wordt gedaan.

1. Informele analyse

De opsomming hieronder beschrijft de essentiële elementen van Responsible Disclosure, zoals beschreven in de leidraad.

- Een systeemeigenaar maakt publiekelijk zijn beleid voor responsible discosure bekend. Een mogelijkheid om dit te doen is bijvoorbeeld via de website van de systeemeigenaar. In dit beleid dient de systeemeigenaar uitspraak te doen over het niet ondernemen van juridische vervolgstappen als de ethische hacker conform het beleid heeft gehandeld. Ook stelt de systeemeigenaar voldoende capaciteit beschikbaar om eventuele kwetsbaarheden te kunnen verhelpen.
- Een ethische hacker ontdekt een kwetsbaarheid en meldt deze direct bij de betreffende kwetsbare systeemeigenaar. Wanneer een ethische hacker een melding doet van een kwetsbaarheid dan vrijwaart hem dit niet van de mogelijkheid van strafrechtelijk onderzoek en vervolging. Hierbij moet ook opgemerkt worden dat de strafrechtelijke kaders niet aangepast worden.
- De kwetsbare systeemeigenaar neemt de melding in ontvangst en zorgt ervoor dat deze melding zo snel mogelijk terecht komt bij de afdeling die de kwetsbaarheid het beste kan beoordelen en het beste in behandeling kan nemen. Ook bevestigt de systeemeigenaar dat hij de melding heeft ontvangen.
- De kwetsbare systeemeigenaar en de melder maken afspraken over de termijn waarop de kwetsbaarheid verholpen zal zijn, over het verder inlichten van de ICT-community en over een eventuele beloning. Ook worden afspraken gemaakt over de bekendmaking en of de ethische hacker erkenning krijgt voor de vondst.
- De kwetsbare systeemeigenaar zorgt ervoor dat de kwetsbaarheid binnen de afgesproken termijn wordt opgelost en houdt de melder op de hoogte.
- De melder en de inmiddels niet meer kwetsbare systeemeigenaar, sluiten de samenwerking af. Als duidelijk is dat de ethische hacker volgens het beleid heeft gehandeld dan doet de systeemeigenaar geen aangifte en spant de systeemeigenaar, de ethische hacker geen civiel proces aan. Ook kan de systeemeigenaar credits en/of een beloning geven aan de ethische hacker als dit eerder is afgesproken.

Uit deze opsomming wordt duidelijk dat de ethische hacker aan Responsible Disclosure doet, want hij maakt een kwetsbaarheid op een verantwoorde manier bekend. Ook wordt duidelijk dat de systeemeigenaar aan Responsible Repair doet en niet zozeer aan Responsible Disclosure. De systeemeigenaar moet er immers voor zorgen dat een kwetsbaarheid op een verantwoorde manier wordt gerepareerd. Dit houdt bijvoorbeeld in dat de systeemeigenaar voldoende capaciteit reserveert en de kwetsbaarheid binnen de opgegeven termijn oplost.

Verder vallen een paar zaken op. Ten eerste is de leidraad onvolledig. Zo wordt bijvoorbeeld zelden beschreven hoe er gehandeld moet worden wanneer één van de partijen niet conform het beleid handelt. Ten tweede heeft de leidraad het steeds over melders, terwijl het over ethische hackers gaat. Een ethische hacker is wel altijd de ontdekker van een kwetsbaarheid, maar is niet altijd ook de melder. Voorheen maakten ethische hackers bijvoorbeeld gebruik van een journalist om hun vondst bekend te maken. Ten derde lijkt er een asymmetrie te zijn tussen de ethische hackers en de systeemeigenaren. Het lijkt alsof de laatste partij meer te zeggen heeft. Een voorbeeld van deze asymmetrie is dat de systeemeigenaren voor het grootste deel beslissen hoe een beleid voor Responsible Disclosure eruit komt te zien en hiermee voor een groot deel ook beslissen hoe de samenwerking gaat verlopen. Tot slot is er een probleem dat te maken heeft met het strafrecht. Het is voor de ethische hacker namelijk onduidelijk wanneer hij vervolgd wordt en wanneer niet. Daarbij komt dat er een grote kans is dat hij als verdachte wordt aangemerkt als hij een directe melding doet.

2. Het recht en Responsible Disclosure

In dit hoofdstuk wordt de relatie tussen de leidraad voor Responsible Disclosure en het recht uitgelegd. We zullen het hebben over het strafrecht en het civiel recht. De invloed van de leidraad voor Responsible Disclosure op deze twee rechtsgebieden zal hieronder kort beschreven worden.

Strafrecht

Als we kijken naar strafrecht en in het bijzonder naar computervredebreuk dan zijn de volgende handelingen strafbaar volgens artikel 138ab van het Wetboek van Strafrecht:

Straf: 1 Jaar cel of een geldboete van de vierde categorie

- Enige beveiliging in een ICT-systeem doorbreken.
- De toegang tot een ICT-systeem verwerven door een technische ingreep, met behulp van valse signalen of een valse sleutel dan wel door het aannemen van een valse hoedanigheid.

Straf: 4 Jaar cel of een geldboete van de vierde categorie

- Gegevens uit de computer vastleggen (voor zichzelf of anderen).
- De verwerkingscapaciteit van de computer aanwenden voor zichzelf.
- De ingebroken computer gebruiken als startpunt voor een verdere inbraakpoging in een andere computer.

In de leidraad geeft de minister duidelijk aan dat alle bovenstaande handelingen strafbaar blijven, dit betekent dus dat de wet geen rekening gaat houden met eventuele ethische motieven. Dit betekent echter niet dat er geen rekening wordt gehouden met deze motieven bij de beoordeling van een ethische hacker. Dit heeft als resultaat dat het onduidelijk is wanneer een ethische hacker vervolgd wordt en wanneer niet. Om dit duidelijker te krijgen, heeft het college van procureurs generaal een kader voorgesteld[6]. Dit kader bestaat uit een drietal vragen en als het antwoord op deze vragen positief is, dan kan afgezien worden van verder strafrechtelijk onderzoek, dan wel geen vervolging instellen. Het kader ziet er als volgt uit:

- Was het handelen van de verdachte noodzakelijk binnen een democratische samenleving?
- Heeft de verdachte bij zijn handelen proportioneel gehandeld? Stond het gekozen middel in verhouding met het te bereiken doel?
- Heeft de verdachte subsidiair gehandeld (waren er andere mogelijkheden om te handelen)?

Het college van procureurs generaal stelt voor om (ethische) hackers eerst als verdachte aan te merken en een strafrechtelijk onderzoek in te stellen, zodat antwoord op de vragen uit het kader kan worden verkregen.

Context bij strafrecht, wat houdt strafrechtelijk onderzoek in?

Tijdens een strafrechtelijk onderzoek naar een verdachte mag het Openbaar Ministerie gebruik maken van een aantal handelingen om te achterhalen of de ethische hacker strafbaar bezig is geweest. Deze handelingen staan beschreven in artikel 125i t/m 125o en artikel 126g t/m 126ni van het Wetboek van Strafvordering. Voorbeelden van deze handelingen zijn het afluisteren van de verdachte of het doen van een huiszoeking bij de verdachte. Daarbij komt dat het Openbaar Ministerie de verdachte mag hacken, als het wetsvoorstel dat de Minister van Justitie recent heeft gedaan, wordt aangenomen. In dit wetsvoorstel stelt de minister voor om de politie de macht te geven om verdachten te hacken, zodat zij bewijs kunnen vinden voor eventuele strafbare feiten.

Civiel recht

Het civiel recht bestaat uit een materieel en een formeel gedeelte. Het materiële gedeelte stelt regels ten aanzien van de verhoudingen tussen burgers onderling, en tussen burgers en goederen. Het formeel civiel recht is het burgerlijk procesrecht: het geeft regels over de handhaving van de materiële regels. Kenmerkend aan het civiel recht is dat een betrokkene zelf het recht moet activeren.

De invloed van Responsible Disclosure op het civiel recht is per geval afhankelijk. Dit komt omdat de invloed op het civiel recht voornamelijk zal komen van het beleid dat een systeemeigenaar opstelt. Dit beleid beschrijft hoe een systeemeigenaar een praktijk van Responsible Disclosure wil invullen. Wanneer een systeemeigenaar of een ethische hacker bewijzen meent te hebben dat de andere partij niet heeft gehandeld conform het beleid, dan kan deze partij, de andere partij een civiel proces aanspannen. Aangezien elke systeemeigenaar zijn eigen beleid mag opstellen, kunnen er veel verschillende soorten processen ontstaan. Hieruit blijkt dat de invloed van Responsible Disclosure op het civiel recht niet eenduidig is.

Beide rechten

Uiteindelijk heeft de leidraad waarschijnlijk de meeste invloed via jurisprudentie. Deze invloed zal dan vooral komen van de bouwstenen die de minister in de leidraad heeft gepresenteerd. Deze bouwstenen beschrijven hoe een goed beleid voor Responsible Disclosure eruit kan zien, volgens de minister. Een rechter zou deze bouwstenen mee kunnen nemen in zijn uiteindelijke beslissing.

3. Hoofdproblemen

In dit hoofdstuk worden de hoofdproblemen van de leidraad voor Responsible Disclosure behandeld. Deze hoofdproblemen zullen in het hoofdstuk analyse verder onderbouwd worden.

Hoofdprobleem 1, Onvolledigheid

De leidraad voor Responsible Disclosure beschrijft in de meeste gevallen alleen wat er gebeurt wanneer beide partijen handelen conform het beleid. Hoe beide partijen moeten handelen wanneer de ethische hacker of de kwetsbare systeemeigenaar niet handelt conform het beleid, wordt in veel gevallen niet of onvoldoende behandeld. Hierdoor is de leidraad minder robuust dan hij zou kunnen zijn wanneer deze gevallen wel beschreven zouden worden. Het betreft de volgende gevallen.

- Wanneer een kwetsbare systeemeigenaar de kwetsbaarheid niet binnen de afgesproken termijn wil of kan verhelpen.
- Wanneer het verhelpen van een kwetsbaarheid inspanningen van derden vereist, die niet of traag reageren.
- Wanneer een kwetsbare systeemeigenaar te weinig capaciteit beschikbaar heeft gesteld om de kwetsbaarheid op te lossen. Überhaupt wordt niet beschreven wat voldoende capaciteit inhoudt.
- Wanneer een kwetsbare systeemeigenaar weigert een kwetsbaarheid te verhelpen, ook al heeft de systeemeigenaar een beleid voor Responsible Disclosure opgesteld. De risico's van deze actie worden onvoldoende benadrukt. Voorbeelden van deze risico's zijn: een grotere kans op Full Disclosure, een grotere kans dat een hacker de kwetsbaarheid vindt, voordat deze is opgelost en het risico dat de systeemeigenaar niet meer kan ontkennen dat hij van de kwetsbaarheid af weet.
- Wanneer een ethische hacker niet conform het beleid handelt. De leidraad beschouwt het handelen conform het beleid als één geheel, terwijl er minstens negen regels in staan waaraan een ethische hacker zich moet houden, zie p. 23-25. Voor het overschrijden van één van de regels, met welke motivatie dan ook, staat één straf: de systeemeigenaar heeft weer de mogelijkheid om de ethische hacker een civiel proces aan te spannen of om hem aan te geven. Niet elke overtreding van het beleid is echter even erg en soms is het maken van een overtreding noodzakelijk om een kwetsbaarheid te vinden of om een kwetsbaarheid aan te tonen.
- Wanneer een ethische hacker een melding maakt, dan vrijwaart dit hem niet van een strafrechtelijk onderzoek en eventuele vervolging. Wat er echter precies gebeurt wanneer het Openbaar Ministerie besluit een onderzoek te starten, is onduidelijk. Blijven de afspraken tussen de ethische hacker en kwetsbare systeemeigenaar bestaan? Gaat het proces van Responsible Disclosure nog door of wordt dit gestaakt? En welke verdenkingen zijn eigenlijk de trigger voor een strafrechtelijk onderzoek?

Hoofdprobleem 2, Melders en ethische hackers

De leidraad spreekt enkel over melders, terwijl de melder van een kwetsbaarheid niet altijd ook de ontdekker hoeft te zijn. Volgens de leidraad is het slecht en dus ongewenst wanneer een kwetsbaarheid niet direct door de ontdekker van de kwetsbaarheid wordt gemeld. In werkelijkheid hoeft dit niet altijd slecht te zijn, zolang zowel de ontdekker als de melder handelt conform het beleid.

Voordat de leidraad voor Responsible Disclosure bestond, gebruikten veel ethische hackers een journalist om de kwetsbaarheid te melden. De journalist lichtte de kwetsbare systeemeigenaar in over de kwetsbaarheid. Hierna wachtte de journalist tot de kwetsbaarheid was opgelost, voordat hij tot volledige bekendmaking van de kwetsbaarheid overging. Een voorbeeld van een dergelijke journalist is Brenno de Winter[3]. Het voordeel van deze manier van werken voor de ethische hacker is dat de journalist een bronbescherming heeft, waardoor een ethische hacker minder bang hoeft te zijn voor zowel strafrechtelijke als civielrechtelijke processen, terwijl de door hem gevonden kwetsbaarheid toch op een verantwoorde manier wordt gemeld en opgelost. Het nadeel voor de kwetsbare systeemeigenaren is dat het lastiger is om te achterhalen wie de hacker is en dus ook lastiger om hem een proces aan te spannen of om hem aan te geven. Het vinden en aanklagen van hackers is echter niet het doel van de leidraad.

Er zullen nog steeds ethische hackers zijn die de indirecte manier van melden zullen prefereren en zoals in het voorbeeld met Brenno de Winter bleek, hoeft dit niet altijd slecht te zijn. Sterker nog, het doel dat de leidraad voor Responsible Disclosure wil bereiken, namelijk het op een verantwoorde manier melden en oplossen van een kwetsbaarheid, kan ook door een indirecte melding worden bereikt. Het grootste verschil is dat de melder en de ontdekker van de kwetsbaarheid, niet meer dezelfde persoon zijn.

Hoofdprobleem 3, Systeemeigenaren vs ethische hackers

In de leidraad lijkt er een asymmetrie tussen systeemeigenaren en ethische hackers te zijn[4]. De leidraad kijkt meer naar de belangen van de systeemeigenaren, dan naar de belangen van de ethische hackers. Dat er sprake is van asymmetrie is te zien aan de volgende twee zaken.

Ten eerste mogen de systeemeigenaren kiezen of zij een beleid voor Responsible Disclosure opstellen. Alhoewel de leidraad nadrukkelijk de voorkeur heeft voor Responsible Disclosure, kan er alleen aan een praktijk van Responsible Disclosure gedaan worden, wanneer een systeemeigenaar dat wil. Stel een ethische hacker vindt een kwetsbaarheid, dan zou hij deze vervolgens niet op een verantwoorde manier kunnen melden als de betreffende kwetsbare systeemeigenaar geen beleid heeft opgesteld voor Responsible Disclosure. Dit dwingt een ethische hacker om een andere manier van bekendmaken te zoeken of om de kwetsbaarheid helemaal niet bekend te maken.

Ten tweede vult de systeemeigenaar in hoe de samenwerking tussen hem en de ethische hacker zal gaan verlopen. De systeemeigenaar stelt een beleid op en als de ethische hacker zich niet aan het beleid houdt, dan loopt hij het risico dat de systeemeigenaar een civiel proces aanspant tegen hem of dat de systeemeigenaar aangifte doet. Houdt de systeemeigenaar zich echter zelf niet aan het beleid, dan is er volgens de leidraad geen negatief gevolg. Dit zou ethische hackers af kunnen schrikken omdat zij maar moeten handelen zoals de systeemeigenaar wil en zelf weinig te zeggen hebben over hoe de samenwerking zal verlopen.

Hoofdprobleem 4, Strafrechtelijke vervolging of niet?

De minister zegt in de leidraad dat de huidige strafrechtelijke kaders niet veranderd worden. Dit houdt dus in dat de wet geen rekening gaat houden met eventuele ethische motieven, omdat dit niet in de huidige strafrechtelijke kaders zit. Dit betekent echter niet dat de motieven van een hacker niet meegenomen worden in zijn beoordeling. Hierdoor ontstaat er een probleem, namelijk dat het onduidelijk is wanneer een ethische hacker vervolgd wordt.

Om dit duidelijker te maken heeft het college van procureurs generaal een kader voorgesteld met daarin drie vragen. Dit kader moet duidelijker maken of een ethische hacker vervolgd moet worden of niet en kan toegepast worden als er redenen zijn om te geloven dat de ethische hacker strafbaar gehandeld heeft. Om antwoord op de vragen in het kader te krijgen moet een ethische hacker strafrechtelijk onderzocht worden. Het probleem is nu echter nog niet helemaal opgelost, het kader brengt namelijk alleen duidelijkheid voor de officier van justitie en niet voor een ethische hacker. Dit betekent dus dat een ethische hacker nog steeds niet weet welke handelingen, wanneer vervolgd worden.

Het is mogelijk dat dit probleem ethische hackers afschrikt en dat is om twee redenen. De eerste reden is dat ethische hackers niet weten wanneer zij vervolgd worden. Een ethische hacker zou een andere manier van bekendmaken kunnen prefereren, als daarbij duidelijker is of hij vervolgd wordt of niet.

De tweede reden is dat het ondernemen van strafrechtelijke processen, ethische hackers af zou kunnen schrikken. Angst om als verdachte gemerkt en vervolgd te worden, waren eerder ook al een reden voor ethische hackers om een melding indirect of helemaal niet te doen. In de luchtvaart heeft een dergelijk probleem zich ook voorgedaan. Jaap-Henk Hoepman beschrijft in zijn blog[5] dat het ondernemen van strafrechtelijke processen tegen piloten heeft gezorgd voor een minder aantal meldingen.

4. Analyse van de leidraad

In dit hoofdstuk wordt de leidraad voor Responsible Disclosure van de minister verder geanalyseerd. Dit wordt gedaan door alle vier de hoofdstukken uit de leidraad alinea per alinea te behandelen. Dit zal als volgt gaan: eerst wordt de alinea uit de leidraad geciteerd in schuingedrukte tekst, hierna volgt een analyse waarin het stuk wordt toegelicht. Deze analyse zal soms vragen oproepen en deze vragen zullen worden genoemd en wanneer mogelijk, ook beantwoord. Tot slot kan het soms nodig zijn om een alinea in context te plaatsen om een vollediger beeld te krijgen van de situatie.

Inleiding van de leidraad

Alinea 1 & 2

Een voorname drijfveer voor 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. Het verkrijgen van kennis over de kwetsbaarheden in de eigen systemen en de beveiliging hiervan verbeteren, is daarmee noodzakelijk voor de dagelijkse bedrijfsvoering.

Analyse

De minister geeft hier aan dat ethische hackers volgens hem een belangrijke rol kunnen vervullen voor kwetsbare systeemeigenaren. Dit inzicht is een belangrijke stimulans geweest om de leidraad voor Responsible Disclosure te maken.

Alinea 3

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.

Context bij alinea 3, waar hebben ethische hackers angst voor?

Wanneer een ethische hacker op zoek is naar een kwetsbaarheid dan is hij mogelijk strafbaar bezig. We zagen bij hoofdstuk 2 al welke handelingen strafbaar zijn met betrekking tot computervredebreuk. Om een kwetsbaarheid te vinden heeft de ethische hacker waarschijnlijk een van die strafbare handelingen moeten uitvoeren. Wanneer hij dan de melding direct bij de betreffende kwetsbare systeemeigenaar doet, loopt hij niet alleen het risico dat die systeemeigenaar hem aangeeft of een civiel proces aanspant, maar ook het risico dat het Openbaar Ministerie hem als verdachte merkt of zelfs vervolgt. Dit zijn redenen voor een ethische hacker om angst te hebben wanneer hij een directe melding doet. Deze angst was eerder al een reden voor ethische hackers om de melding indirect, bijvoorbeeld via een journalist, te doen[3].

Analyse

De minister beschrijft in alinea 3 dat een indirecte melding (dan zijn de melder en de ontdekker dus niet dezelfde persoon) volgens hem altijd een ongewenste situatie is. Hij zegt dat een indirecte melding de kwetsbare systeemeigenaar blootstelt aan gevaar. Zoals we al eerder zagen bij hoofdprobleem twee, hoeft dit niet altijd het geval te zijn. Door de volgende vraag te stellen zullen we het standpunt van de minister analyseren.

Vraag 1.3.1 Is een indirecte melding altijd een onwenselijke situatie ten opzichte van het doel dat de leidraad voor Responsible Disclosure wil bereiken? Deze vraag sluit aan bij hoofdprobleem 2.

Antwoord 1.3.1 Het doel van de leidraad is om kwetsbaarheden op een verantwoorde wijze bekend te maken en op te lossen. Zoals we al bij hoofdprobleem twee zagen kan een indirecte melding dit doel volledig tegemoet komen, wanneer zowel de melder als de ontdekker zich aan het beleid houdt. Dus wanneer bijvoorbeeld een journalist de rol van de melder op zich neemt en hij handelt conform het beleid, dan kan de kwetsbaarheid op een verantwoorde manier worden opgelost. In grote lijnen houdt dit dus in dat de journalist eerst de kwetsbaarheid bekend maakt bij de systeemeigenaar en pas overgaat tot publiekelijk bekendmaking wanneer de systeemeigenaar de kwetsbaarheid heeft verholpen.

Alinea 4

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.

Analyse

Om beide partijen bij elkaar te brengen, zodat zij een praktijk van Responsible Disclosure kunnen uitvoeren, moeten wel beide partijen aan Responsible Disclosure willen doen. Beide partijen hebben echter redenen om niet aan Responsible Disclosure te doen. Om een vollediger beeld te krijgen van hoe beide partijen tegenover Responsible Disclosure staan, zullen deze redenen hieronder besproken worden.

Vraag 1.4.1 Welke redenen zou een systeemeigenaar kunnen hebben om geen beleid voor Responsible Disclosure op te stellen?

Antwoord 1.4.1

- De eerste reden is dat een systeemeigenaar iets te verbergen heeft. Wellicht is hij op de hoogte van een kwetsbaarheid, maar wil hij niet dat iemand anders die ook vindt en kiest er daarom voor om niemand in het systeem te laten kijken. Oftewel security by obscurity. Het verwijderen van een kwetsbaarheid kan duur zijn en veel tijd in beslag nemen. Om deze reden kan het verstoppen van de kwetsbaarheid geprefereerd worden. Een ander voordeel van deze aanpak is dat een kwetsbare systeemeigenaar kan ontkennen dat hij van de kwetsbaarheid af weet. Dit kan bijvoorbeeld handig zijn in een rechtszaak over het lekken van privacy gevoelige klantgegevens door een kwetsbaarheid in het systeem.
- De tweede reden is dat een systeemeigenaar niet zeker kan zijn van de goede bedoelingen van een ethische hacker. Een hacker kan zich voordoen als een ethische hacker, door bijvoorbeeld de melding van de kwetsbaarheid wel te doen, maar tegelijkertijd ook een backdoor te installeren. Het kost veel geld om steeds het volledige systeem te controleren, wanneer een ethische hacker een melding doet. Het is dan makkelijker en goedkoper om gewoon alle type hackers te weren.
- De derde reden is dat een systeemeigenaar ethische hackers uitnodigt om zijn systeem aan te vallen. Het nadeel hiervan voor de systeemeigenaar is dat er behoorlijk veel druk op het systeem kan komen te staan als verschillende ethische hackers tegelijk het systeem controleren op kwetsbaarheden. Stel dat een groep ethische hackers besluit om het inlogsysteem van een partij te onderzoeken. Zij voeren dan meerdere aanvallen uit waardoor het inlogsysteem traag kan worden of zelfs crashen.

Vraag 1.4.2 Welke redenen zou een ethische hacker kunnen hebben om niet te willen doen aan Responsible Disclosure?

Antwoord 1.4.2 Ook voor de ethische hacker zijn een aantal redenen te bedenken.

- De eerste reden is dat een ethische hacker zich beperkt kan voelen door de leidraad. Door te doen aan Responsible Disclosure moet de ethische hacker zich houden aan de opgestelde regels in het beleid van de systeemeigenaar. Dit kan betekenen dat de ethische hacker niet alles kan vinden en/of bekendmaken. Ook kan deze beperking een soort angst opwekken, omdat een ethische hacker bang kan zijn dat hij zich per ongeluk niet aan de regels houdt. Wanneer hij zich niet aan het beleid houdt, loopt hij het risico dat de systeemeigenaar aangifte doet of hem een civiel proces aanspant.
- De tweede reden is dat een ethische hacker gewoon niet altijd aan Responsible Disclosure kan doen, ook al wil hij dit wel. Dit komt voor wanneer een systeemeigenaar geen beleid voor Responsible Disclosure heeft opgesteld. De ethische hacker wil de kwetsbaarheid dan wel op een verantwoorde manier melden, maar kan dit niet doen als de systeemeigenaar er niet voor openstaat.
- De derde reden kan zijn dat een ethische hacker alsnog onderzocht en vervolgd kan worden door het Openbaar Ministerie. Dit creëert wederom een soort angst, angst om zowel de erkenning voor de vondst kwijt te raken, als om vervolgd te worden. Een ethische hacker is al snel strafbaar bezig en het is onduidelijk wanneer het Openbaar Ministerie een ethische hacker vervolgd. Het kader dat is voorgesteld door het college van procureurs generaal brengt hier al wel wat meer duidelijkheid, maar enkel voor een officier van justitie en niet voor een ethische hacker. Een ethische hacker weet namelijk niet hoe een officier van justitie de vragen in het kader zal gaan beantwoorden. Als een ethische hacker geen zin heeft om onderzocht dan wel vervolgd te worden, dan zou hij ervoor kunnen kiezen om niet aan Responsible Disclosure te doen. In de luchtvaart was het ondernemen van strafrechtelijke processen tegen piloten en luchtverkeersleiders de oorzaak voor een vermindering in het aantal meldingen van voorvallen. Het is mogelijk dat hetzelfde gebeurt met Responsible Disclosure[5].

Alinea 5

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 één van waarborgen voorziene handelwijze.

Analyse

Hier staat dus dat goede afspraken volgens de minister de sleutel zijn tot een goede samenwerking tussen ethische hackers en kwetsbare partijen. Ook staat er dat de leidraad inzicht biedt in hoe een organisatie vorm kan geven aan een eigen beleid. Dit roept een aantal vragen op, welke aansluiten bij hoofdprobleem 2 en 3.

Vraag 1.5.1 In deze alinea spreekt de minister over een beleid opstellen en goede afspraken maken en doet hij alsof deze handelingen hetzelfde zijn. Zijn deze handelingen echter wel hetzelfde?

Antwoord 1.5.1 Nee deze handelingen zijn niet hetzelfde. De minister spreekt in alinea 5 over afspraken maken alsof dat hetzelfde is als een beleid opstellen, maar dit is niet het geval. Een beleid opstellen wordt door één partij gedaan, in dit geval de systeemeigenaar. Het maken van afspraken wordt tussen twee partijen gedaan, waardoor afspraken ontstaan waar beide partijen het mee eens zijn.

Vraag 1.5.2 De minister zegt dat het goed is om samen te werken op basis van afspraken en dat goede afspraken zelfs essentieel zijn voor een goede samenwerking. Een groot deel van de 'afspraken' komen voort uit een beleid dat de systeemeigenaar heeft opgesteld en dus is de samenwerking vooral gebaseerd op dit beleid. Is het nu nog wel mogelijk dat er een goede samenwerking ontstaat?

Antwoord 1.5.2 Dit is van twee dingen afhankelijk: het beleid dat een systeemeigenaar opstelt en de belangen van de ethische hacker. Als het beleid de belangen van een ethische hacker voldoende tegemoet komt, dan kan er een goede samenwerking ontstaan. Doet het beleid dit echter niet, dan is de kans groot dat een ethische hacker de melding niet met behulp van Responsible Disclosure zal doen.

Vraag 1.5.3 Wat te doen wanneer een ethische hacker of een kwetsbare partij zich niet aan de afspraken houdt?

Antwoord 1.5.3 De leidraad beschrijft enkel wat er gebeurt wanneer een ethische hacker niet handelt conform het beleid. De systeemeigenaar is dan namelijk niet meer gebonden aan de 'afspraak' om geen aangifte te doen of om geen civiel proces aan te spannen. Wat er echter gebeurt wanneer de systeemeigenaar niet handelt conform het beleid, wordt nergens beschreven in de leidraad.

Alinea 6

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.

Analyse, deel 1

Met alinea 6 geeft de minister aan dat hij de huidige strafrechtelijke kaders niet wil aanpassen. Dit houdt in dat alle strafbare handelingen die in hoofdstuk 2 beschreven zijn, strafbaar blijven, ongeacht de motieven achter een strafbare handeling. Dit roept een vraag op, die aansluit bij hoofdprobleem 4.

Vraag 1.6.1 Is het behouden van de huidige strafrechtelijke kaders bevorderend voor het behalen van het doel dat de leidraad voor Responsible Disclosure wil bereiken?

Antwoord 1.6.1 Nee, in tegendeel zelfs. Door de strafrechtelijke kaders te laten zoals zij nu zijn, zullen ethische hackers al snel strafbaar bezig zijn als zij een kwetsbaarheid zoeken. Dit betekent dat alle ethische hackers die bang zijn om als verdachte gemerkt of vervolgd te worden, een kwetsbaarheid waarschijnlijk niet met behulp van Responsible Disclosure bekend durven te maken. Wellicht kiezen zij voor een andere manier van bekendmaken, waarbij het risico om als verdachte gemerkt te worden kleiner is, of kiezen zij ervoor om de kwetsbaarheid helemaal niet bekend te maken.

Alinea 7

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.

Analyse

De minister zegt met deze alinea dat systeemeigenaren zelf mogen beslissen of zij een beleid voor Responsible Disclosure opstellen of niet. Dit lijkt erg voor de hand te liggen, omdat de systeemeigenaar tenslotte de eigenaar van het systeem is. Dit ligt echter niet altijd zo voor de hand. Deze alinea roept twee vragen op, waarvan de tweede vraag aansluit bij hoofdprobleem 3.

Vraag 1.7.1 Sommige kwetsbaarheden kunnen grote negatieve maatschappelijke, economische en financiële gevolgen hebben, welke niet alleen voor de kwetsbare systeemeigenaar zijn. Dit is bijvoorbeeld het geval bij een kwetsbare systeemeigenaar wiens systeem privacy-gevoelige klantinformatie bevat. Mag de systeemeigenaar dan nog steeds zelf beslissen of hij een beleid voor Responsible Disclosure opstelt?

Antwoord 1.7.1 Om binnen de scope van deze analyse te blijven, zullen we alleen antwoord geven op de vraag vanuit het oogpunt van de minister en met het oog op het doel dat de leidraad wil bereiken. Als we dit doen dan is het antwoord op de vraag ja, de systeemeigenaar mag zelf beslissen of hij een beleid opstelt. De minister maakt namelijk geen onderscheid tussen verschillende soorten kwetsbaarheden of tussen verschillende soorten systemen.

Vraag 1.7.2 Kan een ethische hacker een kwetsbaarheid met behulp van Responsible Disclosure oplossen als de systeemeigenaar geen beleid heeft opgesteld?

Antwoord 1.7.2 Nee dit kan niet. De ethische hacker kan natuurlijk wel handelen zoals in de leidraad wordt beschreven, maar loopt dan het risico dat de systeemeigenaar hem aangeeft of een civiel proces aanspant.

Hoofdstuk 1 van de leidraad, Wat is een kwetsbaarheid?

In dit hoofdstuk beschrijft de minister wat voor kwetsbaarheden er zijn en wat de gevolgen kunnen zijn van een kwetsbaarheid.

Alinea 1 - 3

Systemen kunnen door kwetsbaarheden mogelijkerwijs uitvallen (beschikbaarheid), data binnen het systeem kan gewijzigd worden (integriteit) en data kan 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.

Analyse

Dit stuk benadrukt nog eens waarom het belangrijk is dat kwetsbaarheden gevonden worden, voordat zij uitgebuit kunnen worden. De minister noemt hier niet alle indirecte belanghebbenden van systeemeigenaren, zoals klanten of patiënten.

De minister vergeet hier een paar basis principes van computer security. Hij vergeet namelijk non-repudiation, authenticity en accountability.

Hoofdstuk 2 van de leidraad, Responsible Disclosure

Dit hoofdstuk behandelt wat Responsible Disclosure inhoudt en wat het doel is van Responsible Disclosure.

Alinea 1

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.

Analyse

Met deze alinea wil de minister nog eens benadrukken dat Responsible Disclosure volgens hem echt de voorkeur heeft over Full Disclosure. Het is dus volgens de minister belangrijk dat er zoveel mogelijk kwetsbaarheden worden opgelost met behulp van Responsible Disclosure.

Vraag 2.1.1 Om zoveel mogelijk kwetsbaarheden met behulp van Responsible Disclosure op te lossen, moet Responsible Disclosure wel aantrekkelijk zijn voor ethische hacker. Om het aantrekkelijk te maken, moeten we weten wat een ethische hacker wil bereiken.

Antwoord 2.1.1 Ethische hackers zijn hackers die bewust of onbewust een kwetsbaarheid in een systeem vinden en deze graag verholpen willen zien. Zij willen dus de ICT-wereld verbeteren. Ethische hackers willen waarschijnlijk niet als verdachte gemerkt of vervolgd worden voor hun goede bedoelingen. Ook willen zij waarschijnlijk niet dat de systeemeigenaar hun aangeeft of hun een civiel proces aanspant, als zij de systeemeigenaar proberen te helpen. Verder is het ook mogelijk dat ethische hackers graag erkenning willen voor hun vondst(en) en is een beloning voor het goed omgaan met de kwetsbaarheid waarschijnlijk ook welkom.

Alinea 2

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.

Analyse Het is momenteel onduidelijk wie wel en wie niet deel uitmaakt van de ICT-community.

Alinea 3 - 4

Deze alinea's zijn vooral herhaling van wat het doel is van de leidraad voor Responsible Disclosure, namelijk het op een verantwoorde wijze bekendmaken en oplossen van kwetsbaarheden.

Alinea 5

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.

Analyse

De minister spreekt wederom over afspraken, terwijl er eigenlijk sprake is van een beleid dat de systeemeigenaar opstelt waar de ethische hacker zich aan moet houden. Ook zegt de minister dat de systeemeigenaar niet meer gebonden is aan het niet doen van aangifte, als een ethische hacker niet handelt volgens het door de systeemeigenaar opgestelde beleid.

Alinea 6

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.

Analyse

In deze alinea spreekt de minister wederom alleen over melders, terwijl de melder en de ontdekker van een kwetsbaarheid niet dezelfde persoon hoeven te zijn.

Als het aankomt op het bekendmaken van kwetsbaarheden dan kun je een onderscheid maken tussen voor de systeemeigenaar specifieke kwetsbaarheden, in eigen software, configuratie of versie en algemene kwetsbaarheden, bijvoorbeeld in Windows. De bekendmaking van algemene kwetsbaarheden hoeft niet noodzakelijk in overleg met de systeemeigenaar. De specifieke kwetsbaarheden daarentegen kunnen beter wel pas bekend gemaakt worden, na overleg met de systeemeigenaar.

Hoofdstuk 3 van de leidraad, Verantwoordelijkheden

Dit hoofdstuk gaat over welke partij welke verantwoordelijkheden heeft. Er zijn drie hoofdgroepen betrokken bij Responsible Disclosure, de kwetsbare partij, de melder en ontdekker, en het NCSC. Al deze partijen hebben verantwoordelijkheden tijdens de uitvoering van Responsible Disclosure en daar wordt in dit hoofdstuk naar gekeken.

3.1 Verantwoordelijkheden van de organisatie

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.

Context bij alinea 3.1, verantwoordelijk zijn

Wat houdt het eigenlijk in wanneer een systeemeigenaar verantwoordelijk is voor de beveiliging van het systeem? Dit houdt in dat het systeem van de systeemeigenaar moet voldoen aan een aantal wetten die beschrijven hoe de beveiliging van een systeem moet zijn. Een voorbeeld van deze wetten is de Wet Bescherming Persoonsgegevens (WBP).

Ook houdt deze verantwoordelijkheid in dat de systeemeigenaar aansprakelijk gesteld kan worden als blijkt dat de beveiliging van het systeem niet in orde is. Dit houdt dus ook in dat het een systeemeigenaar kwalijk genomen kan worden, als hij niet verantwoordelijk omgaat met een melding van een kwetsbaarheid. Wie hem dit kwalijk neemt is afhankelijk van wie betrokken zijn bij een veilig systeem. Dit kunnen bijvoorbeeld klanten of medewerkers zijn.

Analyse

De minister zegt met deze alinea dat systeemeigenaren verantwoordelijk zijn voor de beveiliging van hun eigen systeem. De minister zegt ook dat de leidraad die hij heeft opgesteld een goede richtlijn is om een goed gevolg te geven aan een melding van een kwetsbaarheid.

3.2 Verantwoordelijkheden van 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. De melder van een kwetsbaarheid is verantwoordelijk voor het eigen handelen en de wijze waarop hij 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.

Analyse, deel 1 Dit is een interessante alinea en roept dan ook drie vragen op. De eerste twee vragen sluiten aan bij hoofdprobleem 4.

Vraag 3.2.1 Is het voor een ethische hacker mogelijk om nooit strafbaar te handelen, als hij op zoek is naar een kwetsbaarheid?

Antwoord 3.2.1 Het antwoord op deze vraag is zowel ja als nee en is afhankelijk van wat de minister wil bereiken met de leidraad.

Als de minister zoveel mogelijk kwetsbaarheden uit een systeem wil halen met behulp van Responsible Disclosure, dan is het antwoord op deze vraag nee: een ethische hacker moet dan strafbaar handelen. Als een hacker de toegang tot een ICT-systeem weet te verwerven door een technische ingreep, dan is dat een strafbare handeling. Dit betekent dus dat er een kwetsbaarheid in het systeem zit, die een ethische hacker alleen kan vinden, als hij strafbaar handelt. Om dus zoveel mogelijk kwetsbaarheden te vinden, moet een ethische hacker ook strafbaar handelen.

Als de minister echter maar een beperkt aantal kwetsbaarheden wil laten oplossen met behulp van Responsible Disclosure, dan is het antwoord ja, een ethische hacker hoeft niet strafbaar te handelen.

Analyse, deel 2

De minister geeft met alinea 3.2 aan dat het Openbaar Ministerie een ethische hacker strafrechtelijk mag onderzoeken dan wel vervolgen als een ethische hacker (vermoedelijk) strafbaar heeft gehandeld. Aangezien de strafrechtelijke kaders niet zijn aangepast, wordt er vanuit de wet geen rekening gehouden met eventuele ethische motieven en is de ethische hacker dus al snel strafbaar bezig. Dit betekent echter niet dat ethische motieven niet meegenomen worden in de beoordeling van een ethische hacker. Dit heeft als resultaat dat het onduidelijk is wanneer een ethische hacker vervolgd moet worden en wanneer niet. Om dit duidelijker te maken heeft het college van procureurs generaal een kader voorgesteld.

Context bij 3.2, kader van het college van procureurs generaal

Het college van procureurs generaal heeft een kader voorgesteld bestaande uit een drietal vragen. Dit kader is gemaakt om duidelijker te maken wanneer een ethische hacker vervolgd moet worden. Een officier van justitie kan dit kader gebruiken om te bepalen of een ethische hacker vervolgd moet worden, door antwoord te geven op de drie vragen. Om antwoord op de vragen in het kader te krijgen, moet een ethische hacker die (vermoedelijk) strafbaar heeft gehandeld eerst als verdachte worden gemerkt, zodat er dankzij strafrechtelijk onderzoek antwoord kan worden verkregen op de vragen uit het kader[6].

In een vergadering met de tweede kamer op woensdag 29 Mei 2013 is de toepassing van het kader aangepast. Het originele voorstel was om het kader te gebruiken voor ethische hackers die een directe melding doen bij een systeemeigenaar met een beleid voor Responsible Disclosure. Het voorstel is nu om ook ethische hackers te onderzoeken die een melding doen bij een systeemeigenaar zonder beleid voor Responsible Disclosure, zodat ook voor hun antwoord op de vragen in het kader kan worden verkregen.

Analyse, deel 3

Het kader van het college van procureurs generaal maakt het duidelijker wanneer een ethische hacker vervolgd wordt. Het maakt het echter alleen duidelijker voor een officier van justitie en niet voor de ethische hacker zelf. Dit is omdat de ethische hacker niet weet hoe een officier van justitie de vragen in het kader gaat beantwoorden. Wel weet de ethische hacker dat de kans groot is dat hij als verdachte wordt gemerkt, omdat hij waarschijnlijk strafbaar heeft moeten handelen om een kwetsbaarheid te vinden.

Vraag 3.2.2 Kan de leidraad haar doel beter bereiken als gebruik wordt gemaakt van dit kader?

Antwoord 3.2.2 Een ethische hacker weet dus nog niet wanneer hij vervolgd wordt, maar hij weet wel dat hij waarschijnlijk strafrechtelijk onderzocht wordt, zodat een officier van justitie kan bepalen of de ethische motieven van de ethische hacker voldoende ethisch zijn om hem te vrijwaren van verder onderzoek of vervolging. Dit kan als resultaat hebben dat ethische hackers

een andere manier van bekendmaken prefereren, waarbij de kans op strafrechtelijk onderzoek en vervolging kleiner is. Dit zou dus betekenen dat deze ethische hackers geen gebruik maken van Responsible Disclosure. Dit is echter niet zeker omdat er nog niet genoeg empirische data beschikbaar is.

Vraag 3.2.3 Een andere vraag die dit stuk oproept is: waarom doet de minister wel uitspraak over het civiel recht, het recht waar hij eigenlijk niets over te zeggen heeft, maar verandert hij het strafrecht niet, het recht waar hij wel iets over te zeggen heeft?

Antwoord 3.2.3 Het antwoord op deze vraag is onbekend.

3.3 Verantwoordelijkheden van 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.

Analyse Het NCSC kan dus helpen met het bekendmaken van de kwetsbaarheid bij de rest van de ICT-community. Ook kan het NCSC helpen om een melder en een (kwetsbare) systeemeigenaar met elkaar in contact te brengen.

Hoofdstuk 4 van de leidraad, Bouwstenen voor Responsible Disclosure

In dit hoofdstuk beschrijft de minister de bouwstenen voor wat hij noemt Responsible Disclosure.

4.1 De organisatie

De eerste twee alinea's zijn herhaling van wat eerder al is gezegd. Hier wordt voornamelijk uitgelegd dat de systeemeigenaar verantwoordelijk is voor hoe hij met een kwetsbaarheid omgaat en dat hij met het opstellen van een beleid aan kan geven hoe hij een vervolg wil geven aan een melding.

Alinea 3

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.

Analyse

We zagen bij hoofdstuk 3.2, vraag 3.2.2 dat de kans groot is dat ethische hackers als verdachte gemerkt worden en dat ethische hackers die hier angst voor hebben mogelijk voor een andere manier van bekendmaken kiezen. Als een systeemeigenaar zijn beleid echter dusdanig maakt dat een ethische hacker gemakkelijk een anonieme melding kan doen, dan is het goed mogelijk dat een ethische hacker, die bang is om als als verdachte gemerkt of vervolgd te worden, wel gebruik maakt van Responsible Disclosure. Dit is omdat hij dan anoniem kan blijven en zonder angst voor strafrechtelijke processen gebruik kan maken van Responsible Disclosure.

Alinea 4 tot en met 14 Elke alinea representeert een bouwsteen die een systeemeigenaar kan gebruiken in het opstellen van een eigen beleid voor Responsible Disclosure.

- *De organisatie reserveert capaciteit om adequaat op meldingen te kunnen reageren.*

  Het is belangrijk dat een systeemeigenaar voldoende capaciteit reserveert, zodat een kwetsbaarheid binnen de opgegeven termijn opgelost kan worden. Dit is niet alleen om de ethische hacker tevreden te stellen, maar ook om de kans op uitbuiting zo klein mogelijk te maken. Wat echter capaciteit inhoudt en wanneer het voldoende is om adequaat op meldingen te kunnen reageren wordt niet behandeld in de leidraad. Deze bouwsteen is dus onvolledig. Verder is er nog een vraag over deze bouwsteen.

  Vraag 4.1.1 Hoe moeten de systeemeigenaar en de ethische hacker handelen als de systeemeigenaar te weinig capaciteit heeft om de kwetsbaarheid op te lossen?

  Antwoord 4.1.1 Deze kwestie wordt niet besproken in de leidraad.

- *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.*

  Deze afdeling moet dus te allen tijde voldoende capaciteit beschikbaar hebben om een melding van een kwetsbaarheid af te handelen.

- *De organisatie stuurt een ontvangstbevestiging van de melding aan de melder, bij voorkeur digitaal ondertekend om de prioriteit te benadrukken. Hierna treden de organisatie en de melder in contact over het verdere proces.*

Opmerking voor de duidelijkheid: een melder is dus niet altijd ook de ethische hacker.

- *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.*

  Deze bouwsteen roept één vraag op, die aansluit bij hoofdprobleem 1.

  Vraag 4.1.2 Hoe moeten de systeemeigenaar en de ethische hacker handelen als de systeemeigenaar de kwetsbaarheid niet binnen de opgegeven termijn heeft verholpen.

  Antwoord 4.1.2 Deze kwestie wordt niet besproken in de leidraad.

- *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.*

  Kwetsbaarheden zijn er in alle soorten en maten en het verhelpen van de ene kwetsbaarheid kan langer duren dan de andere. Deze bouwsteen houdt daar goed rekening mee.

- *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.*

  Deze bouwsteen is onduidelijk. Ten eerste is het onduidelijk wie bepaalt wanneer een kwetsbaarheid te moeilijk is om op te lossen. Bepaalt de systeemeigenaar dit of de ethische hacker of bepalen zij dit misschien samen? En wat als bijvoorbeeld te systeemeigenaar het probleem te moeilijk acht en de ethische hacker niet[7]?

  Ten tweede is onduidelijk wat de minister precies bedoelt met deze bouwsteen. Bedoelt hij dat de kwetsbaarheid nog wel opgelost moet worden, maar dat de kwetsbaarheid alleen niet bekend gemaakt wordt of bedoelt hij dat het hele Responsible Disclosure proces wordt stopgezet en dat de kwetsbaarheid noch wordt verholpen noch bekend wordt gemaakt?

  Deze bouwsteen is belangrijk omdat het inderdaad voor kan komen dat een kwetsbaarheid echt niet op te lossen is om welke reden dan ook. Het mag echter niet voorkomen dat een kwetsbaarheid onterecht niet verholpen wordt. Het is daarom belangrijk dat deze bouwsteen vollediger wordt uitgewerkt.

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

  Op de hoogte houden is onvoldoende uitgewerkt. Op de hoogte houden kan betekenen dat de systeemeigenaar elke week een uitgebreid rapport stuurt naar de ethische hacker, maar kan ook betekenen dat de systeemeigenaar elke maand even zegt dat hij er nog mee bezig is. Deze bouwsteen komt teveel de belangen van de systeemeigenaar tegemoet, omdat hij momenteel mag beslissen wat op de hoogte houden inhoudt. Deze bouwsteen sluit aan bij hoofdprobleem 1 en 3.

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

  Bij deze bouwsteen moet rekening gehouden worden met het feit dat een andere manier van bekendmaken gegarandeerd credits kan geven voor het ontdekken van de kwetsbaarheid en

dat dat de ethische hacker deze manier kan prefereren als de systeemeigenaar geen credits wil geven.

- *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.*

  Een beloning kan een extra motivatie zijn voor een ethische hacker om een melding direct bij de betreffende kwetsbare systeemeigenaar te doen. Ook kan het een stimulans zijn om zo te handelen dat de systeemeigenaar geen schade ondervindt van het handelen van de ethische hacker. Ook laat het geven van een beloning zien dat een systeemeigenaar waardering heeft voor wat ethische hackers doen. Dit alles creëert een vriendelijk sfeer en daardoor een betere samenwerking.

  Deze bouwsteen heeft echter nog een gevolg. Doordat er nu geld te verdienen valt met het melden van een kwetsbaarheid bij de betreffende kwetsbare systeemeigenaar, zullen hackers minder geneigd zijn om op een andere manier geld te verdienen met de kwetsbaarheid. Dit kunnen ze bijvoorbeeld doen door informatie over de kwetsbaarheid te verkopen in het criminele circuit.

- *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.*

  Er is een grote kans dat de ethische hacker dit zelf al gaat vertellen aan de ICT-community, uiteraard zonder de kwetsbare systeemeigenaar te noemen waar hij de kwetsbaarheid heeft gevonden. Hier kan dus ook weer sprake zijn van een onderscheid tussen algemene en specifieke kwetsbaarheden, waarbij vooral de algemene kwetsbaarheden verder verteld kunnen worden. Het is belangrijk dat de ICT-community wordt geïnformeerd zodat de kwetsbaarheid ook bij andere kwetsbare systeemeigenaren gevonden en verholpen kan worden. Als een commercieel security bedrijf een kwetsbaarheid vindt, dan mag dit bedrijf waarschijnlijk de informatie over de kwetsbaarheid niet verder communiceren vanwege geheimhoudingsplicht. Dit mag de ethische hacker wel. Verder roept dit punt nog een vraag op, die aansluit bij hoofdprobleem 1.

  Vraag 4.1.3 Wanneer moet de ethische hacker zijn vondst publiekelijk bekendmaken? Mag hij dit doen nadat de systeemeigenaar waar hij de kwetsbaarheid heeft gevonden, de kwetsbaarheid heeft verholpen of pas als alle systeemeigenaren in de ICT-community de kwetsbaarheid hebben verholpen?

  Antwoord 4.1.3 Volgens de leidraad mag de ethische hacker zijn vondst publiekelijk bekendmaken zodra de systeemeigenaar bij wie hij de kwetsbaarheid gevonden heeft, deze kwetsbaarheid heeft opgelost. Dit levert echter potentieel gevaar op voor de andere kwetsbare systeemeigenaren, omdat hackers nu ook bekend worden met de kwetsbaarheid. Hierdoor kan er een soort race ontstaan tussen de hackers en de kwetsbare systeemeigenaren, omdat de hackers, de kwetsbaarheid willen uitbuiten en omdat de kwetsbare systeemeigenaar, de kwetsbaarheid op tijd wil verhelpen om uitbuiting te voorkomen.

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

  Het niet ondernemen van juridische vervolgstappen houdt dus in dat de systeemeigenaar geen aangifte doet van de ethische hacker en dat de systeemeigenaar de ethische hacker ook geen civiel proces aanspant.

4.2 De melder

Zoals de leidraad al een aantal keer heeft vermeld, is de melder de spil in het kunnen voeren van een praktijk van Responsible Disclosure. Het woord melder is in dit geval een beetje onduidelijk, omdat niet alleen de melder wordt bedoeld, maar ook de ontdekker. Om deze reden zal het vanaf nu weer om ethische hackers gaan.

Ethische hackers willen kwetsbaarheden vinden en hierdoor bijdragen aan de veiligheid van ICT-systemen, door deze kwetsbaarheden bekend te maken bij de betreffende systeemeigenaar. De ethische hacker ziet dus in dat hij een maatschappelijke verantwoordelijkheid draagt en deze neemt door de kwetsbaarheden verantwoord te openbaren. Hieronder worden een aantal bouwstenen opgesomd, die beschrijven hoe een ethische hacker volgens de minister moet handelen in het Responsible Disclosure proces.

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

  De melding zou eventueel ook bij het NCSC gedaan kunnen worden, zodat het NCSC de ethische hacker en de systeemeigenaar bij elkaar brengt.

- *De melder zal een melding zo snel als mogelijk doen, om te voorkomen dat kwaadwillenden de kwetsbaarheid ook vinden en er misbruik van maken.*

  Dus als een ethische hacker zijn melding niet zo snel mogelijk doet, dan handelt hij niet volgens het beleid en kan de systeemeigenaar hem een civiel proces aanspannen of hem aangeven. Dit punt lijkt erg in het voordeel van de systeemeigenaar.

- *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 kwetsbare systeemeigenaar moet wel duidelijk aangeven bij wie en hoe een ethische hacker een melding moet doen.

- *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.*

    Als iemand door social engineering toegang kan verschaffen tot het systeem, dan is dit wel degelijk een kwetsbaarheid bij de systeemeigenaar, alleen geen kwetsbaarheid in zijn ICT-systeem. Deze leidraad heeft het alleen over kwetsbaarheden in ICT-systemen en daarom zullen we hier niet verder over doorgaan.

  - *door een eigen backdoor in een informatiesysteem te plaatsen om vervolgens daarmee de kwetsbaarheid aan te tonen, aangezien daarmee aanvullende schade kan worden aangericht en onnodige veiligheidsrisicos worden gelopen.*

    Het ICT-systeem controleren op backdoors kan veel geld kosten.

  - *door een kwetsbaarheid verder uit te nutten dan noodzakelijk is om de kwetsbaarheid vast te stellen.*

    Dit punt roept een aantal vragen op, die aansluiten bij hoofdprobleem 1 en 3.

    Vraag 4.2.1 Wat is noodzakelijk?

    Antwoord 4.2.1 Dit is erg geval afhankelijk. Je zou kunnen zeggen dat het minimale al genoeg is. Bijvoorbeeld als het saldo van een OV-chipkaart met behulp van een

kwetsbaarheid zonder te betalen opgehoogd kan worden, dan is het al voldoende om het saldo met €0.01 op te hogen om de kwetsbaarheid aan te tonen. In het geval dat een database niet beschermd is, zou het lezen van één enkele onbelangrijke database record al genoeg moeten zijn. Zo kan er voor elke kwetsbaarheid wel een minimale uitbuiting worden bedacht.

Vraag 4.2.2 Wat als een kwetsbare systeemeigenaar het hoogst noodzakelijke niet genoeg vindt?

Antwoord 4.2.2 De ethische hacker zou de kwetsbaarheid meer kunnen uitbuiten, zodat de systeemeigenaar misschien wel door krijgt dat de kwetsbaarheid serieus genomen moet worden. Zo kan de ethische hacker bijvoorbeeld het saldo van een OV-chipkaart met 100 euro verhogen en kijken of de systeemeigenaar dan reageert. Volgens de leidraad mag hij dit echter niet doen.

Ook kan de ethische hacker proberen om de melding via het NCSC te doen.

– *door gegevens van het systeem te kopiëren, te wijzigen of te verwijderen. Een alternatief hiervoor is het maken van een directory listing van een systeem.*

Een directory listing is de structuur van een directory en is inderdaad een oplossing waarmee de kwetsbare systeemeigenaar zo min mogelijk wordt geschaad.

– *door veranderingen in het systeem aan te brengen.*

Maar wat als het nodig is om aanpassingen te maken aan het systeem om een kwetsbaarheid aan te tonen? Is de ethische hacker dan toch strafbaar bezig, ondanks dat hij de kwetsbaarheid anders niet aan kan tonen?

– *door herhaaldelijk toegang tot het systeem te verkrijgen of de toegang te delen met anderen.*

Soms kan het nodig zijn om meerdere keren toegang te verkrijgen tot het systeem, bijvoorbeeld om nog eens na te gaan hoe de kwetsbaarheid ook alweer in elkaar zit. Deze bouwsteen is erg restrictief voor de ethische hacker en ook onnodig. Zolang de ethische hacker geen schade aanricht aan het systeem, is het niet erg als hij herhaaldelijk toegang verkrijgt. Deze bouwsteen sluit aan bij hoofdprobleem 3.

– *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.*

Soms is de sterkte van wachtwoorden zo zwak dat het bruteforcen van deze wachtwoorden wel degelijk een kwetsbaarheid aantoont. Als bijvoorbeeld de sluizen in Nederland zijn vergrendeld met Stadsnaam gevolgd door het huidige jaartal, dan is dit zeker een kwetsbaarheid.

- *Als melder en organisatie overeenkomen 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.*

Dit stuk roept twee vragen op, die aansluiten bij hoofdprobleem 1.

Vraag 4.2.3 Over welke organisaties heeft de minister het, als hij spreekt over alle betrokken organisaties? Bedoelt hij dan alle kwetsbare systeemeigenaren die deze kwetsbaarheid in het systeem hebben of bedoelt hij de organisaties die betrokken zijn bij de systeemeigenaar waar de kwetsbaarheid is gemeld?

Vraag 4.2.3 Het antwoord op deze vraag is onbekend.

Vraag 4.2.4 In hoofdstuk 4.1 van de leidraad staat bij bouwsteen 4 dat een systeemeigenaar en een ethische hacker in overleg een termijn bepalen waarop eventuele bekendmaking zal plaatsvinden. In deze alinea zegt de minister echter dat een ethische hacker de kwetsbaarheid pas bekend mag maken, als alle betrokken systeemeigenaren goed zijn geïnformeerd en zij aangegeven hebben dat de kwetsbaarheid is opgelost, conform de afspraken. De vraag is nu, mag de ethische hacker de kwetsbaarheid bekendmaken na het verstrijken van de afgesproken termijn of mag dit pas nadat de kwetsbaarheid is opgelost bij alle bekende kwetsbare systeemeigenaren?

Antwoord 4.2.4 Het antwoord op deze vraag is onbekend.

- *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.*

  Door eerst zoveel mogelijk andere kwetsbare systeemeigenaren in te lichten over de kwetsbaarheid, voordat de kwetsbaarheid publiekelijk bekend wordt gemaakt, verklein je het risico dat de kwetsbaarheid wordt uitgebuit bij een andere kwetsbare systeemeigenaar. Dit is omdat deze kwetsbare systeemeigenaren dan al bewust zijn van de kwetsbaarheid en deze kunnen oplossen voordat een hacker bekend wordt met de kwetsbaarheid. Dit roept echter wel een vraag op.

  Vraag 4.2.5 Moet een ethische hacker wachten met publieke bekendmaking van de kwetsbaarheid totdat alle kwetsbare systeemeigenaren de kwetsbaarheid hebben opgelost of mag hij de kwetsbaarheid al eerder bekendmaken?

  Antwoord 4.2.5 Het antwoord op deze vraag is afhankelijk van het antwoord op vraag 4.2.3, namelijk wie zijn die betrokken organisaties die eerst de kwetsbaarheid moeten oplossen, voordat een ethische hacker over kan gaan tot publiekelijke bekendmaking. Het antwoord op deze vraag is dus onbekend.

4.3 Het NCSC

In dit stuk staan de bouwstenen die te maken hebben met het NCSC.

- *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.*

  Dit kan een fijne optie zijn voor een ethische hacker, als hij een kwetsbaarheid heeft gevonden bij een systeemeigenaar die niet zo openstaat voor zijn melding. Dit komt omdat het NCSC waarschijnlijk meer invloed heeft dan een (onbekende) ethische hacker. Dit stuk roept echter wel een vraag op, aansluitend bij hoofdprobleem 1.

  Vraag 4.3.1 Bedoelt de minister met deze alinea dat het NCSC alle ethische hackers en systeemeigenaren zal trachten bij elkaar te brengen of enkel de systeemeigenaren die een beleid voor Responsible Disclosure hebben opgesteld?

  Antwoord 4.3.1 Het antwoord op deze vraag is onbekend.

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

  Deze bouwsteen roept vraag 4.2.5 wederom op, het antwoord is nog steeds onduidelijk.

Conclusie

In dit stuk zal een mogeljk antwoord worden gegeven op de onderzoeksvraag. De onderzoeksvraag is:

Bereikt de leidraad voor Responsible Disclosure in de huidige staat haar doel?

Er zijn vier punten van kritiek gevonden op de leidraad. De invloed van deze punten van kritiek is onduidelijk omdat de empirische data nog niet beschikbaar is. Zo is er bijvoorbeeld nog geen empirische data over hoe Responsible Disclosure processen in de praktijk verlopen en ook niet over hoeveel kwetsbaarheden er opgelost worden met Responsible Disclosure ten opzichte van andere manieren van bekendmaken van kwetsbaarheden. Hierdoor is het niet mogelijk om een volledig kloppend antwoord te geven op de onderzoeksvraag. Door alle kritiekpunten samen te vatten en hun mogelijke invloed te noemen, krijgen we een mogelijk antwoord op de onderzoeksvraag. Dit antwoord kan gebruikt worden om meer inzicht te krijgen in waarom de leidraad voor Responsible Disclosure haar doel niet zou bereiken.

Het eerste kritiekpunt op de leidraad gaat over onvolledigheid. De leidraad is onvolledig in zowel het beschrijven van het gewone Responsible Disclosure proces als de uitzonderingsgevallen, waardoor de leidraad minder robuust is. Dit houdt in dat de kans bestaat dat het Responsible Disclosure proces niet verder kan gaan wanneer een onvolledig beschreven situatie zich voordoet; beide partijen weten niet hoe ze het beste verder kunnen gaan of hebben een andere invulling voor de onbeschreven situatie. In deze gevallen haalt de leidraad haar doel mogelijk niet.

Het tweede kritiekpunt op de leidraad gaat over het feit dat de leidraad enkel spreekt over melders en hiermee aanneemt dat een ethische hacker altijd zowel de ontdekker als de melder is. We zagen dat dit niet altijd het geval hoeft te zijn en dat het de leidraad zelfs kan belemmeren om haar doel te halen als de ontdekker en de melder per sé dezelfde persoon moeten zijn. Het nadeel is dan namelijk dat ethische hackers die, om wat voor reden dan ook, geen melder willen zijn, geen melding zullen maken van de door hun gevonden kwetsbaarheid. Dit betekent dus dat er mogelijk minder kwetsbaarheden worden opgelost met behulp van Responsible Disclosure.

Het derde kritiekpunt op de leidraad is dat er een asymmetrie is tussen systeemeigenaren en ethische hackers. Systeemeigenaren hebben meer vrijheid in hun keuzes dan ethische hackers. Dit is bijvoorbeeld te zien aan het feit dat de systeemeigenaar in zijn beleid voor een groot deel bepaalt hoe de samenwerking gaat verlopen. De invloed hiervan kan zijn dat ethische hackers niet voor Responsible Disclosure kiezen om een kwetsbaarheid bekend te maken. Een ander manier van bekendmaken kan de ethische hacker meer vrijheid bieden.

Tot slot hebben we gezien dat de huidige strafrechtelijke kaders en het door het college van procureurs generaal voorgestelde kader, een negatieve invloed kunnen hebben op de leidraad. Omdat ethische hackers niet weten wanneer ze vervolgd worden, maar ze wel weten dat ze strafrechtelijk onderzocht worden als zij (mogelijk) strafbaar hebben gehandeld, bestaat de kans dat ethische hackers voor een andere manier van bekendmaken kiezen. Dit zou vooral het geval zijn als het bij deze andere manier van bekendmaken duidelijker is wanneer zij vervolgd worden of/en de kans op strafrechtelijk onderzoek kleiner is.

Mogelijk antwoord

Het lijkt erop alsof de leidraad voor Responsible Disclosure niet veel gebruikt gaat worden door ethische hackers omdat de leidraad ethische hackers mogelijk afschrikt. Resultaat is dat minder kwetsbaarheden met behulp van Responsible Disclosure worden opgelost. In het geval dat een kwetsbaarheid wel met behulp van Responsible Disclosure wordt opgelost, kan het zijn dat het Responsible Disclosure proces niet verder kan gaan als een onbeschreven situatie zich voordoet. De leidraad kan haar doel dus wel bereiken, maar zal vermoedelijk in de huidige implementatie, niet vaak succesvol gebruikt worden om kwetsbaarheden op te lossen.

Andere invloeden van de leidraad

De leidraad kan nog meer invloeden hebben. Het zal waarschijnlijk zo zijn dat de leidraad invloed gaat hebben via jurisprudentie. Ook zal de leidraad waarschijnlijk invloed hebben op de gedachtegang van systeemeigenaren omdat zij nu meer bekend worden met het fenomeen 'ethische hacker'.

Aanbevelingen

Er zijn 4 hoofdproblemen te bedenken voor de leidraad. In dit hoofdstuk zal voor elk hoofdprobleem, een aanbeveling gedaan worden.

Onvolledigheid Doordat de leidraad onvolledig is, is de leidraad ook minder robuust dan hij zou kunnen zijn. Om een robuustere leidraad te creëeren zouden zoveel mogelijk onvolledigheden opgelost moeten worden. Deze onvolledigheden staan opgesomd bij hoofdprobleem 1, p. 7.

Ethische hackers en melders De minister wil dat een ethische hacker, altijd zelf de melder van een kwetsbaarheid is. Hierdoor zullen ethische hackers die, om wat voor reden dan ook geen melder willen zijn, geen gebruik maken van Responsible Disclosure. Om dit op te lossen zou de leidraad ook indirecte meldingen moeten accepteren. Het nadeel van het ontvangen van indirecte meldingen is dat het moeilijker is om een ethische hacker strafrechtelijk te onderzoeken of vervolgen als hij (vermoedelijk) strafbaar heeft gehandeld. Het voordeel is dat een systeemeigenaar bekend wordt met de kwetsbaarheid en dat hij deze kan oplossen.

Systeemeigenaren vs ethische hackers Door de asymmetrie in de leidraad is het mogelijk dat ethische hackers wederom voor een andere manier van bekendmaken kiezen. Om deze asymmetrie tegen te gaan zou de vrijheid van systeemeigenaren ingeperkt moeten worden en/of de vrijheid van de ethische hackers vergroot.

Strafrechtelijke vervolging of niet? Momenteel is het voor een ethische hacker onduidelijk wanneer hij vervolgd wordt. Een aanbeveling voor dit probleem is om een duidelijkere grens te maken wanneer er strafrechtelijke vervolging plaatsvindt. Een manier om dit te doen is door, op de vragen in het kader van het college van procureurs generaal, voorbeeldantwoorden te geven. Antwoorden die de trigger zijn voor strafrechtelijke vervolging en antwoorden die dat niet zijn. Hierdoor krijgt een ethische hacker meer inzicht in wat hij wel en niet mag doen.

Referenties

[1] I.W. Opstelten Minister van Justitie en Veiligheid. *Leidraad voor responsible disclosure.* 3 januari, 2013.

[2] Novum. *Kamer bezorgd over 'ethische hackers'.* 29 mei, 2013.

[3] Brenno de Winter. *Responsible disclosure richtlijn is onverantwoord risico.* 3 januari, 2013.

[4] Brenno de Winter. *Hackmeldpunt vindt richtlijn ethisch hacken 'uit balans'.* 6 januari, 2013.

[5] Jaap-Henk Hoepman. *Leidraad Responsible Disclosure behoeft aanscherping (door te leren van ervaringen in de luchtvaart).* 4 januari, 2013.

[6] Het college van procureur generaals. *Brief aan de Minister van Justitie en Veiligheid: hoe te handelen bij 'ethische' hackers.* 18 maart, 2013.

[7] Tony Chan Andrew Cencini, Kevin Yu. *Software Vulnerabilities: Full-, Responsible-, and Non-Disclosure.* 7 december, 2005.

Bijlage

Appendix A

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 systeem 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