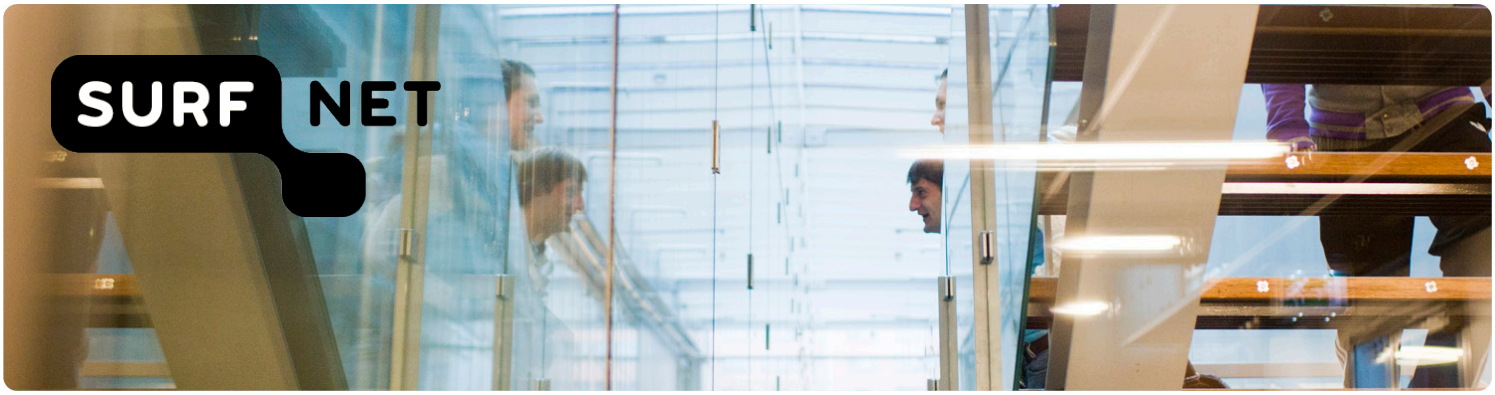


Implementatiehandleiding responsible disclosure

Auteur(s): Milla Cuperus en David van Es, SURFnet

Versie: 1.0

Datum: 9 juli 2014

Moreelsepark 48
3511 EP Utrecht

Postbus 19035
3501 DA Utrecht

088 - 787 30 00
admin@surfnet.nl
www.surfnet.nl

ING Bank NL54INGB0005936709
KvK Utrecht 30090777
BTW NL 0089.60.173.B01

Inhoudsopgave

1 Inleiding

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

SURF heeft een responsible disclosure modelbeleid en een operationele procedure voor responsible disclosure opgesteld voor hoger onderwijsinstellingen. Deze handleiding is ontwikkeld als handvat voor een gedegen invulling van het beleid en de procedure.

Deze implementatiehandleiding is bestemd voor de verantwoordelijke voor het formuleren van het informatiebeveiligingsbeleid van een instelling. De implementatiehandleiding is een middel om te komen tot een gedegen invulling van het responsible disclosure beleid.

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

Het doel van responsible disclosure omvat het volgende:

a) Garanderen dat de geïdentificeerde kwetsbaarheid geadresseerd wordt;
b) Het verkleinen van het risico die ontstaan zijn door de kwetsbaarheid;
c) Gebruikers voorzien van voldoende informatie om de risico's te bepalen die ontstaan zijn door de kwetsbaarheid op hun systemen;
d) Het vaststellen van de verwachtingen om te komen tot een positieve communicatie en coördinatie tussen de betrokkenen.

1.1 Definitie Responsible Disclosure

Er worden uiteenlopende definities gebruikt voor responsible disclosure. De definitie die gebruikt is bij het opstellen van dit document, is de definitie van het Nationaal Cyber Security Center (NCSC): "het op een verantwoorde wijze en in gezamenlijkheid tussen melder en organisatie openbaar maken van ICT-kwetsbaarheden op basis van een door organisaties hiervoor vastgesteld beleid voor responsible disclosure". Uit de definitie van het NCSC blijkt dat er pas sprake is van responsible disclosure als een organisatie een beleid heeft.

1.2 Leeswijzer

In hoofdstuk 2 zijn de argumenten voor het inzetten van responsible disclosure beschreven. Vervolgens is de positionering van het modelbeleid en de procedure aangeven in hoofdstuk 3. De Nederlandse wetgeving en de (internationale) standaarden die van toepassing zijn op responsible disclosure zijn beschreven in hoofdstuk 4 en 5. In hoofdstuk 6 zijn de beslissingspunten voor responsible disclosure beschreven en wordt per beslissing een overweging beschreven die meegenomen kan worden in de besluitvorming door de hoger onderwijsinstelling. In het laatste hoofdstuk staat een stappenplan die gebruikt kan worden om de implementatie van responsible disclosure te plannen.

2 Argumenten voor responsible disclosure beleid HO

IT speelt bij hoger onderwijsinstellingen een belangrijke rol. Een instelling wordt geacht om informatie op een betrouwbare manier te beheren. Om het belang van responsible disclosure voor hoger onderwijsinstellingen aan te geven zijn er hieronder een aantal argumenten opgesomd:

2.1 Verlagen drempel melder

Een hoger onderwijsinstelling kan de drempel tot melden van kwetsbaarheden voor haar doelgroep verlagen. Hoger onderwijsinstellingen en onderzoeksinstellingen komen veel in aanraking met onderzoekers en ICT-kundige studenten. Het is aannemelijk dat onderzoekers en studenten een ICT-kwetsbaarheid herkennen en deze verantwoord willen melden zonder juridische complicaties.

2.2 Spelregels vastleggen

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

2.3 Transparantie

Een transparante houding van hoger onderwijs- en onderzoeksinstellingen is in lijn met hun maatschappelijke rol en vaak ook met de missie en visie van de instelling. Door publicatie van een responsible disclosure beleid geven hoger onderwijs- en onderzoeksinstellingen aan welk standpunt zij innemen in deze kwestie.

2.4 Gemeenschappelijk belang

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

2.5 Verhogen informatiebeveiligingsniveau

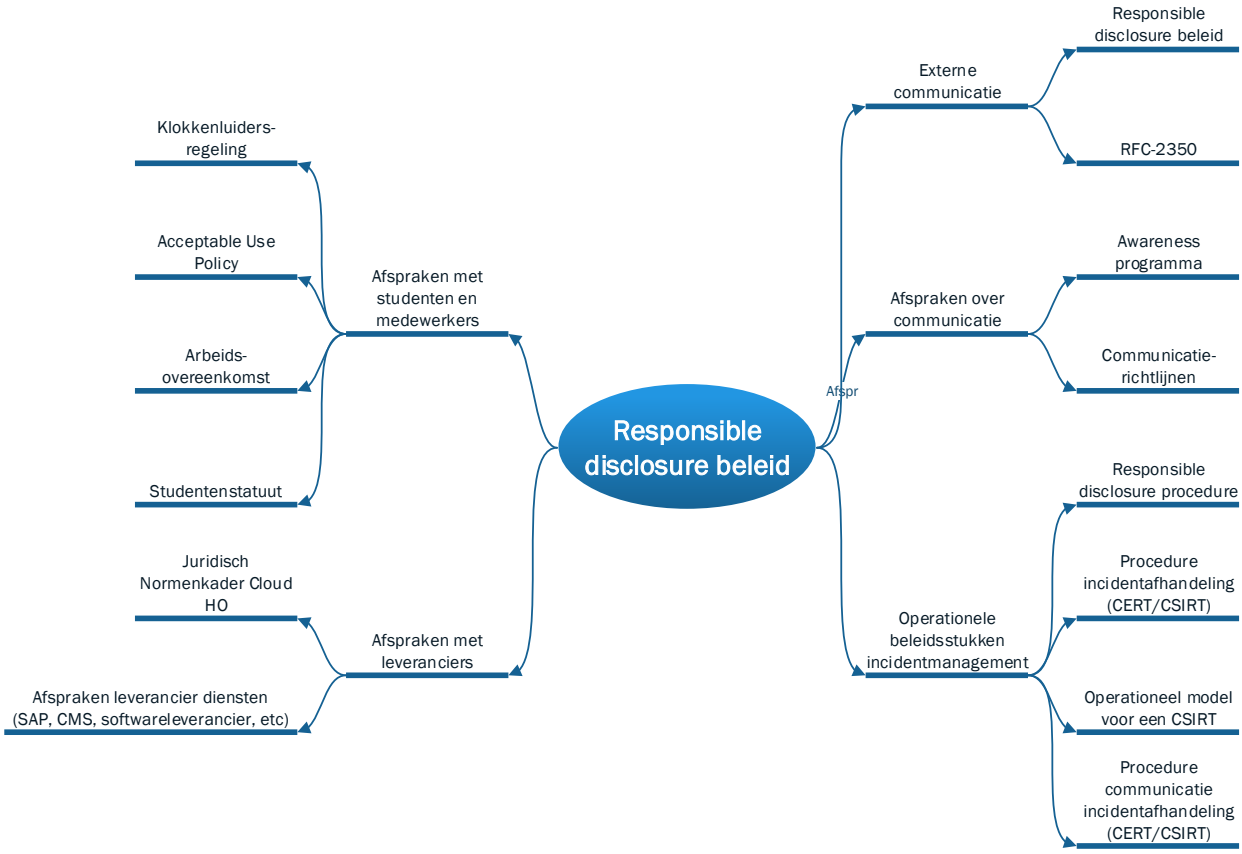
Een instelling heeft nooit alle kennis in huis. Responsible disclosure kan ingezet worden om gebruik te maken van kennis over kwetsbaarheden die buiten de organisatie aanwezig is. Door de mogelijkheid te bieden om op verantwoorde wijze een kwetsbaarheid te melden wordt het voor goedwillende beveiligingsonderzoekers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

2.6 Trend

Responsible disclosure wordt steeds meer branche breed in Nederland gehanteerd. Voorbeelden waarbij responsible disclosure branche breed wordt gestimuleerd zijn de Nederlandse rijksoverheid, de grote Nederlandse telecomproviders, de Nederlandse banken en de Dutch Hosting Provider Association.

3 Positionering

Responsible disclosure kan een grote invloed hebben op de bedrijfsvoering van een instelling. Om ervoor te zorgen alle betrokkenen op de juiste manier op de hoogte worden gesteld en mee kunnen werken aan een responsible disclosure melding moet responsible disclosure beleid aansluiten op bestaande beleidstukken, procedures en overeenkomsten. In figuur 1 is de positionering van het responsible disclosure beleid grafisch weergegeven.



Figuur 1: Samenhang beleidsdocumenten responsible disclosure

3.1 Intern

3.1.1 Operationele beleidsstukken voor incidentmanagement

Een responsible disclosure beleid heeft veel overeenkomsten met incidentmanagement. Voor een groot deel kunnen beide beleidstukken zelfs gelijk zijn. Het grootste verschil met een normale incidentprocedure zijn de extensieve communicatie met melder en de afhandeling van openbaring en beloning. Door de onderdelen schade indamming, beoordeling van de blootstelling en remediatie en herstel van het responsible disclosure beleid af te stemmen op het incidentmanagement wordt voorkomen dat er grote overlap tussen het beleid ontstaat.

3.1.2 Afspraken over communicatie

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

3.1.3 Klokkenluidersregeling

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

3.2 Extern

3.2.1 Afspraken met leveranciers

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

3.2.2 Afspraken met gebruikers

Een hoger onderwijsinstelling is verantwoordelijk voor het beheer van gevoelige informatie van studenten en medewerkers zoals salarisstroken, personeelsdossier, cijferlijsten en dossiers van de studentpsycholoog. Afspraken met de student en medewerkers over de omgang met deze informatie en de rechten en plichten van een student kunnen worden onder andere worden vastgelegd in Acceptable Use Policy (gebruiksreglement voor informatievoorzieningen voor werknemers en studenten), studentstatuut of arbeidsovereenkomst. Aangezien de melder van een kwetsbaarheid zichzelf mogelijk ook toegang verschaft tot informatie over studenten of medewerkers is het belangrijk om deze partijen te informeren over de eventuele impact van responsible disclosure. Daarnaast kan er voor worden gekozen om responsible disclosure terug te laten komen in deze documenten om discussie of een civiele zaak tussen student/medewerker en de melder te voorkomen.

3.2.3 Externe communicatie

Responsible disclosure is een middel om de drempel tot melden van een kwetsbaarheid te verlagen en spelregels vast te stellen voor het onderzoeken van kwetsbaarheden. De melder moet op de hoogte gesteld worden dat de instelling een responsible disclosure beleid hanteert. Door het responsible disclosure beleid vindbaar te maken door het beleid op de website door het publiceren. Daarnaast kan de responsible disclosure procedure opgenomen worden in de RFC-2350 waarin de verwachtingen van de Internet community voor het CSIRT is beschreven.

4 Wetgeving

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

4.1 Wetboek van Strafrecht

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

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

4.2 Vervolging

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

4.2.1 Civielrechtelijke vervolging

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

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

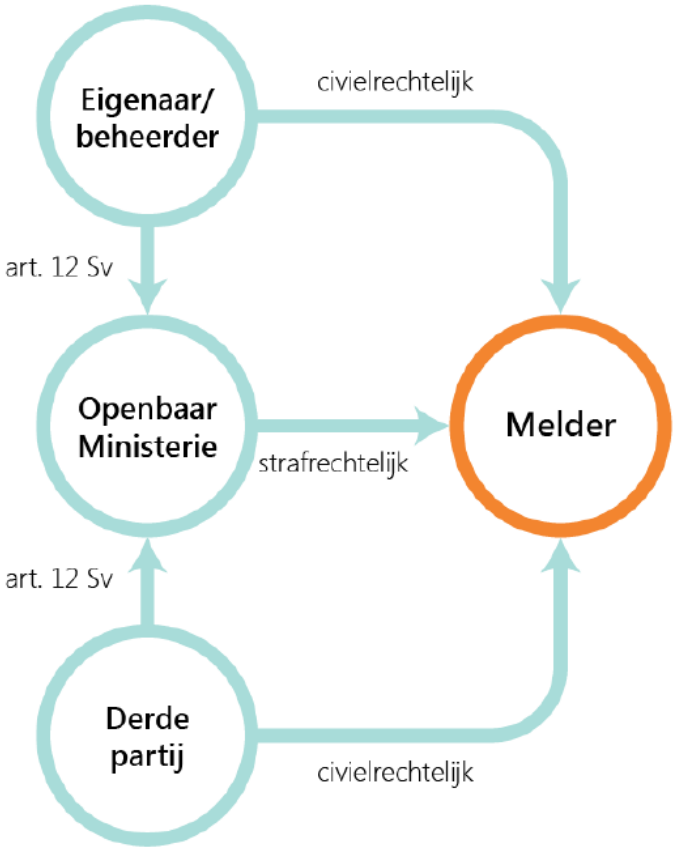
4.2.2 Strafrechtelijke vervolging

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

Verschil civiel- en strafrecht

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

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



Figuur 2: Verhouding vervolging melder

Het OM kan na onderzoek ook afzien van vervolging volgens het zogenoemde opportuniteitsbeginsel[1]. De officier van justitie zal de verdachte in dat geval niet voor de rechter brengen op grond van algemeen belang.

Als het Openbaar Ministerie beslist om niet te vervolgen dan kan een derde partij die rechtstreeks belanghebbende is, bijvoorbeeld de beheerder/eigenaar, een klant of een patiënt, op grond van artikel 12 Sr een klacht indienen met het verzoek aan het gerechtshof om alsnog over te gaan tot vervolging. Een melder kan dus zowel civiel- als strafrechtelijk worden vervolgd en beide vervolgingen kunnen los van elkaar worden gestart. Afzien van een civiele vervolging leidt dus niet direct tot afzien van een strafrechtelijke vervolging en vice versa.

4.3 Vrijheid van meningsuiting (Artikel 10 EVRM)

Om een zaak van zwaar maatschappelijk belang te onderzoeken kan het nodig zijn om de wet te

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

Belangrijk hierbij is wel dat er geen minder verstrekkende methodes voorhanden zijn. Als er mogelijkheden zijn om hetzelfde aan te tonen met minder gevolgen, moet dat worden nagestreefd.

Artikel 10 EVRM is bindend voor alle landen die lid zijn van de Raad van Europa en geldt dus voor Nederland.

Het komt voor dat ethische hackers hun melding doen via een journalist om hun anonimiteit te waarborgen. In Nederland heeft een journalist namelijk het recht om een bron geheim te houden. Dit

[1] Openbaar Ministerie (2013), *Begrippenlijst: Opportuniteitsbeginsel*. Geraadpleegd via http://www.om.nl/onderwerpen/begrippenlijst/?BgrIdt=16809

beschermingsrecht komt voort uit artikel 10 EVRM. In een uitspraak van de Hoge Raad[2] is bepaald dat journalisten hun bron niet hoeven prijs te geven tijdens een getuigenverhoor, tenzij het openbaren van de bron noodzakelijk is voor een democratische samenleving. Er zal dan tegenover het 'zéér zwaarwegende publieke belang' van persvrijheid een nog 'zwaarwegende belang' moeten zijn om het bekendmaken van de bron te rechtvaardigen.

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

In de aanwijzing schrijft de landelijke leiding van het Openbaar Ministerie: "Omdat het recht op bronbescherming niet absoluut is, kan sprake zijn van het toepassen van strafvorderlijke dwangmiddelen tegen een journalist onder bijzondere omstandigheden: als dit het enige denkbare effectieve middel is om een zeer ernstig delict op te sporen en te voorkomen. Het moet gaan om die misdrijven waarbij het leven, veiligheid of de gezondheid van mensen ernstig kunnen worden geschaad of in gevaar kunnen worden gebracht."[3].

Daarnaast biedt bronbescherming voor de melder geen vrijwaring voor vervolging of absolute garantie voor anonimiteit. Een melder kan ook via andere kanalen worden opgespoord, zoals te zien was bij de melding van een zwakheid in systeem van het Groene Hart Ziekenhuis.

De vermoedelijke hacker werd door de Nationale Recherche aangehouden na een onderzoek door het THCT (Team High Tech Crime)[4]. Dit onderzoek word geleid door het Landelijk Parket van het Openbaar Ministerie. Een publicatie via een journalist kon, in dit geval, niet voorkomen dat er in deze zaak een verdachte werd gearresteerd, doordat de vermoedelijke hacker via een andere wijze werd achterhaald.

4.4 Ontwikkelingen wetgeving

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

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

---

[2] Volkskrant (1996), *Hoge Raad gunt journalist bescherming van bronnen*. Geraadpleegd via http://www.volkskrant.nl/vk/nl/2844/Archief/archief/article/detail/426812/1996/05/11/Hoge-Raad-gunt-journalist-bescherming-vanbronnen.dhtml

[3] College van procureurs-generaal (2013), *Aanwijzing toepassing dwangmiddelen tegen journalisten*. Geraadpleegd via https://zoek.officielebekendmakingen.nl/stcrt-2012-3656.html

[4] Landelijke Parket Openbaar Ministerie (2013), *Verdachte aangehouden voor inbraak computer Groene Hart Ziekenhuis*. Geraadpleegd via http://www.om.nl/actueel/nieuws-persberichten/@159844/verdachte/

5 Standaarden

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

5.1 Leidraad responsible disclosure

Naar aanleiding van een motie van Tweede Kamerlid Hachchi (D66) tijdens het AO Cyber Security en Veiligheid van Overheidswebsites op 10 april 2012 heeft minister Opstelten van Veiligheid en Justitie toegezegd om te komen met een kader voor responsible disclosure. Dit kader is aangegeven in de ‘Leidraad om te komen tot een praktijk van Responsible Disclosure’. De leidraad richt zich zowel tot de organisatie die eigenaar/beheerder is van een informatiesysteem als tot de melder van een kwetsbaarheid. Om te komen tot de leidraad zijn onder andere welwillende hackers uit de community geraadpleegd[5] en zijn ook best practices zoals de policy van Markplaats.nl meegenomen.

Het NCSC (Nationaal Cyber Security Centrum) hanteert in haar leidraad de volgende definitie voor responsible disclosure: “Responsible disclosure binnen de ICT-wereld is het op een verantwoorde wijze en in gezamenlijkheid tussen melder en organisatie openbaar maken van ICT kwetsbaarheden op basis van een door organisaties hiervoor vastgesteld beleid voor responsible disclosure.” [6]

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

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

In de leidraad wordt uitgelegd hoe een melder zou kunnen handelen in het geval dat een eigenaar/beheerder geen vastgesteld beleid heeft voor responsible disclosure. De melder wordt in dat geval geacht om direct contact op te nemen met de eigenaar/beheerder. Geeft dit niet het gewenste effect dan kan een melder beslissen om een intermediair in te schakelen. In de leidraad wordt het NCSC aangewezen als intermediair en ook in het responsible disclosure beleid van het NCSC wordt op haar website aangegeven dat het NCSC bij het niet of niet goed reageren door een derde partij kan “optreden als intermediair”[7].

De leidraad heeft geen invloed op strafrechtelijke kaders. Het volgen van de richtlijnen garandeert de melder dus op geen enkele wijze dat hij is gevrijwaard van een strafrechtelijk procedure. Een civielrechtelijke procedure kan eventueel wel door een melder worden voorkomen door met de

---

[5] NCSC (2013), *Kamerbrief responsible disclosure*. Geraadpleegd via https://www.ncsc.nl/binaries/nl/actueel/nieuwsberichten/leidraad-responsible-disclosure/1/Kamerbrief%2BResponsible%2BDisclosure.pdf

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

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

eigenaar/beheerder overeen te komen dat er geen aangifte wordt gedaan of civielrechtelijke stappen worden ondernomen.

5.2 ISO standaarden

De Internationale Organisatie voor Standaardisatie (ISO) heeft twee standaarden uitgebracht over het openbaren van kwetsbaarheden en de afhandeling van meldingen van kwetsbaarheden. Beide standaarden zijn toegepast bij de inrichting van een responsible disclosure procedure voor het modelbeleid.

5.2.1 ISO 29147

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

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

5.2.2 ISO 30111

De NEN-ISO 3011 geeft richtlijnen voor de manier waarop mogelijk informatie over kwetsbaarheden verwerkt moet worden en hoe de kwetsbaarheid opgelost kan worden in een product of online dienst. De norm beschrijft drie richtlijnen:

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

6 Afstemming betrokken partijen

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

6.1 Ketenstructuur

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

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

6.2 Afstemming interne stakeholders

Het is van belang dat er afstemming met stakeholders plaatsvindt om het responsible disclosure proces zo adequaat mogelijk in te richten. Voor het vaststellen van beleid en procedure moeten er in ieder geval de volgende groepen worden geraadpleegd:

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

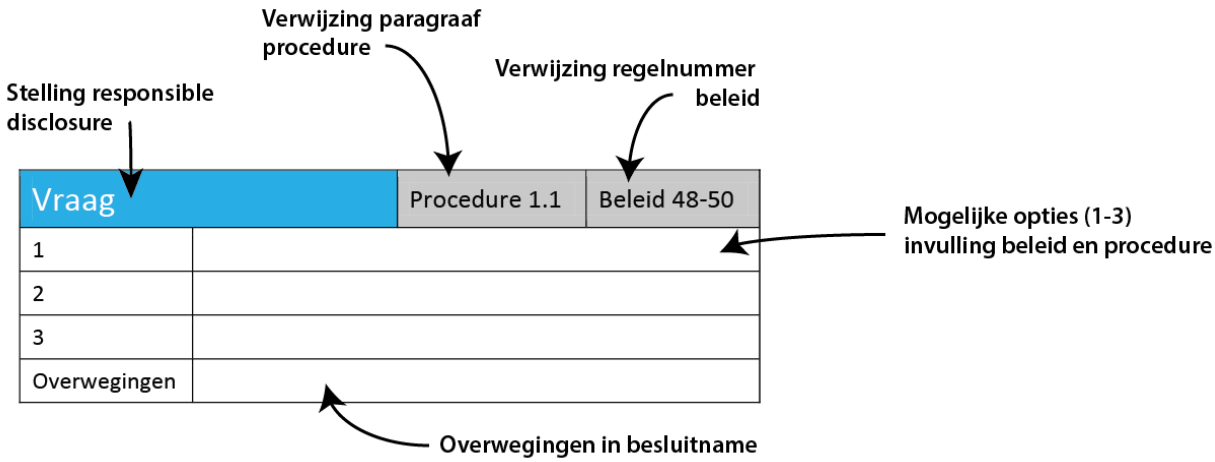
	communicatie naar de gebruikers, medewerkers, IT community en buitenwereld moet goed worden afgestemd.

7 Invulling responsible disclosure beleid

Bij de implementatie van responsible disclosure moet voor de organisatie worden bepaald welke exacte invulling voor het beleid en de procedure gewenst is. Om de afwegingen die moeten worden gemaakt concreet te maken zijn er een aantal stellingen geformuleerd. Aan de hand van het antwoord op de stellingen kunnen beleid en procedure worden aangepast.

Tijdens een onderzoek naar responsible disclosure binnen hoger onderwijsinstellingen is een enquête uitgezet onder SURFibo leden. Aan de hand van de enquête zijn de meest essentiële stellingen besproken. Een aantal antwoorden van respondenten op de enquête zijn meegenomen binnen deze paragraaf om bij eventuele moeilijke beslissingen houvast te bieden.

De stellingen worden als volgt toegelicht:



7.1 Beleggen verantwoordelijkheden

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

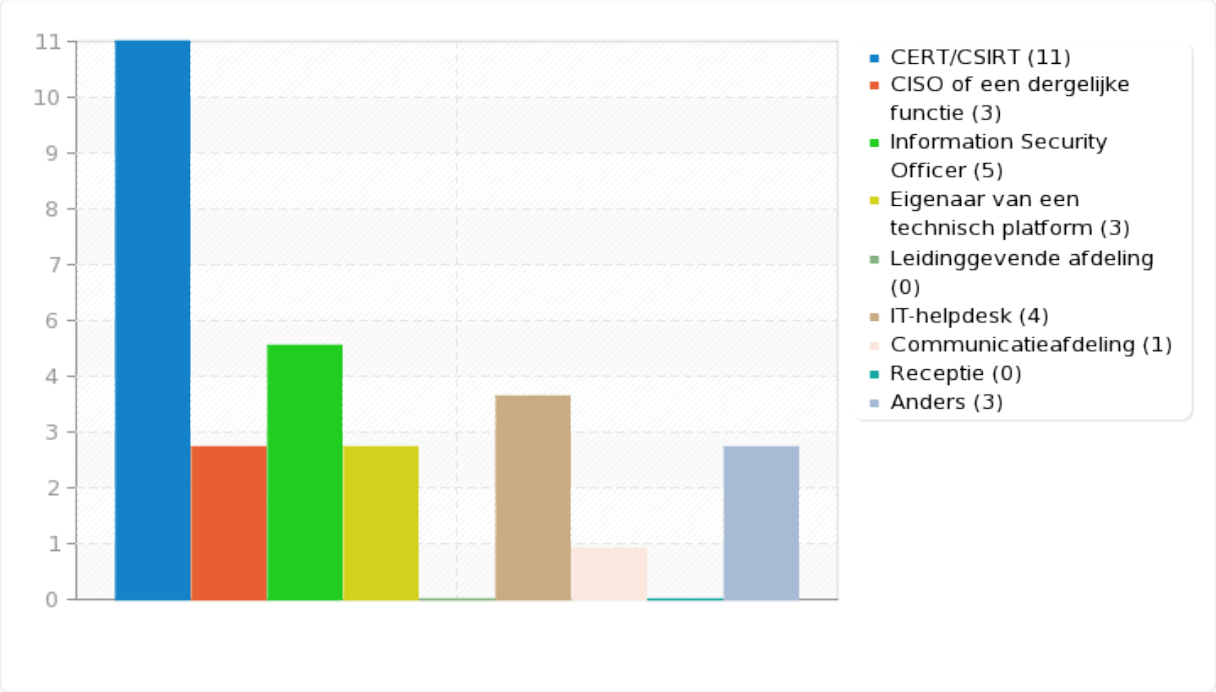
Een aantal verantwoordelijkheden moeten in ieder geval belegd worden om responsible disclosure tot een succes te maken:

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

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

Relevante uitkomst enquête

Op de vraag “Waar moet een melding van een kwetsbaarheid binnenkomen” antwoord het grootste deel van de ondervraagde dat een melding moet binnen komen bij het CERT of CSIRT. Uit de andere antwoorden blijkt dat meldingen bij voorkeur niet direct bij de operationele medewerker worden gedaan.



7.2 Scope responsible disclosure beleid

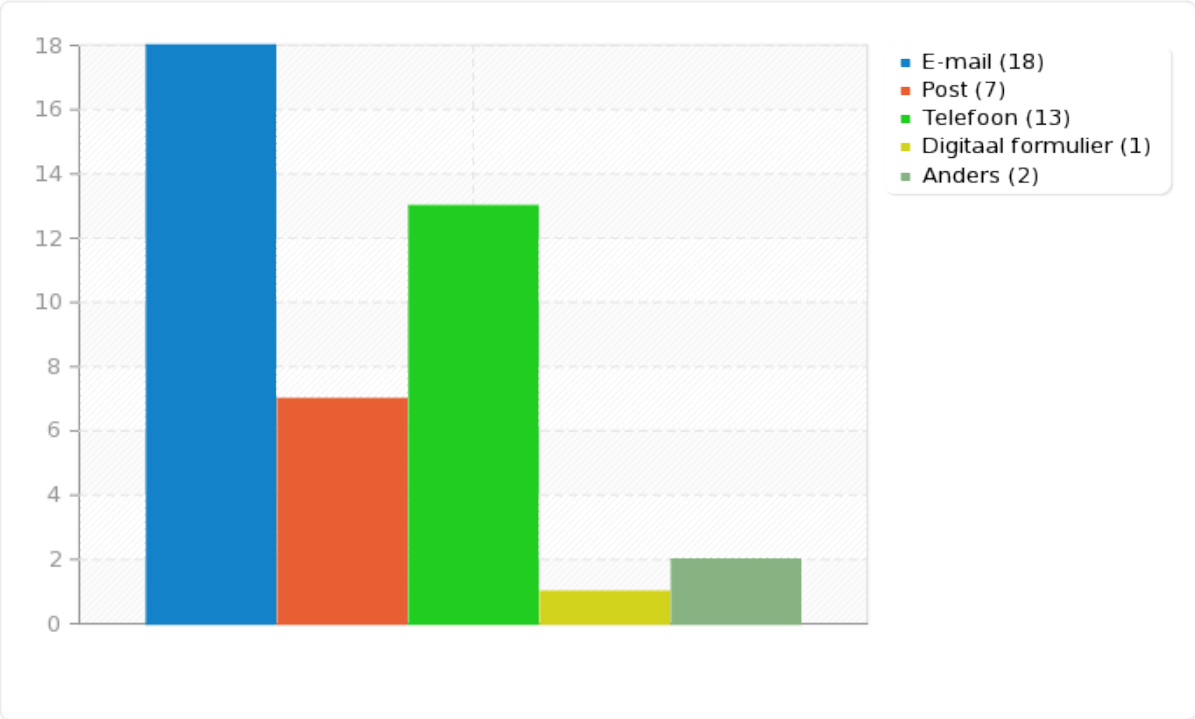
Op welke producten en diensten heeft het beleid betrekking?		Niet in model	Niet in model
1	Alle applicaties		
2	Alle applicaties en de gehele infrastructuur		
3	Alleen de webapplicaties		
Overwegingen	Wanneer alle applicaties en de infrastructuur worden meegenomen in de scope kan dit tot veel meldingen leiden. Bij beperkingen met bijvoorbeeld alleen de webapplicaties kunnen belangrijke bevindingen op bijvoorbeeld een offline applicatie verloren gaan.		

7.3 Manier van melden

Op welke wijze moet er worden gemeld?		Procedure 4.2B	Beleid 16-18
1	E-mail (al dan niet versleuteld)		
2	Post		
3	Digitaal formulier (al dan niet via SSH)		
4	Telefoon		
Overwegingen	Bij het melden via een digitaal formulier kan bij de melder worden afgedwongen dat bepaalde zaken worden vermeld zoals contactgegevens. De drempel kan hierdoor hoger zijn om een melding daadwerkelijk te doen. Dit is bij het melden via e-mail en telefoon minder aan de orde. Wanneer versleuteling bij e-mail noodzakelijk wordt geacht wordt deze drempel voor sommige melders wel weer hoger. Meldingen met betrekking tot kwetsbaarheden in systemen met vertrouwelijke informatie moeten vertrouwelijk behandeld worden. Vaak is versleuteling van de informatie-uitwisseling volgens het informatiebeveiligingsbeleid dan noodzakelijk.		

Relevante uitkomst enquête

De vraag die gesteld is, luidt: “Als een melder een beveiligingslek in uw (web)applicatie vindt, hoe mag hij/zij dit aan uw organisatie melden?”. Uit de antwoorden blijkt dat e-mail en telefoon het meest gewenst is. Iets minder van de helft van de ondervraagden vindt post ook een goed middel om meldingen van kwetsbaarheden te verzenden.

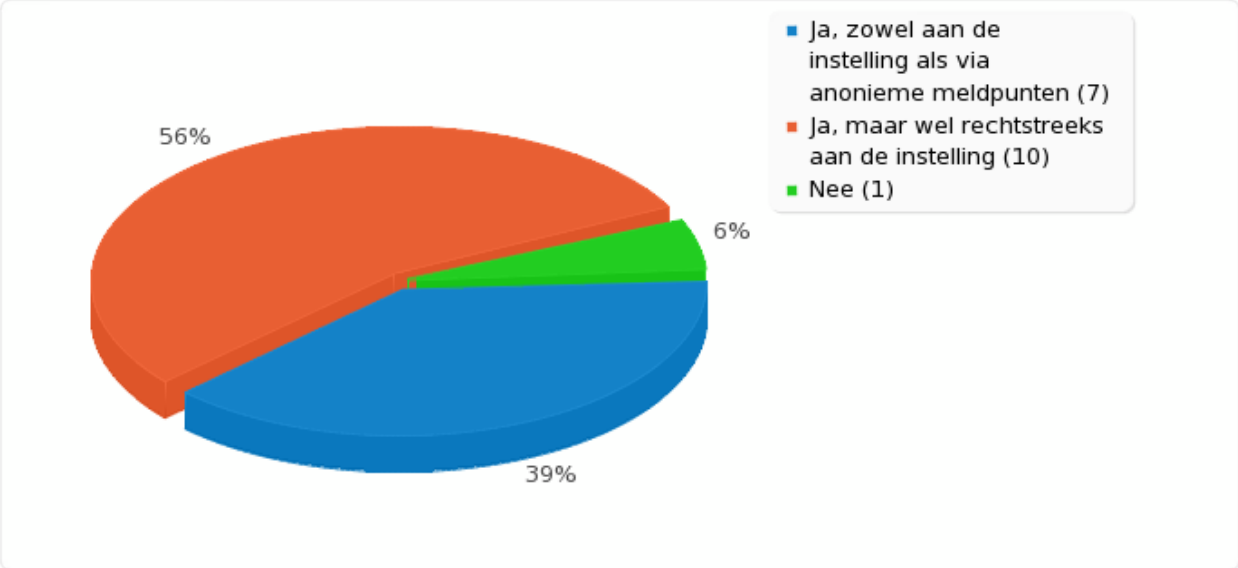


Mag er anoniem gemeld worden?	Procedure Par. 4.2C	Beleid Nr. 36-38
1	De melding kan zowel anoniem, onder een pseudoniem of via een tussen-/vertrouwenpersoon gedaan worden.	
2	Er worden geen meldingen aangenomen die onder een pseudoniem, anoniem of via een tussen-/vertrouwenspersoon worden gedaan.	
3	Meldingen kunnen zowel anoniem als onder een pseudoniem gemeld worden. Meldingen via een tussen-/vertrouwenspersoon (zoals meldpunten als hackmeldpunt.nl zijn niet toegestaan en worden niet behandeld).	
4	Meldingen worden alleen aangenomen wanneer contact mogelijk blijft dus onder een pseudoniem of geheel bekend.	
Overweging	Anoniem melden kan communicatie verhinderen en daarmee afstemming, beloning en eventuele informatie uitwisseling in het geval van onduidelijkheden onmogelijk maken. Daarnaast verhindert of bemoeilijkt het de opsporingsmogelijkheden bij het	

	mogelijk overtreden van de spelregels van het responsible disclosure beleid. Tot slot geeft een anonieme melding mogelijk geen goed beeld van de persoon die achter de melding zit en daarmee is mogelijk ook de intentie van de melder minder zichtbaar. Een voordeel van anoniem melden is dat de drempel voor de melder laag is. Hiermee wordt voorkomen dat een melder die liever anoniem wil blijven besluit om naar de pers te stappen of kiest voor full disclosure.

Relevante uitkomst enquête

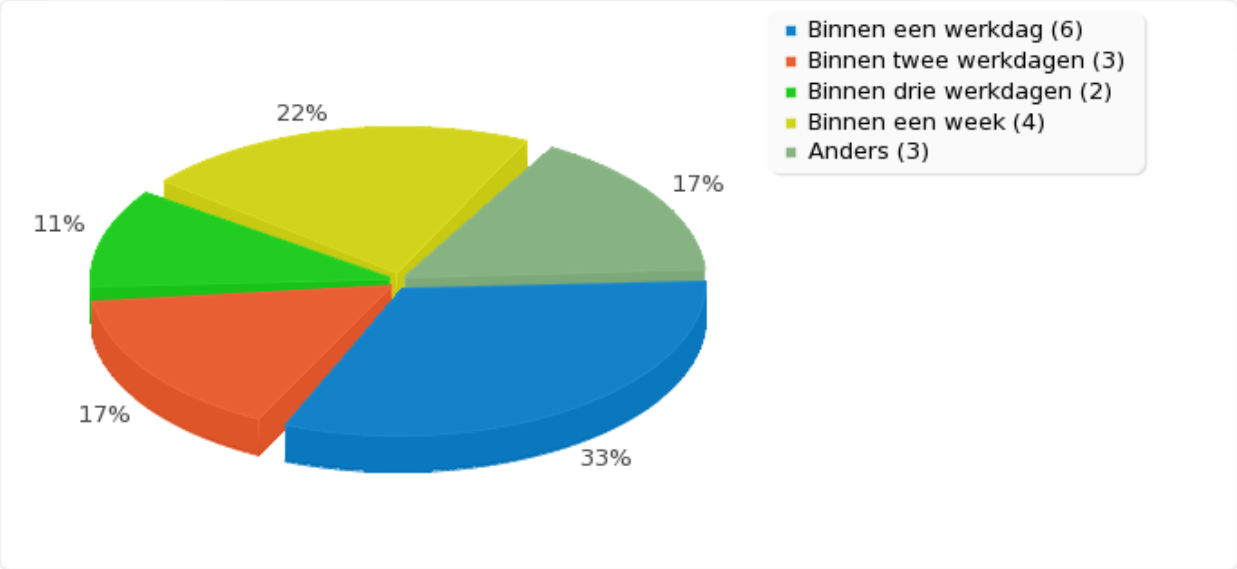
Een overgroot deel van de ondervraagde vindt dat een melder van een kwetsbaarheid zijn melding ook anoniem mag doen. Meer dan de helft daarvan vindt dat deze melder dan wel direct contact moet hebben met de instelling en de melding niet via een anoniem meldpunt doet.



Hoe snel moet de instelling een bevestiging van ontvangst van de melding sturen naar de melder?	Procedure 4.4	Beleid 28-29
1	Binnen een werkdag	
2	Binnen twee werkdagen	
3	Binnen drie werkdagen	
4	Binnen een week	
Overweging	Een snelle reactie naar de melder geeft de indruk dat de melding serieus genomen wordt. Door als instelling de verplichting te stellen dat er snel een reactie gestuurd moet worden naar de melder kan een snellere verwerking van meldingen gestimuleerd worden. Doordat de melder het gevoel heeft dat hij serieus genomen wordt, kan voorkomen worden dat de melder alsnog naar de pers wordt stapt of gebruik maakt van full disclosure.	

Relevante uitkomst enquête

Op de vraag “Hoe snel moet de instelling een bevestiging van ontvangst van de melding sturen naar de melder?” antwoord meer dan de driekwart van de respondenten dat de instelling binnen drie werkdagen een bevestiging van melding moet sturen. De helft van de respondenten vindt dat een reactie binnen twee werkdagen gegeven moet worden.

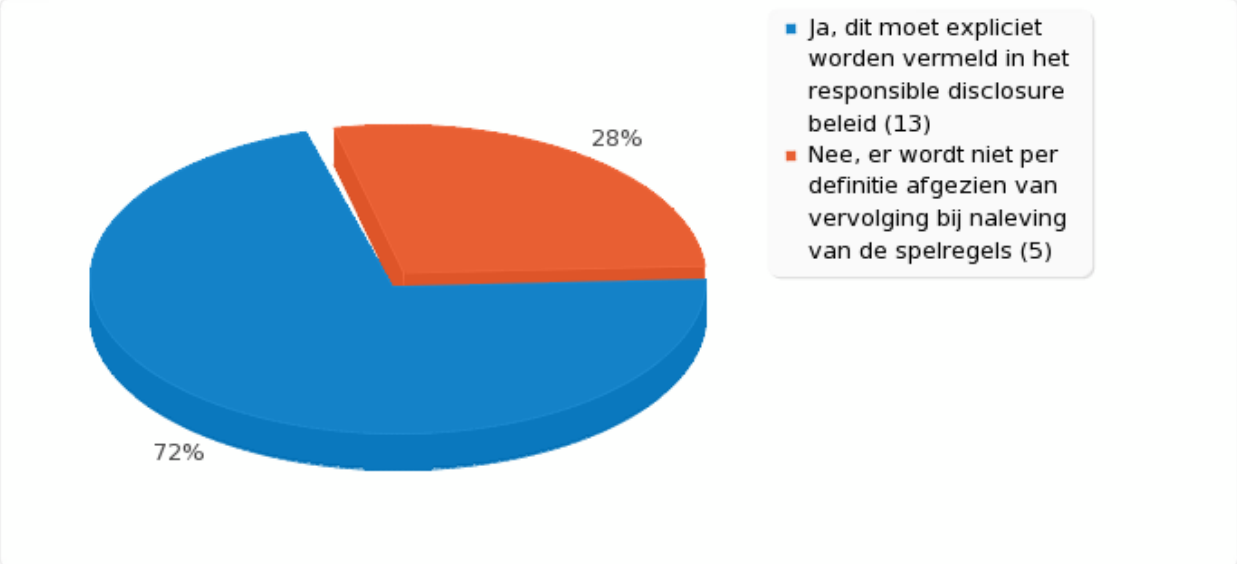


7.4 Afzien van vervolging

Wanneer een melder de spelregels uit het responsible disclosurebeleid heeft nageleefd, moet er dan worden afgezien van vervolging?	Procedure 4.1	Beleid 19-20 / 22-23
1	Ja	
2	Nee	
Overwegingen	Wanneer er expliciet in het beleid wordt vermeld dat er wordt afgezien van vervolging kan dit de melder gerust stellen en is de kans groter dat een melding wordt gedaan. Echter is het wel van belang om duidelijk te vermelden dat het altijd mogelijk is dat er voor de instelling wettelijke verplichtingen zijn om juridische stappen te nemen. Als het niet expliciet wordt vermeld verminderd dit mogelijk risico tot verplichte juridische stappen en het in strijd zijn met het responsible disclosure beleid. Uitgangspunt binnen de organisatie dient bij het volgen van de spelregels wel het afzien van vervolging te zijn.		

Relevante uitkomst enquête

Het grootste gedeelte van de respondenten vindt dat er van civielrechtelijke vervolging door de instelling moet worden afgezien als de melder zich aan de spelregels uit het responsible disclosure beleid heeft gehouden.



7.5 Meldingen met impact op derden

Hoe wordt er gehandeld in het geval dat er melding wordt gedaan over uw systeem die ook impact kan hebben op een systeem van derden, waarbij de derde partij geen responsible disclosure beleid hanteert?	Procedure 4.5	Beleid 19-20 / 22-23

1	Er wordt overlegd met de melder wat er moet gebeuren
2	De instelling bemiddelt tussen de melder en de mogelijk getroffen partij
3	De melding moet door de instelling worden doorgegeven aan de mogelijk getroffen partij
Overwegingen	Wanneer de melder wordt betrokken bij het besluit voor vervolgstappen blijft de verantwoordelijkheid bij de melder en is aan hem/haar de keus om contact op te nemen met de derde partij. Bemiddeling tussen instelling en mogelijk getroffen partij draagt bij een maatschappelijke verantwoording aan de melder dat het eventuele probleem wordt opgelost en aan de derde partij dat het probleem, wat zij mogelijk heeft, wordt gemeld. Indien de melding wordt doorgegeven aan de mogelijk getroffen partij kan het probleem snel worden opgelost. Echter moet nog wel de keuze gemaakt worden om de melder anoniem te houden.

Hoe wordt er gehandeld in het geval dat de melder een kwetsbaarheid vindt in een systeem van een derde partij (bijv. Blackboard) en dit meldt aan uw instelling. Het responsible disclosure proces wordt beëindigd omdat de melding niet van toepassing is op de systemen van de instelling?	Procedure 4.5	Beleid 19-20 / 22-23

1	Er wordt overlegd met de melder wat er moet gebeuren
2	De instelling bemiddelt tussen de melder en de mogelijk getroffen partij
3	De melding moet door de instelling worden doorgegeven aan de derde partij
Overwegingen	Wanneer de melder wordt betrokken bij het besluit voor vervolgstappen blijft de verantwoordelijkheid bij de melder en is aan hem/haar de keus om contact op te nemen met de derde partij. Bemiddeling tussen instelling en derde partij draagt bij een maatschappelijke verantwoording aan de melder dat het eventuele probleem wordt opgelost en aan de derde partij dat het probleem, wat zij mogelijk heeft, wordt gemeld. Indien de melding wordt doorgegeven aan de derde partij kan het probleem snel worden opgelost. Echter moet nog wel de keuze gemaakt worden om de melder anoniem te houden.

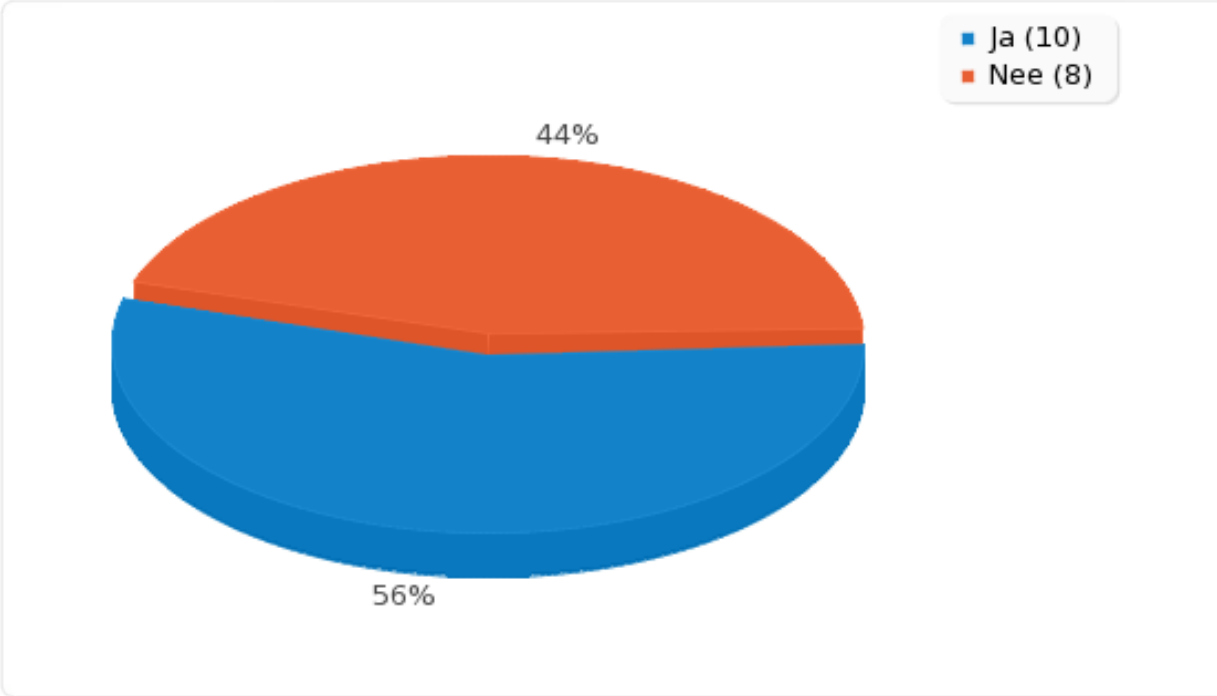
7.6 Opleggen beperkingen

Hoe ver mag de melder gaan in zijn onderzoek?		Niet in model	Beleid 19-20 / 22-23
1	Expliciet vermelden wat wel en niet is toegestaan		
2	Duidelijke lijn aangeven waaraan de melder zich moet houden		
3	Geen richtlijn geven		
Overwegingen	Wanneer expliciete regels worden vermeld wat wel en niet mag kan dit tegenwerken voor de melder. De melder kan zich beperkt voelen en wanneer de melder een stap heeft genomen die niet toegestaan is volgens de regels maar hier geen schade mee heeft aangericht, kan de melder besluiten geen melding te doen in verband met eventuele vervolging. Echter creëert dit wel duidelijke, meetbare regels en draagt bij aan verwachtingsmanagement. Duidelijkheid kan ook worden geboden door een lijn aan te geven waaraan de melder zich moet houden. Hierin worden geen strenge regels opgelegd maar bijvoorbeeld wel van de melder gevraagd geen data te wijzigen of verwijderen en kunnen er enkele beperkingen worden opgelegd. Bij het geheel vrijlaten kan misverstand ontstaan over wat billijk is. Echter kan de melder wel alle kwetsbaarheden aantonen en melden.		

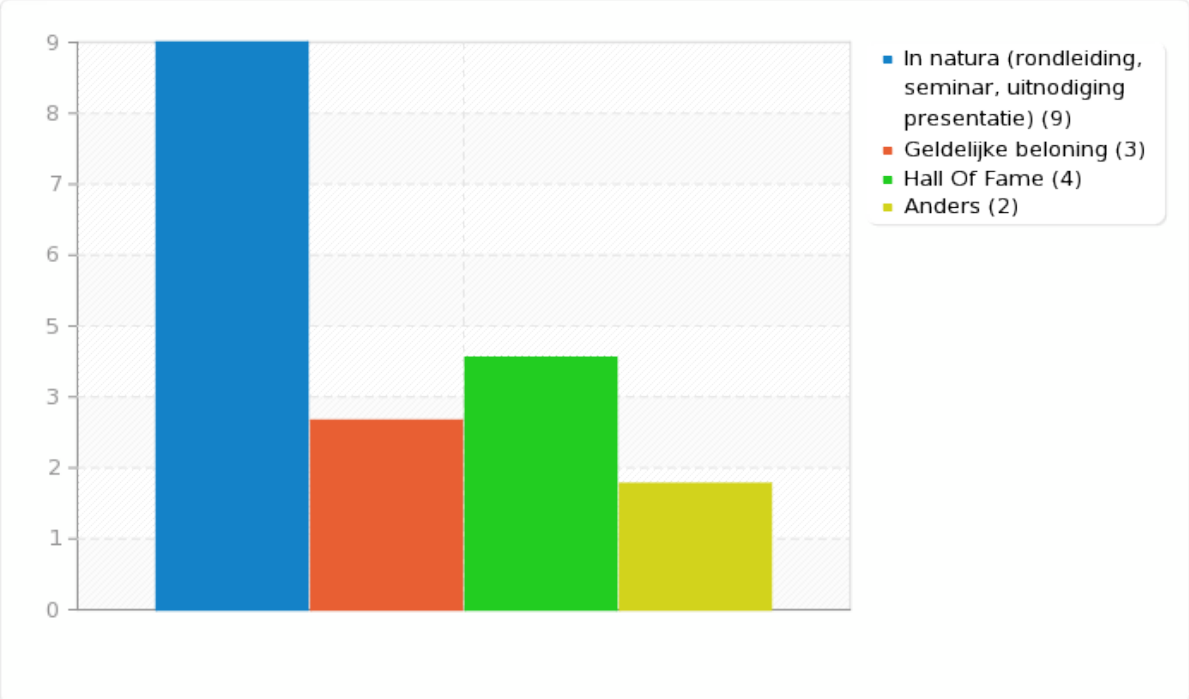
7.7 Belonen melder

Moet de melder beloond worden?	Procedure 4.7	Beleid 41-43
1	Ja door middel van een geldelijke beloning of in de vorm van waardebonnen	
2	Ja, in natura zoals een t-shirt, rondleiding, seminar of een uitnodiging voor een presentatie	
3	Ja, door een plek op de Hall of Fame van de instelling	
4	Nee	
Overwegingen	Er moet overwegen worden wat de eventuele financiële mogelijkheden zijn voor de instelling. Bij het uitkeren van een geldelijke beloning is de kans op melders die handelen vanuit financieel oogpunt groter. Dit betekent meer meldingen wat ook meer geld en tijd kost voor de instelling. De kans op nuttige meldingen van hoge kwaliteit wordt echter wel vergroot. Ethische melders handelen echter vaak vanuit maatschappelijk belang of voor het opbouwen van een goede reputatie. Hieruit zou geconcludeerd kunnen worden dat het geven van een niet geldelijke beloning de kans op alleen ethische melder wordt vergroot.	

Relevante uitkomsten enquête
Iets meer dan de helft van de respondenten vindt dat een melder beloont moet worden voor de melding van een kwetsbaarheid.



Op de vraag hoe de melder mogelijk beloond moeten worden voor zijn melding lopen de opvattingen uiteen. De helft vindt dat de beloning in natura moet worden uitgekeerd. Een geldelijke beloning lijkt geen populaire optie.

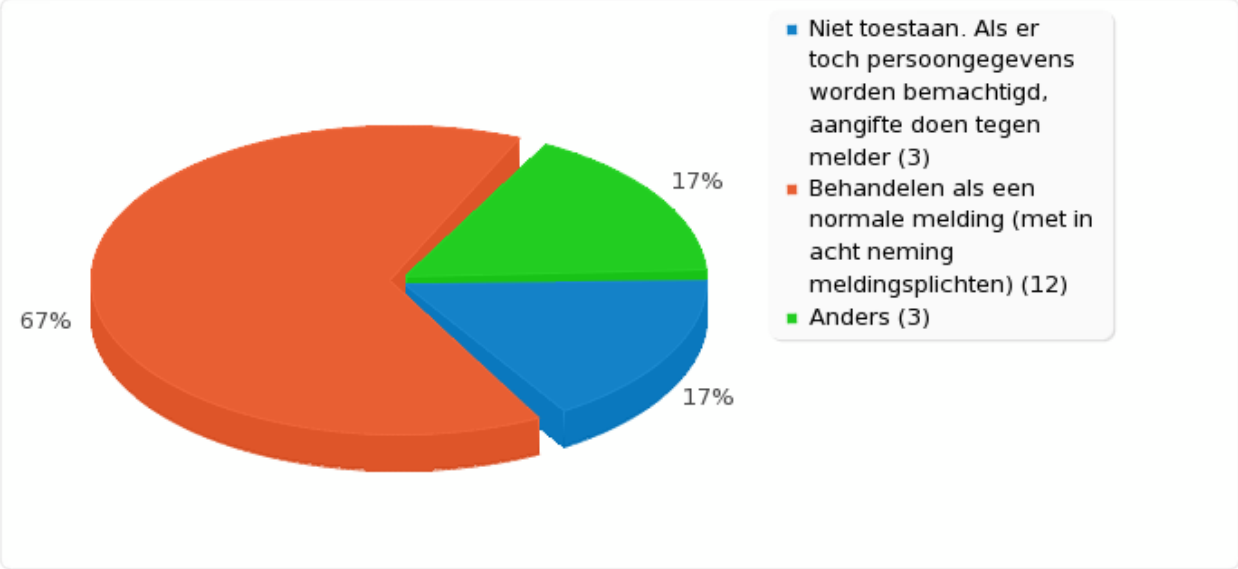


7.7.1 Persoonsgegevens

Hoe moet er worden omgegaan met meldingen van kwetsbaarheden waarbij persoonsgegevens zijn verkregen?	Procedure 4.7	Beleid 41-43
1	Dit te allen tijde niet toestaan. Als er toch persoonsgegevens worden bemachtigd wordt er aangifte gedaan tegen de melder.	
2	De melding behandelen als een normale melding, met in achtneming van wettelijke meldingsplichten.	
3	Per geval bekijken, als er bijvoorbeeld geen sprake is van braak maar slecht geïmplementeerde software kan dit niet te wijten zijn aan de melder.	
Overwegingen	Wanneer expliciet wordt vermeld dat het niet is toegestaan als er persoonsgegevens worden verkregen kan dit een melder afhouden om een melding te doen als de melder niet opzettelijk persoonsgegevens heeft verkregen bij het vinden van een lek.	

Relevante uitkomst enquête

Meer dan de helft van de respondenten vindt dat er geen onderscheidt moet worden gemaakt voor meldingen waarbij persoonsgegevens zijn verkregen. De meerderheid vindt dat de melding als een normale melding behandeld moet worden (met inachtneming van de meldingsplichten).

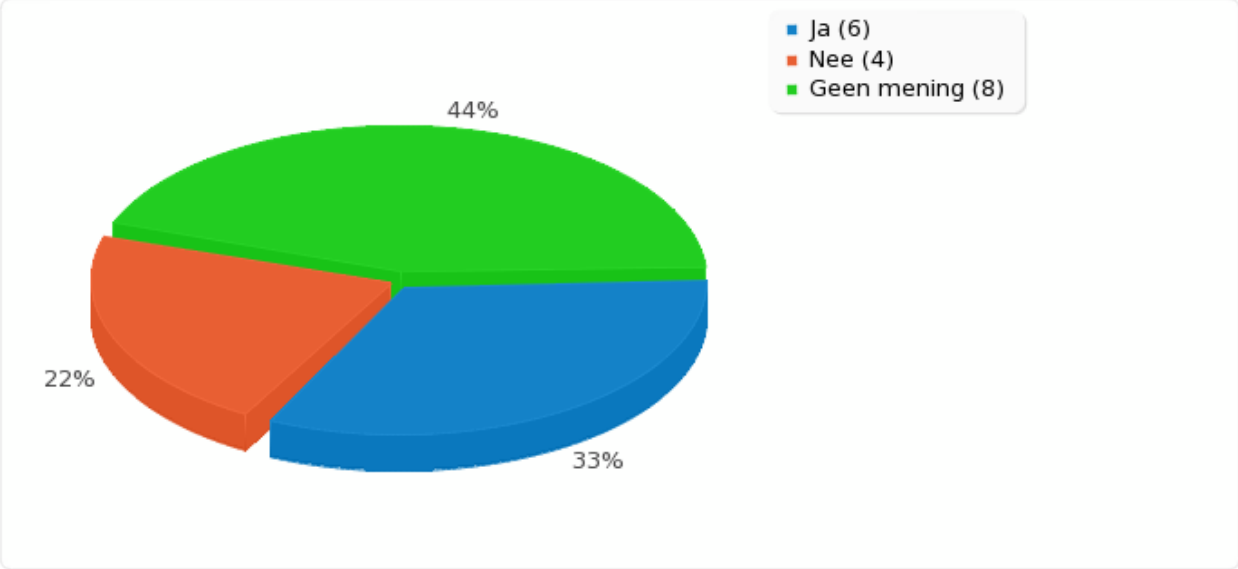


7.7.2 Afspraken met derden

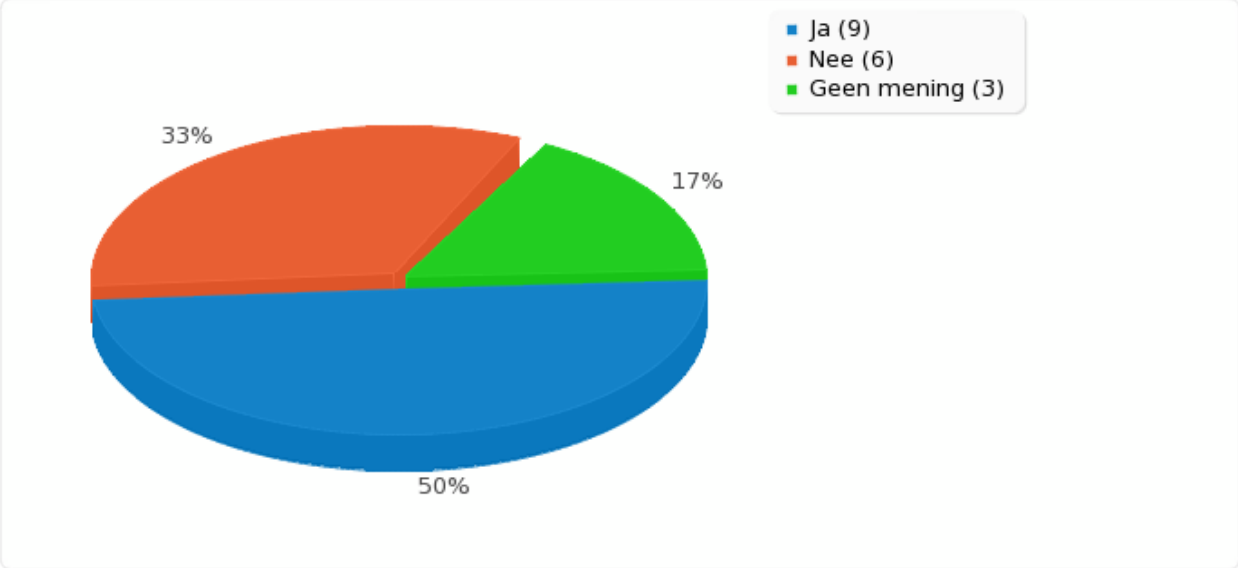
Moeten er afspraken gemaakt worden met leveranciers en/of gebruikers met betrekking tot responsible disclosure?	Procedure 4.7	Beleid 41-43
1	Ja met zowel gebruikers als leveranciers	
2	Alleen met leveranciers	
3	Alleen met gebruikers	
4	Nee	
Overwegingen	Ondersteuning van leveranciers kan nodig zijn bij het oplossen van een kwetsbaarheid. Daarnaast kan een kwetsbaarheid worden gemeld van een systeem van een leverancier. Het is daarom nuttig om van te voren afspraken te maken met leveranciers over bijvoorbeeld oplostijd van kwetsbaarheden. Melders kunnen tijdens het doen van onderzoek naar de kwetsbaarheid mogelijk toegang krijgen tot gegevens van gebruikers van de systemen zoals studenten en medewerkers. Het kan daarom nuttig zijn om afspraken te maken of in ieder geval de gebruikers op hoogte te stellen van het responsible disclosure beleid wat wordt gehanteerd.	

Relevante uitkomst enquête

Op de vraag of er vooraf afspraken gemaakt worden met de gebruikers over het responsible disclosure beleid (bijvoorbeeld in een Acceptable Use Policy) is geen overduidelijke . Een groot deel van de respondenten heeft geen mening over dit onderwerp.



Op de vraag of er vooraf afspraken gemaakt worden met leveranciers (hosting-, software, hardwareprovider) over het responsible disclosure beleid (bijvoorbeeld in de bewerkersovereenkomsten/contracten) is de helft van de respondenten van mening dat het goed is om hierover vooraf afspraken te maken.



8 Stappenplan implementatie responsible disclosure

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

1. **Vaststellen gereedheid instelling**
   Responsible disclosure is alleen succesvol als een instelling adequaat kan reageren op de melding van een kwetsbaarheid. Het ontbreken van een IT-incidentprocedure of ontbreken van mandaat voor het afsluiten van producten of diensten kunnen tekenen zijn dat een instelling nog niet klaar is voor responsible disclosure. Als een instelling de meldingen niet adequaat kan oppakken, kan dit betekenen dat een melder er voor kiest om de kwetsbaarheid alsnog kenbaar te maken via de media of full disclosure.
2. **Bepalen beslissingspunten**
   De invulling van een responsible disclosure beleid kan invloed hebben op het imago van de instelling. Aan de hand van hoofdstuk 7 van dit document kan een instelling de belangrijkste beslissingspunten, zoals scope, toegestane aanvalstechnieken en beloning melder.
3. **Overeenstemming bereiken met betrokkenen (leveranciers, studenten, legal, communicatie, etc.)**
   Het invoeren van een responsible disclosure beleid heeft invloed op de organisatie, degenen waarop de gegevens betrekking heeft en de betrokken leveranciers van diensten, hardware en software. Het is goed om de invoering van responsible disclosure, vanwege de eventuele impact, met deze partijen afgestemd worden.
4. **Opstellen responsible disclosure beleid en procedure**
   De instelling kan aan de hand van het “model responsible disclosure beleid en procedure voor het hoger onderwijs” een beleid en procedure opstellen.
5. **Voorleggen aan bestuur van de instelling**
   Responsible disclosure kan van invloed zijn op de organisatie van een instelling. Daarnaast is het belangrijk dat er mandaat wordt gegeven aan degene die is belast met de uitvoering van responsible disclosure om adequaat handelen te stimuleren. In bijlage A staat een voorbeeldbrief die gebruikt kan worden om responsible disclosure voor te leggen aan het bestuur van de instelling.
6. **Intern communiceren beleid en procedure**
   Omdat er bij responsible disclosure verschillende interne partijen betrokken kunnen zijn, zoals de IT afdeling, juridische afdeling en communicatie, moet duidelijk worden gemaakt welke verantwoordelijkheden zijn belegd en hoe er gehandeld dient te worden. Het benoemen van responsible disclosure tijdens een awareness training voor personeel kan nuttig zijn aangezien men meer bewust wordt van informatiebeveiliging en mogelijk kwetsbaarheden sneller herkent.
7. **Oefenmelding sturen**
   Met behulp van een oefenmelding kunnen aspecten zoals mandaat, tijdige afhandeling, communicatie en de samenwerking tussen de verschillende actoren worden gemeten.
8. **Evalueren**
   Aan de hand van de resultaten van de oefenmelding kunnen er eventueel aanpassingen worden gemaakt in het beleid en de procedure.
9. **Publiceren responsible disclosure beleid**
   Het responsible disclosure beleid moet duidelijk zichtbaar zijn voor melders. Hierbij kan gedacht worden aan een extra link op de contactpagina of een verwijzing op de security pagina van een website.

9 Versiebeheer, revisies

- 9 juli 2014 v 1.0 David van Es en Milla Cuperus
  Gewijzigd: Aanvullingen Alf Moens en Leo van Koppen
- 4 juli 2014 v 1.0 David van Es en Milla Cuperus
- 26 juni 2014 v 0.9 David van Es en Milla Cuperus

Bijlage A: Template aanbiedingsbrief

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

Wat is een responsible disclosure beleid?

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

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

Waarom een responsible disclosure beleid?

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

Eind 2012 heeft de minister van Veiligheid en Justitie ‘een leidraad om te komen tot een praktijk van Responsible Disclosure' opgesteld. Deze leidraad geeft richtlijnen voor het vaststellen van een beleid voor het op verantwoordde wijze openbaar maken van ICT-kwetsbaarheden. Het ministerie van Veiligheid en Justitie geeft aan dat responsible disclosure primair een aangelegenheid is tussen de melder en de betrokken organisatie. Het Openbaar Ministerie heeft daarnaast een intern beleidsstuk gepubliceerd dat in lijn is met de leidraad Responsible Disclosure. Er is geen wetgeving die direct voorziet in responsible disclosure. Organisatie worden dus geacht zelf beleid op te stellen ten aanzien van responsible disclosure. Dit voorstel voorziet in de implementatie van een dergelijk beleid.

Een korte samenvatting van de procedure die onderdeel is van het responsible disclosure beleid:

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

Naast de eerder genoemde argumenten voor de implementatie van een responsible disclosure beleid voor <<Instelling>>, kan het volgende worden overwogen :

Verlagen drempel melder
Een hoger onderwijsinstelling kan de drempel tot melden van kwetsbaarheden voor haar doelgroep verlagen. Hoger onderwijsinstellingen en onderzoeksinstellingen komen veel in aanraking met onderzoekers en ICT-kundige studenten. Het is aannemelijk dat onderzoekers en studenten een ICT-kwetsbaarheid herkennen en deze verantwoord willen melden zonder juridische complicaties.

Transparantie
Een transparante houding van hoger onderwijs- en onderzoeksinstellingen is in lijn met hun maatschappelijke rol. Door publicatie van een responsible disclosure beleid geven hoger onderwijs- en onderzoeksinstellingen aan welk standpunt zij innemen in deze kwestie.

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