Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2014–2015

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 342

BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 18 december 2014

Op 3 januari 2013 heb ik de «Leidraad om te komen tot een praktijk van responsible disclosure» aan uw Kamer doen toekomen (Kamerstuk 26 643, nr. 264). Deze leidraad biedt een kader om te komen tot een praktijk van «responsible disclosure». Private organisaties en overheden kunnen de leidraad gebruiken bij het vaststellen van een beleid voor het op verantwoorde wijze openbaar maken van ICT-kwetsbaarheden in informatiesystemen en softwareproducten die door goedwillende melders of hackers worden ontdekt en gemeld.
Bij de aanbieding van de leidraad heb ik toegezegd om: 1) als coördinerend bewindspersoon voor cybersecurity in gesprek te gaan met mijn collega's om het toepassen van responsible disclosure binnen de Rijksdienst te bevorderen, 2) het gebruik van de leidraad in het algemeen te stimuleren, 3) met het Openbaar Ministerie in gesprek te gaan over meldingen van kwetsbaarheden in informatiesystemen die conform een beleid voor responsible disclosure worden gedaan. Tot slot heb ik: 4) tijdens de bespreking van de leidraad in het AO Cybersecurity d.d. 29 mei 2013 uw Kamer tevens toegezegd u na 2 jaar te informeren over de geboekte voortgang inzake responsible disclosure en de resultaten jaarlijks te betrekken in de reguliere rapportages (Kamerstuk 26 643, nr. 286).

1) Gebruik binnen de Rijkdienst

Sinds de publicatie van de leidraad is de praktijk van responsible disclosure door het Nationaal Cyber Security Centrum (NCSC) actief gestimuleerd. Deze handschoen is door een groot aantal partijen binnen de rijksoverheid opgepakt. Voor de websites van de rijksoverheid is een beleid voor responsible disclosure ingesteld. Het Ministerie voor Wonen en Rijksdienst en de Belastingdienst hebben loketten ingericht om melders die een kwetsbaarheid willen melden hierbij te faciliteren en tot een snelle oplossing van kwetsbaarheden te komen.

kst-26643-342
ISSN 0921 - 7371
's-Gravenhage 2014

2) Stimuleren van het gebruik van de leidraad en private initiatieven

Aan private zijde zijn door zeer veel en uiteenlopende partijen initiatieven op het vlak van responsible disclosure ontplooid. Reeds voorafgaand aan de publicatie van de leidraad is door de Nederlandse telecombedrijven en binnen brancheorganisatie Nederland ICT intensief samengewerkt, hetgeen heeft geresulteerd in staand responsible disclosure-beleid bij de grootste Nederlandse telecombedrijven. Tijdens de NCSC One Conference in 2014 hebben het NCSC en diverse telecombedrijven daarbij actief ervaringen uitgewisseld met de bredere ICT-community. Ook de bancaire sector heeft een beleid voor responsible disclosure opgesteld en breed ingevoerd. Daarnaast is door een grote verscheidenheid aan individuele (binnen en buiten de vitale sectoren) en samenwerkende partijen gewerkt aan het opstellen van een eigen beleid voor responsible disclosure. Zo is bijvoorbeeld door het Verbond van Verzekeraars en enkele grote Nederlandse verzekeraars gewerkt aan het introduceren van responsible disclosure en het ontwikkelen van een handleiding. Tot slot heeft ook de Dutch Hosting Providers Associatie (DHPA) een document opgesteld ten einde klanten van hostingdiensten op dit vlak te faciliteren.
Vanuit de bredere ICT-community zijn diverse initiatieven ontplooid op het gebied van responsible disclosure. Daarbij zijn websites gelanceerd en discussiesessies georganiseerd om responsible disclosure te bevorderen.

3) Openbaar Ministerie

Het Openbaar Ministerie heeft op 18 maart 2013 per brief de parketten geïnformeerd over de gepubliceerde leidraad en de wijze waarop omgegaan kan worden met responsible disclosure-meldingen. Vertrekpunt hierbij is dat proportioneel en subsidiair gehandeld dient te worden zoals ook in de leidraad is omschreven. In de brief d.d. 3 januari 2013 is reeds aangegeven dat organisaties in het door hen vastgestelde beleid van responsible disclosure zich uit dienen te spreken over het niet doen van aangifte indien conform wordt gehandeld. Het OM heeft in 2013 en 2014 geen vervolging ingesteld naar melders die conform het RD-beleid van de desbetreffende organisaties handelden.

Actuele cijfers en duiding

Sinds de publicatie van de leidraad tot en met de peildatum van 1 december jl. zijn bij het NCSC 136 meldingen gedaan waarbij het NCSC een actieve rol op zich heeft genomen. In 2013 ontving het NCSC reeds 56 meldingen. Het ging om 18 meldingen inzake systemen van het NCSC, 25 meldingen betreffende overheidspartijen en 13 meldingen aangaande private organisaties waarbij het NCSC een actieve rol als intermediair tussen melder en organisatie heeft gespeeld. In 2014 heeft deze lijn zich doorgezet en er zijn tot de peildatum van 1 december jl. in totaal 80 meldingen gedaan. Het gaat hierbij om 16 meldingen inzake systemen van het NCSC, 41 meldingen omtrent systemen van de overheid en 23 meldingen waarbij het NCSC als actieve intermediair naar private partijen heeft opgetreden.
Daarnaast is sprake van circa 30 meldingen die onvolledig waren of reeds bij andere partijen waren ingebracht. Deze meldingen zijn als «false positive» niet in de statistieken opgenomen. In aanvulling op deze meldingen waarbij het NCSC een actieve rol heeft gespeeld en die in de cijfers zijn opgenomen, heeft het NCSC in veel gevallen melders en organisaties van wederzijdse contactgegevens voorzien. Deze cijfers illustreren een toenemend aantal meldingen en daarmee een groeiend vertrouwen tussen de bredere ICT-community en overheid en bedrijfsleven, met het NCSC daarbij als intermediair.

Ten einde meldingen omtrent systemen van de rijksoverheid rechtstreeks te kunnen doen plaatsvinden, heeft de Minister voor Wonen en Rijksdienst in 2014 een loket ten behoeve van de rijksoverheid ingericht[1]. Hierop zijn in 2014, tot en met de peildatum van 1 december, reeds 55 meldingen gedaan. In zeker 3 gevallen betreft het hier meldingen die zowel bij het NCSC als het loket zijn gedaan.
Tot slot heeft ook de Belastingdienst specifiek voor systemen van de Belastingdienst een loket ingericht. In 2014 zijn hier 22 meldingen binnengekomen. In geen enkel geval zijn fiscale- of persoonsgegevens in gevaar gekomen.
Hiernaast is uiteraard nog sprake geweest van de meldingen die rechtstreeks door melders bij partijen zijn gemeld die reeds een beleid voor responsible disclosure hanteren. Het formuleren en het al dan niet publiceren van deze cijfers past binnen de eigen verantwoordelijkheid die deze partijen hebben ten aanzien van informatiebeveiliging.
Het is van belang om aan te merken dat zeker niet alle meldingen majeure kwetsbaarheden betreffen, uit analyse van de eigen gegevens blijkt dat het in relatief veel gevallen om kleinere kwetsbaarheden gaat. Een aanzienlijk deel van de meldingen kan niet rechtstreeks resulteren in het ook daadwerkelijk benutten van de gesignaleerde kwetsbaarheid. Veelal betreft het kleinere implementatiefouten of onjuist uitgevoerde updates. Desalniettemin is het waardevol dat deze gemeld worden zodat ook deze kwetsbaarheden adequaat kunnen worden verholpen.
In diverse gevallen betrof het echter majeure kwetsbaarheden waarbij responsible disclosure een belangrijke rol heeft gespeeld. Voorbeelden van grote kwetsbaarheden die zijn gemeld zijn een kwetsbaarheid in Internet Explorer in 2013 en een kwetsbaarheid in libxml2 (een programmeerbibliotheek die door veel Linux-systemen wordt gebruikt) in 2014, waarbij samen met ontwikkelaars van de genoemde producten gewerkt is aan het oplossen van de kwetsbaarheid alvorens deze zo spoedig mogelijk te publiceren.

Vervolgacties

De cijfers laten zien dat met responsible disclosure in de afgelopen 2 jaar aanmerkelijke stappen zijn gezet. Twee jaar geleden was Nederland het eerste land in de wereld dat de stap van het actief uitdragen van responsible disclosure heeft gezet. Deze stap is gezet in een gezamenlijke beweging van overheid, private partijen en spelers binnen de bredere ICT-community. In de afgelopen 2 jaar is actief geïnvesteerd in het uitdragen van dit geluid in Nederland, zowel door het NCSC als door anderen zoals bijvoorbeeld de bancaire en telecommunicatiesector. Daarbij zijn in nationaal en internationaal verband presentaties gehouden en zijn ervaringen over de leidraad gedeeld. Hierbij gaat het onder meer over de wijze waarop Nederlandse (internationaal opererende) bedrijven met responsible disclosure om kunnen gaan. Dit krijgt in 2015 verdere verdieping langs de volgende drie sporen:

1. Het uitvoeren van een verkenning naar de wijze waarop responsible disclosure zich verhoudt tot diverse (internationale) rechtsstelsels, dit in het licht van het EU-voorzitterschap van Nederland in 2016;
2. internationale inzet om responsible disclosure actief uit te dragen, onder andere door het uitdragen van good practices tijdens de door Nederland georganiseerde Global Conference on CyberSpace in 2015 met als aanloop hiernaartoe de NCSC One Conference;
3. het in 2015 in samenspraak met betrokkenen binnen het bedrijfsleven en de bredere ICT-community toetsen en waar nodig aanvullen van de «Leidraad om te komen tot een praktijk van responsible disclosure».

[1] Te vinden op: http://www.rijksoverheid.nl/onderwerpen/cybercrime/cybercriminaliteit-bestrijden/responsible-disclosure.

Tot slot

Met de «Leidraad om te komen tot een praktijk van responsible disclosure» is sinds de publicatie in januari 2013 een feitelijke praktijk van responsible disclosure ontstaan, waarbij het wederzijdse vertrouwen tussen partijen binnen de ICT-community groeit. Hiermee groeit het op verantwoorde wijze melden en het daadwerkelijk verhelpen van ICT-kwetsbaarheden. De brede samenwerking tussen overheid, bedrijfsleven en ICT-community in Nederland heeft hier in belangrijke mate aan bijgedragen. De inzet van responsible disclosure in Nederland levert daarmee een belangrijke bijdrage aan het versterken van de digitale weerbaarheid van Nederland.

De Minister van Veiligheid en Justitie,
I.W. Opstelten