Ministerie van Veiligheid en Justitie

> Retouradres Postbus 16950 2500 BZ Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Nationaal Coördinator Terrorismebestrijding en Veiligheid
Directie Cyber Security

Oranjebuitensingel 25
2511 VE Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Ons kenmerk
336692

Bijlagen
1

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Datum 28 december 2012
Onderwerp Kader voor Responsible Disclosure

In het AO Cyber Security en Veiligheid van Overheidswebsites d.d. 10 april jl. heb ik uw Kamer toegezegd om te komen met een kader voor 'responsible disclosure', oftewel een leidraad voor (vitale) organisaties en overheden voor het vaststellen van een beleid voor het op verantwoorde wijze openbaar maken van ICT-kwetsbaarheden in informatiesystemen en softwareproducten. De 'leidraad om te komen tot een praktijk van responsible dicslosure' (zie bijlage 1) richt zich tevens op melders die responsible disclosure willen toepassen.

Over kwetsbaarheden in ICT en de wijze waarop deze verholpen kunnen worden is binnen de ICT-security-community veel kennis. Ook is er veel wil om deze te delen en er de juiste dingen mee te doen. De samenwerking van publieke en private partijen met de ICT-security-community is daarom van het grootste belang in het kader van het gezamenlijke streven naar cyber security. Ik wil hierbij dan ook nadrukkelijk, in lijn met de tijdens het AO Cyber Security d.d. 6 december jl. door uw Kamer uitgedragen wens, coalities bevorderen met partijen in de ICT-security-community die bereid zijn om bij te dragen aan het realiseren van een veilige en vitale digitale samenleving. Door een aantal organisaties uit onder andere de telecomsector en de financiële sector is reeds een handreiking op de eigen websites gezet voor het doen van meldingen over kwetsbaarheden in informatiesystemen. Deze ontwikkeling juich ik van harte toe.

Er bestaan meerdere manieren om kwetsbaarheden in ICT bekend te maken. Een kwetsbaarheid kan volledig publiekelijk bekend worden gemaakt waarbij een veiligheidsrisico groter wordt (full disclosure) of dit kan op een meer besloten manier gebeuren (de verantwoorde of 'responsible' disclosure). De responsible disclosure heeft nadrukkelijk mijn voorkeur. De door het Nationaal Cyber Security Centrum (NCSC) opgestelde leidraad dient dan ook om het toepassenvan responsible disclosure bij alle partijen te stimuleren. Bij het opstellen van deze leidraad om te komen tot een praktijk van responsible disclosure zijn in de afgelopen periode zowel beveiligingsonderzoekers als publieke en private partijen betrokken.

Nationaal Coördinator Terrorismebestrijding en Veiligheid
Directie Cyber Security

Datum
28 december 2012

Ons kenmerk
336692

Uitgangspunten bij responsible disclosure
- Eigenaars van informatiesystemen zijn zelf primair verantwoordelijk voor de beveiliging daarvan. Het op verantwoorde wijze melden van kwetsbaarheden kan in belangrijke mate bijdragen aan het verhogen van de veiligheid van deze systemen. Melders hebben daarbij een belangrijke maatschappelijke verantwoordelijkheid om kwetsbaarheden te ontdekken en op verantwoorde wijze te openbaren. Organisaties daarentegen dienen adequaat te reageren op meldingen.

- Centraal bij het werken met responsible disclosure staat dan ook het verhelpen van de kwetsbaarheid en het verhogen van de veiligheid van informatiesystemen. Hierin past het voor melders dan ook niet om onnodige schade aan te richten of verder te gaan dan noodzakelijk is voor het aantonen van de kwetsbaarheid. Organisaties dienen hierop te acteren en zo nodig de kwetsbaarheid te verhelpen.

Bouwstenen responsible disclosure
- Responsible disclosure heeft betrekking op de melder en de organisatie. De organisatie draagt publiekelijk en bijvoorbeeld ondersteund door een formulier op de website, het beleid voor responsible disclosure uit.

- De organisatie en melder maken afspraken over de termijn waarop de kwetsbaarheid verholpen zal zijn en over de wijze waarop zij met elkaar zullen communiceren.

- De organisatie en de melder maken afspraken over eventuele openbaarmaking en het verder inlichten van de ICT-security-community, zodat anderen lering kunnen trekken uit de kwetsbaarheid in kwestie.

- In het door de organisatie vastgestelde beleid van responsible disclosure dient de organisatie zich uit te spreken over het niet doen van aangifte indien conform wordt gehandeld. Deze leidraad laat de geldende strafrechtelijke kaders onverlet en beperkt niet de bevoegdheid van het Openbaar Ministerie om in bepaalde gevallen ambtshalve te vervolgen.

Rol NCSC
Responsible disclosure ziet primair op de relatie tussen een melder en een betrokken organisatie. In overleg kunnen zij besluiten om het Nationaal Cyber Security Centrum (NCSC) te informeren over een (met name nog niet bekende) kwetsbaarheid, om andere partijen binnen de ICT-security-community te informeren met het oog op het voorkomen of beperken van vervolgschade. Het NCSC is primair gericht op de cyber security van de Rijksoverheid en de vitale sectoren; kwetsbaarheden in deze sectoren hebben voor het NCSC dan ook de prioriteit. Na een duiding van de aard en omvang van de kwetsbaarheid kan het NCSC adequate actie ondernemen. Indien een (potentiële) melder direct in contact treedt met het NCSC, zal het NCSC trachten de melder met de organisatie in contact te brengen.

Acties in de komende maanden
Het NCSC zal bijgaande leidraad op de website plaatsen en het gebruik hiervan actief stimuleren bij de doelgroep en relaties van het NCSC. Verder zal ik als

coördinerend bewindspersoon voor cyber security in gesprek gaan met mijn collega's binnen de Rijksoverheid om te bevorderen dat responsible disclosure breed binnen de Rijksoverheid wordt toegepast. Tenslotte zal ik in de eerste helft van 2013 in overleg treden met het Openbaar Ministerie over meldingen van kwetsbaarheden in informatiesystemen die conform een beleid voor responsible disclosure worden gedaan.

Nationaal Coördinator Terrorismebestrijding en Veiligheid
Directie Cyber Security

Datum
28 december 2012

Ons kenmerk
336692

Tot slot
Het samenwerken aan de veiligheid van informatiesystemen en het verstandig en doeltreffend gebruikmaken van capaciteiten in de samenleving is een belangrijk onderdeel van het kabinetsbeleid op het vlak van cyber security. Het samenwerken via responsible disclosure is daarvan een voorbeeld. Ik zal mij dan ook sterk blijven maken om kwetsbaarheden via responsible disclosure te kunnen verhelpen om daarmee bij te dragen aan een veilige en vitale digitale samenleving.

De Minister van Veiligheid en Justitie,

I.W. Opstelten