Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2013–2014

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 297

BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 12 december 2013

In mijn brief van 3 april 2013 (Kamerstuk 26 643, nr. 272) heb ik, als coördinerend bewindspersoon voor cybersecurity, gesteld dat in de tweede Nationale Cyber Security Strategie (NCSS2) zal worden gekeken naar het versterken van de positie van het Nationaal Cyber Security Centrum (NCSC) als onderdeel van de Nationaal Coördinator Terrorismebestrijding en Veiligheid. Tijdens het algemeen overleg van 29 mei 2013 (Kamerstuk 26 643, nr. 286) heb ik toegezegd een juridische verkenning uit te voeren om te bezien hoe en op welke basis het NCSC gegevens kan verwerken om ook in de toekomst effectief te kunnen blijven optreden.

De NCSS2, die recent aan uw Kamer is gestuurd (Kamerstuk 26 643, nr. 291), schetst de ambities van het kabinet ten aanzien van de verdere ontwikkeling van de rol van het NCSC als centrale kennisautoriteit en expertisecentrum. Deze ambities en de aanvullende stappen die gezet moeten worden om hier de noodzakelijke voorwaarden voor te creëren worden in deze brief nader uitgewerkt.

Rol en ontwikkeling NCSC

Het NCSC heeft zich de afgelopen twee jaar ontwikkeld tot de centrale cybersecurity organisatie in Nederland. Er zijn aanzienlijke stappen gezet door het aansluiten van private partijen bij het NCSC in de vorm van de Information Sharing and Analysis Centres (ISAC's) op het gebied van energie, drinkwater, telecom, transport, financiën (banken en verzekeraars), nucleair, multinationals en de managed service providers. Deelnemers aan de ISAC's wisselen actief informatie uit. Het nationaal detectie en responsnetwerk is thans in voorbereiding met publieke en private partijen en wordt in 2014 op- en uitgebouwd. Ook is gebleken dat bij onder andere het Pobelka-incident en de DDOS-aanvallen in 2013 er een rol ligt voor het NCSC in aanvulling op bestaande crisismanagementstructuren. Dit is in lijn met de recent uitgebrachte Nationale Cyber Security Strategie. Daarin wordt een beweging geschetst van publiek-private samenwerking naar privaat-publieke participatie.

kst-26643-297
ISSN 0921 - 7371
's-Gravenhage 2013

Het NCSC, als onderdeel van het ministerie van Veiligheid en Justitie, vervult zijn taken ter voorkoming en beperking van verstoringen in het digitale domein in het belang van de nationale veiligheid, en richt zich gelet daarop op de (rijks)overheid en vitale sectoren. Het NCSC werkt samen met andere organisaties die op het gebied van cyber security een eigen verantwoordelijkheid hebben, zoals de politie en de inlichtingen- en veiligheidsdiensten (bijvoorbeeld ten aanzien van digitale spionage). Met de versterking van het NCSC ontstaat een dekkend stelsel van elkaar aanvullende taken en verantwoordelijkheden.

Als spin in het web heeft het centrum toegang tot een veelheid aan informatie over ICT-gerelateerde kwetsbaarheden en dreigingen. Het NCSC ontwikkelt zich steeds meer tot centraal meldpunt. In dit verband wijs ik op het ontwerp wetsvoorstel melding inbreuken elektronische informatiesystemen (*security breach notification*), dat ik inmiddels in procedure heb gebracht. Ook geldt er sinds 1 november jl. een wettelijke meldplicht voor certificatiedienstverleners ten aanzien van gekwalificeerde certificaten[1]. De verwachting is dat door het streven naar de hierboven genoemde intensivering van de samenwerking met (vitale) publieke en private partijen de informatiepositie van het NCSC nog verder wordt versterkt. Daarbij is het van groot belang de vertrouwelijkheid van aan het NCSC gemelde informatie afdoende te kunnen waarborgen.

De afgelopen periode is verder duidelijk geworden dat coördinatie bij de duiding van en de respons op digitale dreigingen en incidenten gewenst is. Dit geldt niet alleen tijdens een crisis maar ook wanneer anderszins sprake is van een dreiging of incident met mogelijke cascade-effecten waardoor maatschappelijke ontwrichting kan optreden. Door de veelheid aan partijen die geraakt kunnen worden door een incident en de snelheid waarmee een dreiging zich kan ontwikkelen, ontbreekt het individuele organisaties vaak aan het overzicht en het netwerk om direct effectief te kunnen reageren. Door zijn centrale positie in het cybersecurity netwerk en de publiek-private samenwerking, kan het NCSC, met inachtneming van de bestaande publiek-private contacten en crisismanagementstructuren, de coördinatie op zich nemen voor een gezamenlijke respons en ervoor zorgen dat de onderzoeksactiviteiten van de betrokken overheidspartijen elkaar ondersteunen en aanvullen.

Tevens zal het NCSC steeds vaker de zogeheten triage bij incidenten uitvoeren. Dit houdt in datna een incidentmelding het NCSC, in samenspraak met andere betrokken overheidspartijen, de eerste analyse zal uitvoeren van de aard van de verstoring, een inschatting zal maken van de potentiële maatschappelijke gevolgen en (gevraagd of ongevraagd) advies zal verstrekken aan betrokken organisaties over te nemen maatregelen. In voorkomende gevallen zal het NCSC ook anderszins (bv. technische) ondersteuning bieden aan vitale organisaties bij de reactie op dreigingen en incidenten.

De bovenstaande ontwikkelingen zorgen ervoor dat het NCSC zich blijft versterken in zijn rol als het nationale kennis- en expertisecentrum en samenwerkingsplatform op het gebied van cybersecurity en kan doorgroeien van nationale CERT tot het nationale cybersecurity operations center (NCSOC). Bovenstaande draagt tevens bij aan het versterken van de operationele crisiscoördinatie door het NCSC in het geval van een potentieel maatschappijontwrichtend cyberincident.

[1] Het belang van veilige certificaten blijkt uit de Diginotarcasus, waar beveiligingscertificaten gecompromitteerd waren.

Om binnen de geschetste ontwikkeling de rol van het NCSC te kunnen versterken zullen de komende periode de volgende drie acties worden uitgevoerd: 1) het verstevigen van de wettelijke grondslag van de taken en bevoegdheden van de minister van Veiligheid en Justitie op het terrein van cyber security, 2) het nader invulling geven aan het waarborgen van vertrouwelijkheid en 3) het versterken van de adviserende rol van het NCSC.

Wettelijke grondslag

Zoals toegezegd heb ik bezien hoe en op welke basis het NCSC nu en in de toekomst gegevens kan verwerken om effectief te kunnen optreden, zonder overigens in de taken en bevoegdheden van bijvoorbeeld de inlichtingen- en veiligheidsdiensten te treden. Uitkomst hiervan is enerzijds dat voor de huidige verwerking van persoonsgegevens door het NCSC thans een afdoende wettelijke grondslag als vereist in de Wet bescherming persoonsgegevens voorhanden is. Anderzijds is het, juist ook gelet op bovenvermelde ontwikkelingen met betrekking tot het NCSC, aangewezen de taken in het kader waarvan verwerking van persoonsgegevens geschiedt (zoals de analyse ten behoeve van advisering en ondersteuning bij incidenten of dreigingen) alsmede de bevoegdheid tot die verwerking van een steviger wettelijke grondslag te gaan voorzien. In het verlengde hiervan acht ik het gewenst dat met het oog op dezelfde taken ook de bevoegdheid tot het verwerken van andere gegevens (bijvoorbeeld over *malware* of kwetsbaarheden) van een concrete wettelijke basis wordt voorzien. In dat verband zal wettelijk ook worden geregeld onder welke voorwaarden de bevoegdheid tot verstrekking van gegevens aan andere partijen plaats kan vinden. Tenslotte verdient het naar mijn oordeel aanbeveling de bevoegdheid om bijvoorbeeld bij andere publiekrechtelijke organisaties de voor bovengenoemde taakuitoefening benodigde gegevens te vragen, alsook waar nodig de bevoegdheid van die andere bestuursorganen om de gevraagde informatie te verstrekken, van een wettelijke basis te voorzien.

De hiervoor benodigde wetgeving zal ik, in samenhang met het wetsvoorstel melding inbreuken elektronische informatiesystemen, in voorbereiding nemen.

Waarborgen vertrouwelijkheid

Een randvoorwaarde voor het realiseren van de ambities van het NCSC is dat de vertrouwelijkheid van de aangeleverde informatie in voldoende mate kan worden gewaarborgd. Wanneer partijen uit de vitale sectoren te terughoudend worden met het delen van informatie over hen aangaande incidenten met het NCSC, omdat bijvoorbeeld hun namen in relatie tot specifieke incidenten openbaar gemaakt zouden kunnen worden, benadeelt dat het NCSC in ernstige mate in het goed kunnen uitvoeren van zijn taken in het belang van de nationale veiligheid. Voor de betrokken organisaties geldt dat het openbaar worden van tot hen herleidbare informatie over concrete kwetsbaarheden in netwerken en systemen, of het beheer daarvan, ertoe kan leiden dat zij kwetsbaarder worden voor gerichte aanvallen. Ook kan dergelijke informatie schade toebrengen aan de reputatie en concurrentiepositie van deze organisaties.

Ten aanzien van bij het NCSC berustende gegevens geldt dat daarop de Wet openbaarheid van bestuur (Wob) van toepassing is. Om bovenvermelde redenen is volledige openbaarmaking van bij het NCSC door het bedrijfsleven gemelde informatie naar mijn oordeel echter niet gewenst. Daarom zal ik bij toekomstige Wob-verzoeken als vaste beleidslijn voeren dat naar aanleiding van Wob-verzoeken waarin verzocht wordt om door

private partijen aan het NCSC gemelde informatie over incidenten, de naam van de getroffen organisatie, overige kenmerken van de melding die tot identificatie van de betrokken organisatie kunnen leiden en informatie over (het beheer van) de bij het incident betrokken systemen van die organisatie in beginsel niet openbaar worden gemaakt. Ik zal hiertoe in ieder geval de in de Wob opgenomen uitzonderingsgronden toepassen die stellen dat openbaarmaking achterwege blijft voor zover het vertrouwelijk aan de overheid meegedeelde bedrijfs- en fabricagegegevens betreft (artikel 10, eerste lid, aanhef en onder c) en voor zover het belang van openbaarmaking niet opweegt tegen het belang om oneven-redige benadeling van het NCSC dan wel de meldende organisatie te voorkomen (artikel 10, tweede lid, aanhef en onder g). Daarnaast zal ik bezien of er met het oog hierop ten aanzien van meldingen van organisaties bij het NCSC, gekozen zou moeten worden voor een in de wet op te nemen bijzondere openbaarheidsregeling.

Overigens zal ik, teneinde de samenleving te informeren over dreigingen tegen en kwetsbaarheden bij organisaties, de andere door private partijen bij het NCSC gemelde informatie, zoals aantallen meldingen en typen incidenten, openbaar maken door periodiek een naar sectoren uitgesplitst overzicht te publiceren.

Adviezen NCSC

In de NCSS2 wordt benadrukt dat de overheid gezien het toegenomen belang van het digitale domein daar waar nodig een meer zichtbare rol op zich neemt.

Zoals hierboven gesteld is het NCSC belast met de operationele crisisco-ördinatie in het geval van een cyberincident. Het is echter ook nodig dat het NCSC in staat is om, bij vaststelling van kwetsbaarheden die kunnen leiden tot uitval van vitale diensten en daarmee tot maatschappelijke ontwrichting, de relevante partijen een richtinggevend advies te geven. Ik acht het ongewenst dat, wanneer het NCSC in zijn taakuitvoering op voormelde kwetsbaarheden stuit, de reactie van organisaties op het advies van het NCSC met betrekking tot de aanpak van de kwetsbaarheden een te vrijblijvend karakter heeft. In ernstige gevallen zal het NCSC daarom, gevraagd of ongevraagd, een schriftelijk advies verstrekken aan de betrokken organisatie(s) waarin wordt vermeld welke maatregelen genomen zouden kunnen worden om de vastgestelde kwetsbaarheden weg te nemen. Het blijft vervolgens primair de eigen verantwoordelijkheid van de betrokken organisatie om mede gelet hierop de meest passende maatregelen te nemen teneinde uitval of verstoring van genoemde diensten zo veel als mogelijk te voorkomen of beperken. Ook is het aan de organisatie om, wanneer daar aanleiding toe is, de eigen toezicht-houder(s) of vakdepartementen hiervan op de hoogte te stellen.

Wanneer het NCSC een advies heeft verstrekt blijft het met de betrokken organisatie in overleg. Indien mocht blijken dat de betrokken organisatie geen of onvoldoende maatregelen treft, en het risico op maatschappelijke ontwrichting aanwezig blijft, kan ik in die uitzonderlijke gevallen, onder medezending van het advies van het NCSC, het voor de betreffende sector verantwoordelijke ministerie, met het oog op diens wettelijke verantwoordelijkheid, daarvan op de hoogte stellen. Voor het in dit verband ook kunnen delen van meldingsinformatie zal ik zo nodig een wettelijke basis in bovengenoemde ontwerpwetgeving opnemen.
Op deze wijze wil ik bevorderen dat ernstige kwetsbaarheden voortvarend en in nauwe samenwerking worden opgelost. Over de precieze invulling van bovenstaande werkwijze zal ik mij nog nader verstaan met de betrokken organisaties.

De Cybersecurityraad is geconsulteerd en heeft zijn steun uitgesproken voor de bovengenoemde uitgangspunten en beleidskeuzes.

Met de bovenstaande acties wordt, conform de ambitie van de NCSS2 om Nederland leidend te laten zijn op het gebied van cybersecurity, het NCSC in staat gesteld om structureel als de centrale kennisautoriteit, expertisecentrum en samenwerkingsplatform voor cybersecurity te functioneren.

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