Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2013–2014

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 322 **BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 10 juli 2014

Hierbij bied ik uw Kamer, vanuit mijn coördinerende verantwoordelijkheid voor cybersecurity, de vierde editie van het Cyber Security Beeld Nederland (CSBN-4) aan[1]. Het CSBN wordt jaarlijks, onder de verantwoordelijkheid van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), opgesteld door het Nationaal Cyber Security Centrum (NCSC). De rapportage komt tot stand in samenwerking met publieke en private partners.

Het cyberdomein is steeds meer verweven met ons dagelijks leven. Deze verregaande digitalisering dient niet alleen gemak, plezier en efficiëntie, maar is ook een belangrijke drijver voor innovatie. Veiligheid is hierbij een basisvoorwaarde. Veilige ICT versterkt het vertrouwen van eindgebruikers bij het gebruik, geeft een impuls voor de ontwikkeling van meer (online) diensten en leidt tot meer economische groei. Het CSBN biedt daarom inzicht in belangen, dreigingen en kwetsbaarheden van onze digitale samenleving. De inzichten uit het CSBN bieden houvast om waar nodig digitale weerbaarheid van Nederland te versterken of lopende cybersecurity-programma's aan te scherpen. Het CSBN-4 bestrijkt de maanden april 2013 tot en met maart 2014.

Ik hecht er aan uw Kamer te informeren over de beleidsopvolging van het CBSN-4. Alvorens hier op in te gaan wil ik het internationale karakter van cybersecurity benadrukken. Dit internationale karakter vraagt om een internationale aanpak. Om die reden organiseert Nederland volgend jaar de «Global Conference on Cyber Space 2015» waarbij cybersecurity en cybercrime belangrijke thema's zullen zijn. Cybersecurity en cybercrime zijn ook als prioritaire thema's voor het Nederlandse EU voorzitterschap in 2016 aangemerkt. Het CSBN-4 zal in deze en andere internationale gremia worden uitgedragen om de in het beeld geschetste dreigingen en risico's ook internationaal onder de aandacht te brengen.

[1] Raadpleegbaar via www.tweedekamer.nl

kst-26643-322
ISSN 0921 - 7371
's-Gravenhage 2014

Het CSBN-4 laat zien dat het dreigingsbeeld uit het CSBN-3 zich doorzet en bevestigt de noodzaak tot een integrale, publiek-private, (inter)nationale cyber security-aanpak. De geactualiseerde Nationale Cyber Security Strategie 2 (NCSS-2) die ik uw Kamer in oktober 2013 toezond (Kamerstuk 26 643, nr. 291), is hierbij voor publieke en private partners in cybersecurity het raamwerk om de beleidsopvolging vorm te geven.

Cybercrime en digitale spionage blijven de grootste dreiging die in het CSBN-4 worden gesignaleerd. Door de technische mogelijkheden om data te verzamelen komt de privacy onder druk te staan. Als gevolg van een steeds verder toenemende digitalisering, een toenemende afhankelijkheid van ICT en de koppeling van ICT-systemen (internet of things) worden veiligheidsvraagstukken steeds complexer. Een voorbeeld hiervan is het risico verbonden aan het toenemende aantal apparaten dat aan internet is verbonden, terwijl de software van de apparaten niet voor langere tijd door de leveranciers onderhouden (kan) worden. De apparatuur kan hierdoor kwetsbaar worden. Deze problematiek wordt in het CSBN aangeduid als ICT-duurzaamheidsproblematiek.

Deze trends en ontwikkelingen, die in het CSBN-3 al werden geconstateerd, versterken elkaar en worden nadrukkelijker zichtbaar. Door de toenemende digitalisering en afhankelijkheid van ICT neemt de impact, alsmede het risico van cyberaanvallen en verstoringen toe. Grootschalige verstoringen van de digitale infrastructuur kunnen binnen de vitale sectoren leiden tot ontwrichting of uitval van dienstverlening met maatschappelijke onrust als mogelijk gevolg. Deze ontwikkeling zorgt er voor dat de digitale weerbaarheid van Nederland onder druk blijft staan. Het CSBN-4 bevestigt hiermee het belang van de met de NCSS-2 ingeslagen weg en de noodzaak om de komende jaren als overheid, in privaat-publieke participatie, met kennisinstellingen en vitale sectoren te blijven investeren in cybersecurity. De Cyber Security Raad heeft het CSBN-4 en deze beleidsopvolging besproken en is positief over de geschetste lijn.

Hieronder treft u de vier kernbevindingen uit het CSBN-4 aan en de maatregelen waarmee de overheid hier op inspeelt.

1. Potentiële impact van cyberaanvallen en verstoringen neemt toe door snelle digitalisering

Waar in het CSBN-3 werd geconstateerd dat de afhankelijkheid van ICT aanzienlijk is en toeneemt als gevolg van ontwikkelingen als hyperconnectiviteit en cloudcomputing, blijkt uit het CSBN-4 dat deze trend zich onverminderd voortzet. Dit vergroot de potentiële impact van aanvallen en verstoringen. Het voorkomen van maatschappelijke ontwrichting als gevolg van een verstoring of uitval van vitale producten en diensten heeft de constante aandacht van de overheid.

- In het kader van het voorkomen van maatschappelijke ontwrichting als gevolg van de uitval van vitale producten en diensten brengt de overheid in de aanpak vitale infrastructuur, samen met vitale partijen, in kaart welke ICT-afhankelijke diensten en processen vitaal zijn. Hieraan is een programma gekoppeld dat op basis van risicoanalyses (basis-)eisen stelt aan de veiligheid van deze diensten en processen. Daarnaast wordt een trainingsprogramma of -module voor respons bij grootschalige ICT-incidenten ontwikkeld.
- In, onder andere, Europees verband wordt ingezet op de verbetering of ontwikkeling van standaarden die de veiligheid van ICT-producten bevorderen. Ook in het kader van de Global Conference on Cyber Space 2015 die volgend jaar in Nederland plaatsvindt wordt hier aandacht aan besteed.

- De Rijksoverheid neemt voor haar eigen ICT-systemen «security by design» mee in aanbestedingstrajecten, om systemen veiliger te maken en de impact van een mogelijke verstoring beperkt te houden. Andere overheden worden opgeroepen hetzelfde te doen.
- Er loopt een verkenning naar de wenselijkheid en haalbaarheid van gescheiden ICT-netwerken en diensten voor publieke en private vitale processen.
- 100% veiligheid bestaat niet. Wel kunnen we inzetten op een versterkte inzet en samenwerking op detectie, analyse en responscapaciteiten zodat digitale aanvallen snel gedetecteerd kunnen worden en de schade zo beperkt mogelijk blijft door een snelle en adequate respons.
- In april 2014 is bij de rijksoverheid een pilot gestart in het kader van de op- en uitbouw van het Nationaal Detectienetwerk (NDN). De pilot heeft een looptijd van zes maanden. Eind 2014 zal er daarmee een geteste en robuuste opzet voor detectie staan. De ervaringen in de pilot zijn leidend voor het vervolg, nl. het aansluiten van nieuwe partners, ook buiten de rijkoverheid.
- Het Nationaal Respons Netwerk is in april 2014 gelanceerd. Met de vijf lanceringspartners zijn samenwerkingsconvenanten afgesloten die onderlinge bijstand bij incidenten regelen. Deze partners zullen in het najaar voorstellen hebben uitgewerkt om te komen tot gezamenlijke risicoanalyses, oefeningen en wederzijdse stages. Vanuit het NCSC worden momenteel meerdere organisaties ondersteund bij de inrichting van eigen responscapaciteiten om aan het NRN bij te kunnen dragen. Ook heeft zich een aantal nieuwe potentiele partners aangemeld. Daarmee zal het NRN verder worden uitgebreid.
- De capaciteiten en positie van het NCSC wordt versterkt. Ook worden de onderzoeks- en analysecapaciteiten van NCSC, Politie, AIVD en MIVD versterkt waardoor beter inzicht ontstaat in dreigingen en risico's in het cyberdomein.
- De mogelijkheden tot inzet van digitale capaciteiten van Defensie bij het voorkomen en afweren van aanvallen op de vitale infrastructuur, onder civiel gezag en binnen de hiervoor geldende juridische kaders, worden nader uitgewerkt.

2. Gebrek aan ICT-duurzaamheid en toenemende koppeling vormen risico voor maatschappelijke veiligheid

In het CSBN-4 wordt opnieuw geconstateerd dat de kwetsbaarheid van ICT hoog is, door de ontdekking van nieuwe kwetsbaarheden en de ontwikkeling van nieuwe diensten en innovatieve apparatuur. Ook vormt de duurzaamheid van ICT een risico voor de maatschappelijke veiligheid als gevolg van de toenemende koppeling van ICT. Vooral waar het gaat om het voorkomen van maatschappelijke ontwrichting als gevolg van de verstoring van vitale producten en diensten is dit een belangrijk aandachtspunt.

- Legacy systemen[2] en andere mogelijke risico's in de vitale infrastructuur worden in kaart gebracht. Het gaat hier onder andere om systemen waarbij de risico's gerelateerd aan de ICT-duurzaamheid een rol speelt. De resultaten hiervan zullen worden meegenomen in de brede aanpak vitale infrastructuur.
- Zoals hierboven reeds is aangegeven wordt cybersecurity meegenomen in de aanpak vitale infrastructuur, waarbij de overheid samen met vitale partijen risico's in kaart brengt en er onder andere een programma wordt opgesteld dat (basis-)vereisten aan veiligheid stelt.

[2] Legacy systemen: software die verouderd is, wel nog gebruikt wordt, maar minimaal wordt onderhouden met alleen kleine updates.

- Met de sectorale toezichthouders wordt overleg gevoerd om cybersecurity-vereisten op te nemen bij toezicht. De risico's gerelateerd aan ICT-duurzaamheid worden meegenomen in dit traject.
- In de derde, landelijke Alert Online campagne van 27 oktober tot 6 november a.s. wordt aandacht besteed aan de problematiek van ICT-duurzaamheid. Deze zal ook op individuele gebruikers zijn gericht die even goed te maken kunnen krijgen met deze problematiek. Een voorbeeld is het staken van de ondersteuning van Windows XP waardoor niet meer wordt voorzien in beveiligingsupdates. Het is van belang dat mensen zich bewust zijn van digitale risico's zodat men op tijd de eigen verantwoordelijkheid kan nemen omwille van de persoonlijke digitale veiligheid. In dat kader zal tijdens de Alert Online campagne ook de website Veiliginternetten.nl worden gelanceerd. Op de website worden eindgebruikers geïnformeerd over de risico's van internetgebruik en wordt handelingsperspectief geboden. De website is een samenwerking tussen het Ministerie van Economische Zaken, het Ministerie van Veiligheid en Justitie en ECP, platform voor de informatiesamenleving.

3. De dreiging die uitgaat van criminelen en statelijke actoren blijft onverminderd groot

Het aantal digitale spionageaanvallen is toegenomen evenals de complexiteit en de impact van deze aanvallen. Bijna elke buitenlandse inlichtingendienst heeft de afgelopen jaren geïnvesteerd in zijn digitale capaciteiten. Door digitale spionage kunnen Nederlandse publieke en economische belangen ernstig worden geschaad. Nederland dient een «safe place to do business» te blijven.

- De overheid investeert in een verhoging van de algehele digitale weerbaarheid, mede om de weerbaarheid tegen digitale spionage te verhogen. Zo behelst deze investering het versterken van capaciteiten die zijn gericht op het detecteren, afweren en mitigeren van digitale spionagepogingen, zoals detectie, analyse- en responscapaciteiten. Ook worden onderzoeks- en analysecapaciteiten van NCSC, Politie, AIVD en MIVD versterkt om inzicht te krijgen in dreigingen en risico's in het cyberdomein zoals digitale spionage.

Op het gebied van cybercriminaliteit wordt een toenemende professionalisering en internationalisering waargenomen. Hierdoor komen (complexe) cyberaanvallen binnen het bereik van minder (digitaal) ervaren of geëquipeerde criminelen.

- Cybercrime wordt krachtig aangepakt. Hiertoe wordt (straf)wetgeving versterkt. Belangrijk is in dit kader de Wet Computercriminaliteit III die de Nationale Politie meer slagkracht geeft op het gebied van cybercrime. Internationaal wordt ingezet op het versterken van de samenwerking en het harmoniseren van wetgeving.
- Naast een versterking van (straf)wetgeving worden ook de capaciteiten van de Nationale Politie kwantitatief en kwalitatief versterkt zodat meer cybercrimezaken kunnen worden aangepakt.
- Ook het gebruik van botnets wordt aangepakt. Over deze aanpak bent u conform mijn toezegging tijdens het Algemeen Overleg met uw Kamer van 27 maart 2014, recent afzonderlijk over geïnformeerd.

4. Privacy onder druk door technische mogelijkheden om data te verzamelen

In het CSBN-4 wordt geconstateerd dat door technische mogelijkheden om data te verzamelen de privacy onder druk staat. De trend waarbij steeds meer aspecten van ons dagelijks leven, zoals zoek- of aankoopgedrag of muziekvoorkeuren die direct of indirect digitaal worden

vastgelegd zal de komende jaren onverminderd voortzetten. Het betreft hier een ontwikkeling die onder andere nauw samenhangt met het verdienmodel van veel populaire (gratis) producten en diensten. Hier bestaat een spanningsveld tussen vrijheid, maatschappelijke groei (waaronder economische ontwikkeling) en veiligheid. Dit spanningsveld is ook beschreven en geduid in de NCSS-2, de notitie; «vrijheid en veiligheid in de digitale samenleving, een agenda voor de toekomst» (Kamerstuk 26 643, nr.298) en de visie op e-privacy (Kamerstuk 32 761, nr. 49). Deze trend staat daarmee nadrukkelijk op de agenda van het Kabinet. Ik heb de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) met betrekking tot deze problematiek om advies gevraagd.

- De WRR is gevraagd om een advies waarin wordt ingegaan op de volgende drie hoofdvragen:
    1. moet er een sterker onderscheid worden gemaakt tussen toegang tot en gebruik van gegevens bij «big data»;
    2. hoe kan er bij het gebruik van «big data» voor worden gezorgd dat het proces van «profiling», «datamining» en andere analysetechnieken ten behoeve van de veiligheid voldoende transparant zijn; en
    3. wat betekent de komst van kwantumcomputers voor het proces van gegevensverwerking ten behoeve van de veiligheid.
- Daarnaast hebben initiatieven gericht op privacy by design extra prioriteit gekregen.
    1. De Rijksoverheid neemt voor haar eigen ICT-systemen «privacy by design», systemen waarbij bij het ontwerp al rekening is gehouden met privacy aspecten, mee in aanbestedingstrajecten. Andere overheden worden opgeroepen hetzelfde te doen.
    2. In, onder andere, Europees verband wordt ingezet op de verbetering of ontwikkeling van standaarden die privacy in ICT-producten bevorderen.

Naast voornoemde acties wordt in algemene zin ook onverkort ingezet op het stimuleren van cybersecurity-onderwijs en kennisontwikkeling. Het cybersecurity domein is een kennisintensief domein. Het is essentieel voor de weerbaarheid van het Nederland van vandaag en morgen dat er voldoende cybersecurity-experts zijn en zowel publieke als private (vitale) partijen een voldoende kennisbasis hebben om de snelle ontwikkeling van dreigingen bij te houden en waar mogelijk voor te zijn.

Zoals reeds aangegeven is de NCSS-2 het raamwerk waarbinnen de in deze beleidsreactie genoemde maatregelen worden uitgevoerd. Voor het einde van het jaar wordt u door mij per brief geïnformeerd over de voortgang van de implementatie van de strategie.

Met bovenstaande maatregelen versterkt het kabinet de algehele weerbaarheid van de samenleving tegen cyberdreigingen en wordt bijgedragen aan een open, vrije en veilige digitale samenleving, waar de kansen die digitalisering ons biedt optimaal worden benut.

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