Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 258

BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 12 november 2012

In september 2011 onderstreepten de gebeurtenissen bij DigiNotar in welke mate de overheid, en in het verlengde hiervan de gehele maatschappij, afhankelijk is geworden van het onverstoord functioneren van informatie en communicatietechnologie (ICT).

In het plenair debat DigiNotar d.d. 13 oktober 2011 (Handelingen II 2011/12, nr. 12, item 26, blz. 99–127) is door de Minister van Binnenlandse Zaken en Koninkrijksrelaties en mij reeds aangegeven dat het van groot belang is om te leren van dergelijke incidenten en deze grondig te evalueren. Derhalve hebben de Minister van Binnenlandse Zaken en Koninkrijksrelaties en ik zowel de Onderzoeksraad voor de Veiligheid (OVV) als de Inspectie Veiligheid en Jusitie (IVenJ) verzocht om een onderzoek uit te voeren. De OVV heeft zich daarbij gericht op het gehele stelsel waarin betrokken partijen de digitale veiligheid waarborgen van (internet)communicatie tussen burgers en de overheid. De IVenJ heeft zich daarbij gericht op de crisisbeheersingsaspecten van het incident bij DigiNotar. De Minster van Binnenlandse Zaken en Koninkrijksrelaties heeft de OVV op 12 november jl. reeds een reactie doen toekomen op het rapport van de OVV (Kamerstuk 26 643, nr.257). Deze reactie is tevens aan uw Kamer verzonden.

In deze brief zal ik ingaan op het rapport[1] van de IVenJ, zoals ik uw Kamer d.d. 9 juli jl. heb doen toekomen en de conclusies en aanbevelingen die daarin gedaan zijn. Verder zal ik ingaan op de door mij ondernomen acties om de crisisbeheersing verder te versterken. Tot slot zal ik op verzoek van uw Kamer het Nationaal Crisis Plan ICT toelichten en aan uw Kamer doen toekomen.

Conclusies van de Inspectie Veiligheid en Justitie

Ten aanzien van het rapport van de Inspectie Veiligheid en Justitie kan ik u ten eerste aangeven dat alle aanbevelingen van de Inspectie onverkort over zullen worden genomen.

[1] Zie Kamerstukken 2011/2012, 26 643 nr. 250

kst-26643-258
ISSN 0921 - 7371
's-Gravenhage 2012

De IVenJ concludeert in haar rapport «Evaluatie van de Rijkscrisisorganisatie tijdens de DigiNotar-crisis» het volgende: «de Rijkscrisisorganisatie heeft tijdens de DigiNotar-crisis doeltreffend gefunctioneerd. Het doeltreffend functioneren van de Rijkscrisisorganisatie is mede te danken aan de korte lijnen, de goede samenwerking en het doortastende optreden van de belangrijkste sleutelfunctionarissen. Vanaf het begin van de crisis reageert de crisisorganisatie alert. De mogelijke gevolgen van de hack bij DigiNotar zijn snel onderkend. Hoewel men in het begin nog geen compleet beeld heeft van de dreiging schaalt men de crisisorganisatie vlot op. Hierdoor maak men snel een start met de beheersing van de (dreigende) crisis.»

Het is verheugend om te zien dat de crisisorganisatie ten tijde van een incident doeltreffend heeft kunnen functioneren. Dit neemt niet weg dat ik blijvend inzet op het verder versterken van de crisisorganisatie binnen het digitale domein. In dit kader zijn in de afgelopen maanden de volgende aanvullende initiatieven gestart:

1. Door de toegenomen afhankelijkheid van ICT neemt tevens de kans toe dat de oorzaak of oplossing van crises ligt in security-gerelateerde aspecten van ICT. Het Nationaal Cyber Security Centrum (NCSC) werkt daarom aan de verdere ontwikkeling en professionalisering van de diverse onderdelen van haar operationeel coördinerende rol bij crisisbeheersing op het vlak van cyber security. Dat doet het NCSC door de interne crisissctructuur te versterken en te zorgen dat het optimaal als centraal contactpunt voor (inter)nationale bedrijven en organisaties kan fungeren. In het bijzonder is gewerkt aan de verdere doorontwikkeling en uitrol van de publiek-private «ICT-Response Board» (IRB), als adviserend instrument binnen de nationale crisisstructuur. Voor de IRB is een e-learning omgeving en een simulatietraining ontwikkeld, die IRB-leden de processen eigen leert maken en ermee leert oefenen. Daarnaast ontwikkelt het NCSC een oefenbeleid en zal het NCSC zich door middel van oefeningen verder prepareren op de voornoemde operationeel coördinerende rol bij ICT-crises. Zo vond recent de internationale oefening Cyber Europe 2012 plaats en zal ook in 2013 door het NCSC worden deelgenomen aan (inter)nationale oefeningen op het vlak van cyber security.

2. In de brief van de Minister van Binnenlandse Zaken en Koninkrijksrelaties aan de Onderzoeksraad voor de Veiligheid d.d. 12 november jl., die door de Minister van Binnenlandse Zaken en Koninkrijksrelaties ook aan uw Kamer is verzonden, wordt reeds aangegeven dat binnen de samenwerking met VNG/KING de gemeentelijke Informatiebeveiligingsdienst (IBD) zich in de kwartiermakerfase bevindt. Vanuit BZK en V&J wordt de ontwikkeling van deze dienst verwelkomd. Vanuit het NCSC zal een adviseur ter beschikking gesteld worden om met het opzetten van de IBD bij te dragen aan de belangrijke stap van de landelijke ontwikkeling van sectorale capaciteiten op het gebied van ICT-response. Deze ontwikkeling geeft een impuls aan de verbintenis tussen het NCSC en partijen waar een groot belang aan wordt toegekend buiten de primaire doelgroep (Rijksoverheid en vitale sectoren) van het NCSC. Niet alleen kunnen langs deze weg verschillende sectoren binnen de eigen verantwoordelijkheid zelfstandig digitale weerbaarheid vergroten, ook wordt hiermee de uitrol van een effectief landelijk netwerk van sectorale informatiebeveiligingsdiensten gestimuleerd. Dit ligt in lijn met het vanuit het NCSC geïnitieerde Programma Nationaal Response Netwerk. Het doel van dit programma is het vergroten van de weerbaarheid van de Nederlandse samenleving door het creëren en stimuleren van een netwerk van response-organisaties binnen Nederland. Dit doet niet af

aan de eigen verantwoordelijkheid van de deelnemende organisaties voor de beveiliging van hun bedrijfsprocessen en bedrijfsgegevens. De leden van het netwerk kunnen elkaar echter ondersteunen via vertrouwde relaties en heldere afspraken. Zo kunnen bij een (grote) dreiging of verstoring snel de juiste partijen gemobiliseerd worden en neemt de weerbaarheid tegen cyber security verstoringen toe binnen de diverse sectoren of domeinen.

3. Het constant actueel houden van de planvorming ten aanzien van de crisisorganisatie. Verder in deze brief zal ik nader ingaan op het Nationaal Crisisplan ICT (NCP-ICT). Dit is het leidende plan in het geval van een cyber-incident en het strekt tot aanbeveling om dergelijke plannen consequent te bezien in het licht van ontwikkelingen in het digitale domein. De ontwikkelingen in het digitale domein voltrekken zich in een hoog tempo. In dit plan wordt ingegaan op de specifieke organisaties en hun rol bij crises in het digitale domein. Specifiek voor ICT-crises is dat gebruik gemaakt wordt van publiek-private gremia zoals de IRB en dat het NCSC een operationeel coördinerende rol heeft. Verder wordt gebruik gemaakt van de kaders van de generieke Rijkscrisisstructuur.

Aanbevelingen

In haar rapport doet de IVenJ de volgende twee aanbevelingen:

1. Blijf investeren in een vaste kernbezetting van de rijkscrisisorganisatie, met deelnemers die door opleiding en oefening over de juiste crisiscompetenties beschikken.

2. Bezie de bemensing, werkwijze en status van het Adviesteam binnen de rijkscrisisorganisatie vanuit het oogpunt van doeltreffendheid. Indien waarde wordt gehecht aan het Adviesteam, organiseer het Adviesteam dan zo, dat het zijn rol als adviseur van de MCCb en de ICCb kan waarmaken.

Ik onderschrijf de aanbevelingen. De eerste aanbeveling is in lijn met het leidende principe van crisisbeheersing *«train as you fight and fight as you train»*. Rijksbreed wordt intensief samengewerkt aan de opleiding en oefening van deelnemers van de rijkscrisisorganisatie o.a. door middel van de NationaalCrisisCentrum (NCC) -academie en crisisoefeningen zoals bijvoorbeeld de ICT-oefeningen Cyberstorm[1] en Copy Paste, maar ook bijvoorbeeld de oefening Vulcanus die 4 oktober jl. heeft plaatsgevonden waarin natuurbranden centraal stonden. Over de uitkomsten van de oefening Vulcanus wordt u separaat geïnformeerd voor het zomerreces.

Zoals bovenstaand al vermeld is er recent ook in Europees verband geoefend binnen de oefening Cyber Europe 2012. Ook in 2013 zal er regelmatig deel worden genomen aan nationale en internationale oefeningen.

Ten aanzien van de tweede aanbeveling onderschrijven wij het belang om de rol van het Adviesteam nader te bezien. Een en ander wordt meegenomen in het rijksbrede traject met betrekking tot herziening van het Nationaal Handboek Crisisbesluitvorming, dat thans gaande is. Het aangepaste Handboek zal naar verwachting eind 2012 door de ministerraad worden vastgesteld.

[1] Kamerstuknummer: 26643–185

Nationaal Crisisplan ICT:

In reactie op het verzoek van het lid Elissen (PVV) van uw Kamer is in het Algemeen Overleg Cyber Security d.d. 10 april jl. (Kamerstuk 26 643, nr. 240) reeds toegezegd uw Kamer het NCP-ICT te doen toekomen. Een dergelijk crisisplan vormt de basis van het acteren van de crisisorganisatie op een bepaald specifiek domein, zoals in dit geval het digitale domein. In bijlage 1 treft u dan ook het NCP-ICT aan.*)

Het NCP-ICT is een beschrijving van de rijkscrisisstructuur bij een ICT-crisis. Het doel van het NCP-ICT is het waarborgen dat tijdens een ICT-crisis zo veel als mogelijk wordt gewerkt volgens de generieke crisisstructuur aangevuld met de noodzakelijke specifieke kennis en expertise om een ICT-crisis te beheersen.

Het terrein van cyber security is constant in beweging. Een crisisplan is echter een momentopname van de huidige situatie. Beleidsontwikkelingen of nieuwe wet- en regelgeving kunnen pas opgenomen worden in een crisisplan wanneer deze van kracht zijn. Om deze reden is het NCP-ICT een levend en regelmatig te actualiseren document.

Hoewel de crisisbeheersing effectief heeft gefunctioneerd is dit een onderwerp waarop blijvend inspanning noodzakelijk is om de crisisbeheersing nu en in de toekomst op het gewenste niveau te houden. Daartoe zal onverminderd worden ingezet op het opleiden, trainen en oefenen van medewerkers en de kwaliteit van de crisisorganisatie om in het geval van een incident effectief op te kunnen treden.

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

*) Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer