Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 285

BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 3 juli 2013

Conform de toezegging van 23 september 2011 (Kamerstuk, 26 643, nr. 220) zend ik u hierbij de derde editie van het Cybersecuritybeeld Nederland (CSBN-3)[1]. Het Cybersecuritybeeld Nederland wordt jaarlijks onder verantwoordelijkheid van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) opgesteld door het Nationaal Cyber Security Centrum (NCSC) en komt tot stand in samenwerking met publieke en private partners. De rapportageperiode bestrijkt de maanden april 2012 tot en met maart 2013. Tevens zijn de belangrijkste ontwikkelingen tot begin mei 2013 meegenomen.

Het CSBN biedt inzicht in de belangen die we moeten beschermen, vanuit welke hoek de grootste dreigingen komen en op welke punten onze digitale samenleving kwetsbaar is. Deze kennis is nodig voor een goede aanpak van cybersecurity, met proportionele acties gericht tegen de juiste dreigingen.

Trends tonen aan dat de afhankelijkheid van ICT aanzienlijk is en dat deze sterk toeneemt door ontwikkelingen als hyperconnectiviteit, cloudcomputing en de mate waarin internet wordt ingezet. De potentiële impact van incidenten wordt hierdoor groter. Digitale spionage en cybercriminaliteit blijven de grootste bedreigingen voor overheid en bedrijfsleven. Burgers zijn bijna even vaak slachtoffer van hacken als van fietsendiefstal. Afgelopen jaar is een criminele cyber dienstensector, waarin hulpmiddelen via «cybercrime-as-a-service» commercieel beschikbaar worden gesteld, nadrukkelijk toegenomen. Daarmee is ook de toegang tot deze hulpmiddelen laagdrempeliger geworden voor verschillende actoren. Burgers, maar ook bedrijven en de overheid zijn regelmatig het slachtoffer van botnets en ransomware. Hoewel botnets veelal gericht zijn op manipulatie van (financiële) transacties, tonen incidenten (zals Pobelka) aan dat de impact van met botnets ontvreemde informatie (als bijvangst) groot kan zijn. De verstoringen van online dienstverlening zijn de

[1] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer

kst-26643-285
ISSN 0921 - 7371
's-Gravenhage 2013

afgelopen periode regelmatig zichtbaar geweest, vooral verstoring als gevolg van DDoS-aanvallen.

De conclusies van het CSBN ondersteunen het grote belang dat het kabinet hecht aan een adequate versterking van cyber security in Nederland, met alle betrokkenen. Dit vergt gezamenlijke inspanningen van overheid, private organisaties en burgers. Om deze reden wordt de Nationale Cyber Security Strategie geactualiseerd waarin een brede cyber security aanpak met private en publieke partijen verder wordt uitgebouwd. In het najaar staat de herziene Nationale Cyber Security Strategie op de agenda van de Ministerraad. Hiermee wordt richting gegeven aan de benodigde acties om de snelle ontwikkelingen in de digitale samenleving bij te houden en continu in te kunnen spelen op de risico's die deze met zich mee brengen.

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