Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2011–2012

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 245

BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 6 juli 2012

Conform de toezegging d.d. 23 december jl. (2011–2012, 26 643, nr. 220) zend ik u hierbij het tweede Cyber Security Beeld Nederland (CSBN)[1]. Het CSBN is opgesteld door het Nationaal Cyber Security Centrum (NCSC). In het CSBN zijn de dreigingen, incidenten, kwetsbaarheden en de genomen maatregelen in hoofdlijnen in beeld gebracht. Ten opzichte van de vorige editie is dit CSBN-2 over de hele linie van dreigingen, weerbaarheid en casuïstiek verbreed. Hiermee worden de eerste stappen gezet voor verdere differentiatie en kwantificering van het Cyber Security Beeld.

Digitale spionage en cybercriminaliteit blijven de grootste dreigingen voor overheid en bedrijfsleven. Gezien de ernst moeten de dreigingen onveranderd de aandacht krijgen. Op hoofdlijnen zijn er geen grote verschuivingen in dreigingen waarneembaar. Wel zijn de handelingen van de hacktivisten, beroepscriminelen en cyberonderzoekers de afgelopen periode zichtbaarder geweest. De overige nieuwe dreigersgroepen (interne actoren en calamiteiten) vormen vooralsnog een lage tot middelmatige dreiging.

Het Kabinet constateert dat de urgentie van de uitdagingen waar wij ons in het kader van cyber security voor gesteld zien, door alle betrokken partijen gedeeld wordt. Zoals wordt toegelicht in de gelijktijdig met dit beeld te verschijnen Voortgangsbrief Nationale Cyber Security Strategie, worden de actielijnen uit de strategie voortvarend aangepakt. In de afgelopen periode is hiermee het fundament gelegd voor een integrale Nederlandse cyber security aanpak. Nu is het zaak voort te bouwen op dit fundament, om in publiek-private, civiel-militaire en (inter)nationale samenwerking te komen tot integraal cyber security management, waarin verantwoordelijkheden helder zijn benoemd en intensievere samenwerking leidt tot synergie. Een belangrijke stap hiertoe is de intensivering van mogelijkheden om digitale aanvallen te detecteren die gericht zijn op de Rijksoverheid en vitale infrastructuren. Ook het vergroten van de weerbaarheid en het versterken van het herstelvermogen zal hier onderdeel uit van moeten maken. Het Kabinet zal zich blijven inspannen

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

kst-26643-245
ISSN 0921 - 7371
's-Gravenhage 2012

voor de implementatie van de Nationale Cyber Security Strategie en het versterken van de publiek-private en internationale samenwerking voor een veilige en vitale digitale samenleving.

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