Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

Vragen gesteld door de leden der Kamer

2013Z03400

Vragen van de leden **Oosenbrug** en **Recourt** (beiden PvdA) aan de minister van Veiligheid en Justitie over *de reactie op een grote botnet-infectie door het Nationaal Cyber Security Centrum* (ingezonden 20 februari 2013).

Vraag 1
Heeft u kennisgenomen van de kritiek van enkele beveiligingsbedrijven op de reactie van de politie en het Nationaal Cyber Security Centrum (NCSC) toen zij op de hoogte gesteld werden van een grootschalige infectie in Nederland door een botnet?[1] Zijn de gegevens in het genoemde artikel over de aangeleverde informatie aan het NCSC en de politie en hun reactie daarop juist? Zo nee, wat is dan de juiste beschrijving van de gebeurtenissen rond deze grote cyber-inbraak?

Vraag 2
Is het correct dat het NCSC de afgelopen week de wens uitgesproken heeft om de ip-adressen van vitale organisaties te krijgen om een betere reactie te kunnen geven bij informatie over inbreuken op de beveiliging? Zo ja, waarom komt dit verzoek juist nu en op welke wijze is dit verzoek aan de betrokken sectoren gedaan?

Vraag 3
Is in dit geval een «notice-and-take-down procedure» gestart door het bedrijf Digital Investigation voor de centrale servers van het botnet? Is het gebruikelijk dat deze procedure in gang gezet wordt door een privaat bedrijf? Welke gevolgen heeft deze procedure gehad voor het traceren van de daders en de schade door het botnet?

Vraag 4
Wordt er op dit moment onderzoek gedaan naar de verantwoordelijken voor dit botnet? Zo ja, wat is de voortgang en de slagingskans van dit onderzoek? Zo nee, waarom niet?

[1] http://webwereld.nl/nieuws/113408/politie-en-ncsc-laks-na-hack-duizenden-bedrijven.html

Vraag 5
Bent u van mening dat het blokkeren van verkeer naar de «command-and-control servers» van botnets een effectieve manier is om deze netwerken te belemmeren? Zo ja, ziet u mogelijkheden om deze werkwijze toe te staan zonder schending van de netneutraliteit?

Vraag 6
Wat is de rolverdeling en afbakening tussen het NCSC en de nieuwe Integrale Beveiligingsdiensten (IBD) en het centrum Abuse Information Exchange (Abuse-IX) van respectievelijk de gemeenten en enkele grote internetbedrijven? Met welke vergelijkbare diensten werkt het NCSC samen?

Vraag 7
Op welke wijze is de relatie georganiseerd tussen het NCSC en vitale sectoren? Welke informatie wordt hierin uitgewisseld en hoe frequent is dit contact? Welke sectoren zijn aangemerkt als vitale sectoren? Herkent u het beeld dat in dit informatietijdperk de informatiesystemen van steeds meer sectoren vitaal zijn?

Vraag 8
Welke plicht hebben bedrijven om aan hun klanten te melden dat hun gegevens mogelijk gestolen zijn, waardoor zij een groot veiligheidsrisico kunnen lopen? Weet u of alle bedrijven die getroffen zijn door het Pobelka-botnet hun klanten ingelicht hebben?

Vraag 9
Deelt u de mening dat de beveiliging van de infrastructuur van vitale sectoren op dit moment nog teveel afhankelijk is van de bereidheid van bedrijven om gegevens te delen en alert te reageren op informatie over beveiligingsproblemen? Zo nee, waarom bent u van mening dat de huidige situatie voldoet? Zo ja, wat ziet u als de beste richting om dit gebrek aan regie op te lossen?

Vraag 10
Herkent u de verwachting dat het NCSC of een onafhankelijke partij een actievere rol op zich neemt bij de melding van inbreuken op de veiligheid van Nederlandse computersystemen? Zo ja, bent u bereid een plan te ontwikkelen waarin een dergelijke partij de digitale veiligheid in Nederland vergroot, zonder de grondrechten van bedrijven en burgers aan te tasten?

Toelichting:

Deze vragen dienen ter aanvulling op eerdere vragen van het lid Gesthuizen (SP), ingezonden 18 februari 2013 (vraagnummer 2013Z03273)