Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

1198

Vragen van het lid **Gesthuizen** (SP) aan de minister van Veiligheid en Justitie over *het lekken van gevoelige informatie door 50.000 harddisks en scanners* (ingezonden 21 december 2012).

Antwoord van minister **Opstelten** (Veiligheid en Justitie) (ontvangen 7 februari 2013) Zie ook Aanhangsel Handelingen, vergaderjaar 2012–2013, nr. 964

Vraag 1
Wat is uw reactie op de uitzending «Zo lek als een mandje» van het programma Reporter waaruit blijkt dat door een gebrek aan beveiliging tienduizenden harddisks, scanners, netwerkschijven en printers toegankelijk zijn via het internet?[1]

Antwoord 1
Ik heb kennis genomen van de uitzending van het programma Reporter. In deze uitzending wordt ingegaan op het feit dat veel burgers en bedrijven naast computers ook andere apparaten aan hun eigen netwerk gekoppeld hebben. Het blijkt dat dergelijke apparatuur in een aantal gevallen vanaf het internet bereikbaar is. Deze apparatuur moet, net als computers, afdoende beveiligd worden tegen misbruik door kwaadwillenden. Het Nationaal Cyber Security Centrum (NCSC) heeft op de eigen website een factsheet[2] geplaatst waar de problematiek in wordt toegelicht. Ook wordt uitgelegd wat men kan doen om vast te stellen of eigen apparaten kwetsbaar zijn voor misbruik vanaf het internet en worden concrete stappen beschreven waarmee eventuele kwetsbaarheden weggenomen kunnen worden. Aangeraden wordt om ervoor te zorgen dat apparatuur niet vanaf het internet bereikbaar is. Indien de bereikbaarheid van apparaten vanaf internet noodzakelijk is, dan dienen er afdoende maatregelen om deze toegang te beveiligen getroffen te worden. Dat is en blijft primair een verantwoordelijkheid voor bedrijven en consumenten zelf.

[1] http://reporter.kro.nl/seizoenen/2012/afleveringen/07-12-2012
[2] https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/factsheets/factsheet-beveilig-apparaten-gekoppeld-aan-internet.html

ah-tk-20122013-1198
ISSN 0921 - 7398
's-Gravenhage 2013

Vraag 2
Deelt u de mening van de diverse experts die in voornoemde uitzending verwoorden dat de producenten van deze apparaten de beveiliging op een juiste manier zouden moeten meeleveren of in ieder geval consumenten zouden moeten informeren over de noodzakelijkheid van beveiliging, in plaats van hopen dat alle consumenten voldoende kennis hebben van privacybeveiliging en hier ook nog de noodzaak van zien? Zo ja, ziet u mogelijkheden voor uzelf om hieraan uitvoering te geven en welke mogelijkheden zijn dat dan?

Antwoord 2
Zoals hierboven is vermeld, hebben bedrijven en consumenten als gebruikers een eigen verantwoordelijkheid om hun apparatuur en bijbehorende instellingen juist in te stellen door zichzelf goed in te laten lichten en de juiste vragen te stellen. Ik ben met u van mening dat leveranciers de verantwoordelijkheid hebben om hun klanten te wijzen op de noodzaak van adequate beveiligingsmaatregelen.
Branche organisatie ICT Nederland heeft in samenwerking met het privaat-publieke programma DigiVeilig/DigiBewust in november 2012 de website «bescherm je bedrijf» gelanceerd, waar bedrijven beveiligingsvragen kunnen doorlopen en praktische handreikingen krijgen. Dit geeft bedrijven een goed inzicht in hun beveiligingsbehoeften, en stelt hen in staat hun rol als opdrachtgever goed in te vullen. Via het programma DigiVeilig zal ook in 2013 voorlichting over veilige apparatuur worden gegeven en worden nieuwe tools en handreikingen voor het MKB en consumenten ontwikkeld.
Dit vrijwaart de leveranciers van de apparatuur echter niet om ook zelf verantwoordelijkheid op te pakken voor het ontwikkelen van intrinsiek veilige hardware en software ten behoeve van de eindgebruikers. Het Ministerie van Economische Zaken voert gesprekken in de sector om te zien of het ontwikkelen van een normenkader en certificering voor veilige software een haalbare kaart is, zodat leveranciers zich kunnen onderscheiden op dit vlak, en veilige software de aandacht krijgt die het verdient. Naar verwachting zal aan het belang van voorlichting en het gebruik van standaarden ook in de aankomende mededeling van de Europese Commissie over Cyber Security aandacht worden besteed.