Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20011 2500 EH Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Directie Cyber Security

Turfmarkt 147
2511 DP Den Haag
Postbus 20011
2500 EA Den Haag
www.nctv.nl

T 070 370 79 11

Ons kenmerk
2145821

Uw Kenmerk
2017Z14446

Datum 24 november 2017
Onderwerp Antwoorden Kamervragen over de artikelen aangaande de onveiligheid van Internet of Things (IoT) in Nederland

Hierbij bied ik u de antwoorden aan op vragen van het lid Kuiken (PvdA) inzake de verschenen artikelen over de onveiligheid van Internet of Things in Nederland. Deze vragen werden ingezonden op 31 oktober 2017 met het kenmerk 2017Z14446.

De Minister van Justitie en Veiligheid,

Ferd Grapperhaus

Directie Cyber Security

Antwoorden van de minister van Justitie en Veiligheid op de vragen van het lid Kuiken (PvdA) over de artikelen aangaande de onveiligheid van Internet of Things (IoT) in Nederland. (ingezonden 31 oktober, nr. 2017Z14446).

Datum
24 november 2017

Ons kenmerk
2145821

Vraag 1
Kent u de berichten "Hackers krijgen ruim baan van u" 1) en "Sophos-onderzoek onthult IoT-risico's: Nederland 'gevoelig' met 4e plaats wereldwijd"?

Antwoord op vraag 1
Ja.

Vraag 2
Hoe komt het dat Nederland zo slecht scoort voor betreft de beveiliging van 'smart-home'-componenten, zoals draadloze raamcontacten, rookmelders, automatische deuropenings- of vergrendelingssystemen en camerasystemen? Waarom is dit in bijna alle andere landen ter wereld beter?

Vraag 3
Was u al eerder op de hoogte van de in de berichten genoemde beveiligingsrisico's? Zo ja, waar blijkt dat uit?

Antwoord op vraag 2 en 3
Nederland scoort in verhouding tot andere landen hoog op het gebied van connectiviteit, het aantal burgers dat toegang tot het internet heeft en gebruikt en daar de vaardigheid voor heeft (CSBN 2017). Dat brengt met zich mee dat het aantal IoT-gebruikers in Nederland naar verhouding eveneens hoog is. Naar aanleiding hiervan is de toenemende dreiging vanuit IoT reeds genoemd in het Cyber Security Beeld Nederland (CSBN) 2017. Het CSBN wordt jaarlijks vastgesteld door de NCTV en biedt inzicht in de belangen, dreigingen, weerbaarheid en daarmee samenhangende ontwikkelingen op het gebied van cybersecurity over de periode mei 2016 tot en met april 2017. Hieruit blijkt ook dat een intensivering van het beleid om deze onveiligheid te bestrijden noodzakelijk is. Zowel de Europese Commissie (EC) als het kabinet onderkennen de noodzaak hiertoe. De EC beziet in dat kader de mogelijkheden van certificering van IoT apparaten. Het kabinet werkt aan de opstelling van een roadmap veilige hard en software, zie verder antwoord 4.

Vraag 4
Deelt u de mening dat door de genoemde beveiligingsrisico's "er kans is dat cybercriminelen die op zoek zijn naar je geld en data makkelijk kunnen binnendringen"? Zo ja, wat doet u concreet om deze risico's te verkleinen of wat gaat u daar aan doen? Zo nee, waarom deelt u die mening niet?

Antwoord op vraag 4
Naast menselijk handelen zijn kwetsbaarheden in hard- en software een achilleshiel van cybersecurity. Om te bevorderen dat IoT-apparaten beter worden beveiligd, stelt het Ministerie van Economische Zaken en Klimaat in samenspraak met het Ministerie van Justitie en Veiligheid en andere departementen en private partijen een roadmap veilige hard- en software op. Hierin wordt bezien welke combinatie van instrumenten effectief bijdragen aan de veiligheid van (het gebruik) van hard- en software. Om onder andere de samenhang met de in het regeerakkoord aangekondigde cybersecuritystrategie te behouden, zal de roadmap voorjaar 2018 aan de Tweede Kamer worden aangeboden.

Het creëren van awareness door middel van voorlichting is en blijft essentieel. Het publiek-private initiatief www.veiliginternetten.nl en de jaarlijkse bewustwordingscampagne Alert Online dragen bij aan het gezamenlijk vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein. De website www.veiliginternetten.nl is het kanaal om gebruikers bewust te maken van verschillende kwetsbaarheden. Daarbij wordt nauw samengewerkt met het NCSC. De website is daarmee een neutrale en betrouwbare plaats om informatie en handelingsperspectieven te vinden.

Bovendien is in het Regeerakkoord structureel 95 miljoen euro gereserveerd voor cybersecurity. De middelen worden onder andere ingezet voor de uitbreiding van personele capaciteit en ICT-voorzieningen en verdeeld over de departementen Justitie en Veiligheid (NCTV), Defensie (MIVD), Binnenlandse Zaken en Koninkrijksrelaties (AIVD), Buitenlandse Zaken, Infrastructuur en Milieu en Economische Zaken en Klimaat. Een deel van dit geld zal op bredere voorlichtingcampagnes op dit onderwerp worden ingezet.

Vraag 5
Zijn u aangiftes bekend van particulieren of bedrijven die slachtoffer zijn geworden van hackers die misbruik hebben gemaakt van slecht beveiligde webinterfaces van 'Internet-of-Things'-apparatuur? Zo ja, om hoeveel aangiften gaat het? Bezit de politie voldoende expertise om daar mee om te gaan?

Antwoord op vraag 5
Aangiften van particulieren en bedrijven die het slachtoffer zijn van cybercriminelen worden onder meer geregistreerd als computervredebreuk (hacking) of als het ontoegankelijk maken van een geautomatiseerd werk (bijvoorbeeld in het geval van ransomware, of een DDoS-aanval). Of bij het binnendringen of het ontoegankelijk maken door criminelen gebruik is gemaakt van slecht beveiligde IoT-apparatuur wordt niet als zodanig geregistreerd.

In algemene zin geldt dat in het geval van een lage digitale weerbaarheid het risico om slachtoffer te worden van cybercrime toeneemt. Cybercriminelen kiezen immers meestal de weg van de minste weerstand teneinde maximaal effect te kunnen sorteren. IoT-apparaten vertonen daarbij relatief vaak kwetsbaarheden die misbruikt kunnen worden. Hierbij kunnen IoT-apparaten doelwit zijn, maar ook ingezet worden als middel, bijvoorbeeld als onderdeel in een DDoS-aanval.

De politie heeft in de afgelopen jaren haar digitale expertise en de capaciteit voor de aanpak van cybercrime uitgebreid. Met de beschikbaar gestelde gelden uit de Miljoenennota en het Regeerakkoord vindt vanaf 2018 een verdere versterking plaats.

1)_https://eenvandaag.avrotros.nl/item/hackers-krijgen-ruim-baan-van-u/

2) https://www.emerce.nl/wire/sophosonderzoek-onthult-iotrisicos-nederland-gevoelig-4e-plaats-wereldwijd