Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2017–2018

Aanhangsel van de Handelingen

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

1346

Vragen van de leden **Van Toorenburg** (CDA) en **Verhoeven** (D66) aan de Ministers van Justitie en Veiligheid en van Economische Zaken en Klimaat over *het bericht «Experts: overheid moet ingrijpen bij internetapparaten»* (ingezonden 17 januari 2018).

Antwoord van Minister **Grapperhaus** (Justitie en Veiligheid), mede namens de Staatssecretaris van Economische Zaken en Klimaat (ontvangen 7 maart 2018). Zie ook Aanhangsel Handelingen, vergaderjaar 2017–2018, nr. 1097.

Vraag 1
Bent u bekend met het artikel «Experts: overheid moet ingrijpen bij internetapparaten»?[1]

Antwoord 1
Ja.

Vraag 2, 3 en 4
Hoe beoordeelt u de oproep van Amerikaanse internetexperts om de op dit moment gebrekkige beveiliging van op internet aangesloten apparaten te verbeteren?
Ziet u mogelijkheden om de verkoop van onvoldoende veilige internetapparaten beter te reguleren, bijvoorbeeld door de verkoop van bewezen onveilige apparaten in Nederland te verbieden?
Bent u bereid te pleiten voor een Europees keurmerk dat dient ter waarborging van de veiligheid van internetapparaten? Zo nee, waarom niet?

Antwoord 2, 3 en 4
Het beeld dat de Amerikaanse internetexperts schetsen is herkenbaar. Zoals reeds in de beantwoording van Kamervragen over de onveiligheid van «Internet of Things» in Nederland[2] is aangegeven is «de toenemende dreiging vanuit aan internet aangesloten apparaten oftewel IoT reeds genoemd in o.a. 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.

[1] Algemeen Dagblad, 8 januari 2018
[2] Aanhangsel Handelingen, vergaderjaar 2017–2018, nr. 530

ah-tk-20172018-1346
ISSN 0921 - 7398
's-Gravenhage 2018

Hieruit blijkt ook dat een intensivering van het beleid om deze onveiligheid te bestrijden noodzakelijk is. Zowel de Europese Commissie (EC) als het kabinet onderkent de noodzaak hiertoe».
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, andere departementen en private partijen thans een roadmap veilige hard- en software op. Hierin wordt bezien welke combinatie van instrumenten effectief bijdraagt aan de veiligheid van (het gebruik) van hard- en software, zoals bewustwording, certificering en aansprakelijkheid. Bij deze analyse wordt onder meer het recente advies[3] inzake de cybersecurity van Internet of Things (IoT) van de Cyber Security Raad betrokken. Om onder andere de samenhang met de in het regeerakkoord aangekondigde cybersecuritystrategie te behouden, zal de roadmap in dit voorjaar naar verwachting aan de uw Kamer worden aangeboden.
Op 13 september 2017 heeft de Europese Commissie een ontwerpverordening[4] gepubliceerd, waarin de Commissie onder meer een voorstel doet voor het inrichten van een Europees kader voor cyberbeveiligingscertificering voor ICT-producten en -diensten. In het BNC-fiche van 20 oktober 2017[5] over deze ontwerpverordening, heeft het kabinet aangegeven dat het voorstel van de Europese Commissie aansluit bij de Nederlandse inzet op het gebied van de digitale interne markt en de rol van certificering. Maar zoals in het BNC-fiche wordt weergegeven zijn er ook aandachtspunten. Deze worden in de inmiddels lopende onderhandelingen ingebracht.

Vraag 5
In hoeverre richten bewustwordingscampagnes als Alert Online en www.veiliginternetten.nl op de gevaren van internetapparaten? Kan een gerichte bewustwordingscampagne over dit onderwerp van nut zijn? Zo nee, waarom niet?

Antwoord 5
De ministeries van Justitie en Veiligheid en van Economische Zaken en Klimaat zetten al regelmatig middelen zoals voorlichtingscampagnes in om de bewustwording rondom digitale veiligheidsrisico's en wat daartegen gedaan kan worden te vergroten. Zo is er de voorlichtingscampagne Alert Online, een initiatief dat de overheid, het bedrijfsleven, onderwijs, wetenschap en consumenten in Nederland faciliteert en stimuleert samen te werken aan cybersecurity én hen meer cyber secure te laten handelen. Een ander voorbeeld is het publiek-private initiatief Veiliginternetten.nl waarin de overheid samenwerkt met het bedrijfsleven aan de weerbaarheid van de Nederlandse samenleving in het digitale domein. De website www.veiliginternetten.nl is het kanaal om burgers en bedrijfsleven voor te lichten over en handelingsperspectieven te bieden voor (het voorkomen van) ICT-incidenten als malware en softwarelekken, maar ook ze bewust te maken van verschillende kwetsbaarheden.
In het regeerakkoord is structureel 95 miljoen euro gereserveerd voor cybersecurity, verdeeld over de departementen Justitie en Veiligheid (NCTV), Defensie (MIVD), Binnenlandse Zaken en Koninkrijksrelaties (AIVD), Buitenlandse Zaken, Infrastructuur en Waterstaat en Economische Zaken en Klimaat. Een deel van dit geld zal worden ingezet voor bredere voorlichtingscampagnes over dit onderwerp. Daarnaast zal in de eerdergenoemde roadmap digitaal veilige hard- en software ook het instrument bewustwordingscampagnes een plaats hebben.

Vraag 6
Hoe is de aansprakelijkheid van producenten van onveilige internetapparaten op dit moment geregeld? Kunnen producenten van onveilige apparaten aansprakelijk worden gesteld voor geleden schade veroorzaakt door botnets die gebruik maken van deze apparaten? Zo nee, dient de wetgeving dan niet aangepast te worden?

---

[3] «Naar een veilig verbonden digitale samenleving» Advies inzake de cybersecurity van Internet of Things (IoT), Cyber Security Raad, januari 2018
[4] Verordening agentschap ENISA en Europees kader voor Cyberbeveiligingscertifcering
[5] Kamerstuk 22 112, nr. 2405

Vraag 6
Hoe is de aansprakelijkheid van producenten van onveilige internetapparaten op dit moment geregeld? Kunnen producenten van onveilige apparaten aansprakelijk worden gesteld voor geleden schade veroorzaakt door botnets die gebruik maken van deze apparaten? Zo nee, dient de wetgeving dan niet aangepast te worden?
De regeling van productaansprakelijkheid betreft implementatie van een EU-richtlijn (Richtlijn 85/374/EEG). De richtlijn is in 2017 geëvalueerd. Daarbij is ook de toepassing van de richtlijn op moderne technologieën onderzocht. IoT-apparaten zijn daarbij expliciet genoemd. De Europese Commissie verwacht de uitkomsten van de evaluatie in april 2018 vast te stellen. Dit is bij uitstek een grensoverschrijdend onderwerp. Het kabinet zal de uitkomsten aangrijpen om in EU-verband te beoordelen of het wenselijk is dat de regeling van productaansprakelijkheid wordt aangepast met het oog op nieuwe technologieën, zoals IoT-apparaten. Daarnaast zal in de eerdergenoemde roadmap digitaal veilige hard- en software ook aansprakelijkheid een plaats hebben.