Ministerie van Economische Zaken
en Klimaat

> Retouradres Postbus 20401 2500 EK Den Haag

De Voorzitter van de Tweede Kamer
der Staten-Generaal
Binnenhof 4
2513 AA DEN HAAG

Directoraat-generaal Energie, Telecom & Mededinging
Directie Telecommarkt

Bezoekadres
Bezuidenhoutseweg 73
2594 AC Den Haag

Postadres
Postbus 20401
2500 EK Den Haag

Overheidsidentificatienr
00000001003214369000

T 070 379 8911 (algemeen)
F 070 378 6100 (algemeen)
www.rijksoverheid.nl/ezk

Datum 29 juni 2018
Betreft Beantwoording vragen over het bericht 'Agentschap Telecom slaat alarm over hackbare apparaten'

Ons kenmerk
DGETM-TM / 18136935

Uw kenmerk
2018Z10731

Geachte Voorzitter,

Hierbij stuur ik u, mede namens de minister van Justitie en Veiligheid en de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties, de beantwoording toe op de vragen van de Leden Weverling, Arno Rutte, Middendorp en Wörsdörfer (allen VVD) over het bericht 'Agentschap Telecom slaat alarm over hackbare apparaten'.

Hoogachtend,

mr. drs. M.C.G. Keijzer
Staatssecretaris van Economische Zaken en Klimaat

Directoraat-generaal Energie, Telecom & Mededinging
Directie Telecommarkt

Ons kenmerk
DGETM-TM / 18136935

2018Z10731

Vragen van de leden Weverling, Arno Rutte, Middendorp en Wörsdörfer (allen VVD) aan de minister van Justitie en Veiligheid en de staatssecretarissen van Binnenlandse Zaken en Koninkrijksrelaties en van Economische Zaken en Klimaat over het bericht 'Agentschap Telecom slaat alarm over hackbare apparaten' (ingezonden 7 juni 2018).

1
Kent u het bericht 'Agentschap Telecom slaat alarm over hackbare apparaten'?[1]

Antwoord
Ja, dat bericht is bekend.

2
Kunt u zich vinden in de uitspraak van het Agentschap Telecom (AT) dat er haast gemaakt moet worden met een keurmerk voor veilige apparaten? Zo nee, waarom niet?

Antwoord
Het Agentschap Telecom (AT) houdt in de Staat van de Ether 2017[2] een pleidooi voor de snelle invoering in Europa van minimumeisen aan met internet verbonden apparatuur (IoT) via een CE-markering (of keurmerk). Ik deel dit pleidooi gezien de enorme groei van (onveilige) IoT-apparatuur. Vandaar dat ik deze oplossingsrichting ook noem in de Roadmap Digitaal Veilige Hard- en Software[3]. Omdat er niet één maatregel bestaat die de digitale veiligheid van IoT-apparatuur kan realiseren, bevat de roadmap een mix van maatregelen.

3
Eerder heeft u aangegeven dat u bezig bent met een keurmerk voor veilige apparaten, kunt u aangeven hoe dit proces vordert? Wanneer verwacht u een voorstel te kunnen doen?

4
Deelt u de mening van het AT dat het CE-keurmerk als voorbeeld zou kunnen dienen voor een keurmerk voor veilige 'slimme' apparaten? Zo nee, waarom niet?

Antwoord 3 en 4
Het CE-keurmerk waar het AT op doelt, is gebaseerd op de Radio Equipment Directive (RED). De RED schrijft eisen voor waar (radio)apparatuur aan moet voldoen om het Europese keurmerk CE te mogen dragen. AT is toezichthouder op de RED. De voorschriften gaan tot dusver over zaken als gebruiksveiligheid, het voorkomen van interferentie en storingsgevoeligheid. De RED biedt daarnaast de

[1] https://nos.nl/artikel/2234933-agentschap-telecom-slaat-alarm-over-hackbare-apparaten.html
[2] https://magazines.agentschaptelecom.nl/staatvandeether/2018/01/index
[3] TK 26643, nr.535

mogelijkheid om, na activering door de Europese Commissie, minimale eisen te stellen aan de digitale veiligheid van draadloze apparaten. Het kan daarmee dan ook dienen als keurmerk voor veilige 'slimme' draadloze apparaten.

Met de Europese Commissie onderzoekt het kabinet hoe invulling te gegeven aan voornoemde mogelijkheid om het huidige CE-keurmerk van de RED uit te breiden met minimale eisen aan de digitale veiligheid van draadloze apparaten. Nederland heeft daartoe onlangs in Europa een voorstel gedaan. De Commissie heeft positief op dit voorstel gereageerd en overweegt om als eerste stap veiligheidseisen voor bepaalde productcategorieën versneld in te voeren. Dit is een belangrijke eerste stap. Daarbij is de Nederlandse inzet dat op de langere termijn alle met internet verbonden apparatuur moet voldoen aan minimale eisen ten aanzien van de digitale veiligheid (security by design).

5
Wordt in de ontwikkeling van het keurmerk voor veilige apparaten ook nagedacht over hoe voor consumenten zo zichtbaar en duidelijk mogelijk kan worden gemaakt welke 'slimme' apparaten veilig zijn en welke niet, aangezien dit volgens het AT vaak niet zichtbaar is? Zo nee, waarom niet?

Antwoord
Het CE-keurmerk op basis van de RED betekent dat alle apparaten die onder deze richtlijn vallen aan de minimumeisen moeten voldoen. Onveilige apparatuur die niet aan de minimum eisen voldoet, kan door de toezichthouder (het AT) van de markt worden verwijderd. Als de regelgeving van de RED wordt uitgebreid met veiligheidseisen voor digitale veiligheid, is het CE-keurmerk daarvoor ook geldend. De CE markering (in de vorm van een CE-logo) moet op ieder apparaat aangebracht zijn. AT houdt toezicht of dit ook terecht gebeurt.

6
Ziet u voldoende kansen voor telecommunicatie- en internetproviders om hun netwerk af te speuren naar onveilige apparaten? Zo nee, waarom niet?

Antwoord
Aanbieders van internettoegang kunnen vanuit hun beheerstaak van de internetverbinding een rol spelen bij het terugdringen van digitale kwetsbaarheden. In dialoog met aanbieders van internettoegang wordt bekeken hoe zij, analoog aan de succesvolle aanpak van botnets, een bijdrage kunnen leveren aan de bestrijding van onveilige apparaten.

7
Vindt u het wenselijk dat bedrijven zelf met een keurmerk zouden komen, zoals het AT suggereert? Zo nee, waarom niet?

Antwoord
Mijn voorkeur gaat uit naar een Europees keurmerk, zoals het eerdergenoemde CE-keurmerk met verplichte minimumeisen. Dit is het meest effectief en draagt bij

aan de Digitale Interne Markt (het voorkomt versnippering en verstoring van het level playing field). Totdat zo'n keurmerk er is, kan de overheid geen toezicht houden om zo nodig producten van de markt te weren. De roadmap bevat mede daarom meerdere maatregelen om onveilige producten samen met bedrijven aan te pakken. Zoals standaardisering en certificering. Met de Cybersecurity Act wordt op Europees niveau gewerkt aan een raamwerk voor (vrijwillige) cybersecurity certificatie. Uw Kamer is onlangs, voorafgaand aan de Telecomraad van 8 juni, geïnformeerd over de Cybersecurity Act[4]. Dat raamwerk biedt bedrijven de mogelijkheid om Europese standaarden en certificaten te (helpen) ontwikkelen voor specifieke producten, processen of diensten. Bedrijven kunnen er vervolgens voor kiezen om hun product, proces of dienst vrijwillig te laten certificeren tegen de bij een certificaat behorende eisen.

8
Deelt u de mening dat het snel en actief invoeren van een keurmerk voor 'slimme' apparaten nodig is om innovaties, ontwikkelingen en ondernemerschap te stimuleren? Zo nee, waarom niet?

Een keurmerk kan het maatschappelijk verantwoord innoveren stimuleren als het zo wordt ingericht dat apparaten digitaal veiliger worden en er ruimte blijft voor innovatie, het meenemen van ontwikkelingen en ondernemerschap.

[4] Kamerstuk 21501-33, nr. 706