Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

Aanhangsel van de Handelingen

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

2007

Vragen van de leden **Buitenweg** (GroenLinks) en Verhoeven (D66) aan de Minister voor Rechtsbescherming over *de privacyrisico's van onveilige beveiligingscamera's* (ingezonden 28 januari 2020).

Antwoord van Minister **Dekker** (Rechtsbescherming) (ontvangen 9 maart 2020). Zie ook Aanhangsel Handelingen, vergaderjaar 2019–2020, nr. 1755.

Vraag 1
Kent u de uitzending van Pointer, waaruit blijkt dat honderden beveiligingscamera's eenvoudig te lokaliseren en te hacken zijn? Zo ja, wat vindt u van dit bericht?[1]

Antwoord 1
Ja.
Het is een zorgelijke ontwikkeling dat het gebruik van bepaalde beveiligingscamera's negatieve gevolgen kan hebben voor de veiligheid en de persoonlijke levenssfeer van de betrokkenen.

Vraag 2
Welke eisen worden aan dergelijke camera's gesteld? Deelt u de mening dat deze camera's alleen op de Nederlandse markt mogen worden toegelaten als is komen vast te staan dat ze adequaat zijn beschermd tegen (online) hacks? Zo ja, welke maatregelen stelt u zich voor om het beveiligingsniveau van beveiligingscamera's te verbeteren? Wat vindt u bijvoorbeeld van het in de uitzending genoemde idee om een minimumstandaard voor online veiligheid in te stellen en eenvoudig te hacken rommelproducten te verbieden?

Antwoord 2
In de uitzending van Pointer gaat het om camera's die met het internet zijn verbonden en door middel van het IP-adres gemakkelijk te lokaliseren zijn, zogenoemde IP-camera's. Nederlandse en Europese wet- en regelgeving stellen thans geen digitale veiligheidseisen aan IP-camera's. Nederland maakt zich in de Europese Unie (EU) wel sterk voor het stellen van wettelijke minimum digitale veiligheidseisen aan IoT-apparaten, zoals IP-camera's, via

[1] Pointer, 24 januari 2020, https://pointer.kro-ncrv.nl/artikelen/honderden-nederlandse-beveiligingscameras-zijn-onveilig

ah-tk-20192020-2007
ISSN 0921 - 7398
's-Gravenhage 2020

de Europese richtlijn voor radioapparatuur,[2] welke zijn geïmplementeerd via de Telecommunicatiewet. Apparaten die niet aan de minimumeisen voldoen, kunnen dan van de markt worden geweerd en gehaald. In Nederland houdt het Agentschap Telecom toezicht op deze richtlijn. Op initiatief van Nederland wordt momenteel in EU-verband gekeken naar de invulling van de minimumeisen. Nederland zal de komende periode een aanjagende rol blijven vervullen om ervoor te zorgen dat de minimumeisen in 2020 van kracht worden in de hele EU.[3]

Vraag 3
Is u bekend in hoeveel gevallen per jaar sprake is van gehackte beveiligingscamera's? Hoe vaak wordt daarvan melding gedaan bij de Autoriteit Persoonsgegevens en bij de politie? In hoeveel gevallen wordt politieonderzoek ingesteld en in hoeveel gevallen vindt strafvervolging en veroordeling plaats? Vindt u dat sprake is van een adequaat handhavingsniveau op de bescherming van burgers tegen dit soort vormen van online criminaliteit?

Antwoord 3
Het totaal aantal gevallen per jaar waarbij sprake is van gehackte beveiligingscamera's is mij niet bekend. Wel heeft de Autoriteit Persoonsgegevens mij laten weten dat sinds de meldplicht datalekken in Nederland van toepassing is, zij tussen 1-1-2016 en 28-1-2020 zeven datalekmeldingen heeft ontvangen waarbij sprake was van (mogelijk) gehackte beveiligingscamera's. De politie heeft gemeld dat zij geen cijfers beschikbaar heeft over het aantal meldingen van gehackte beveiligingscamera's. Gehackte beveiligingscamera's worden niet als aparte delicten in de politiesystemen geregistreerd. Om die reden is niet bekend in hoeveel gevallen politieonderzoek wordt ingesteld en in hoeveel gevallen strafvervolging en veroordeling plaatsvindt en kan eveneens geen uitspraak worden gedaan over de adequaatheid van het handhavingsniveau.

Vraag 4
Bent u bereid om, samen met de Staatssecretaris van Economische Zaken, producenten bewust te maken van de noodzaak van «privacy by design and default» om te voorkomen dat persoonsgegevens na een hack kunnen uitlekken? Zo ja, welke maatregelen stelt u zich daarbij voor?

Antwoord 4
Artikel 25 van de Algemene verordening gegevensbescherming kent een verplichting voor producenten om «privacy by design and default» toe te passen op hun producten. Deze verplichting geldt ook voor producenten van beveiligingscamera's. Producenten dienen daaraan gevolg te geven, om te voorkomen dat persoonsgegevens na een hack kunnen uitlekken. Producenten dienen zich in dat verband af te vragen of zij de juiste eisen stellen aan de aanbieders en ontwikkelaars van die producten. Daarnaast kan de Autoriteit Persoonsgegevens producenten wijzen op de noodzaak van «privacy by design and default». Ik zie het niet als mijn taak om samen met de Staatssecretaris van Economische Zaken de bewustwording van producenten over de noodzaak van «privacy by design and default» te versterken, dit is aan de AP en de producenten zelf. Wel zet Nederland zich in EU-verband, als reeds aangegeven, in voor het stellen van minimumeisen aan IoT-apparaten.

[2] The Radio Equipment Directive 2014/53/EU (RED)
[3] Kamerstuk 26 643, nr. 618.