Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

Aanhangsel van de Handelingen

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

2801

Vragen van het lid **Buitenweg** (GroenLinks) aan de Minister van Justitie en Veiligheid en de Staatssecretaris van Economische Zaken en Klimaat over *het bericht dat Huawei toegang had tot gegevens van miljoenen Telfort-klanten* (ingezonden 30 maart 2021).

Antwoord van Staatssecretaris **Keijzer** (Economische Zaken en Klimaat), mede namens de Minister van Justitie en Veiligheid (ontvangen 19 mei 2021). Zie ook Aanhangsel Handelingen, vergaderjaar 2020–2021, nr. 2407.

Vraag 1
Bent u bekend met het artikel «Huawei had toegang tot gegevens miljoenen Telfort-klanten»?[1]

Antwoord 1
Ja, ik ben met het artikel bekend.

Vraag 2, 3 en 4
Wat is uw reactie op deze berichtgeving, die erop wijst dat Huawei toegang had tot de klant- en facturatiegegevens van miljoenen Telfort abonnees? Klopt het dat uit het aangehaalde KPN-rapport blijkt dat Huawei geregeld bestanden uit de klantomgeving van Telfort haalde? Zo ja, wat is uw reactie op de verklaring van hetzelfde bedrijf dat er geen enkele aanleiding is om te veronderstellen dat er gegevens van Telfort-klanten waren ontvreemd, door wie dan ook? Bent u bereid om hier bij KPN opheldering over te vragen? Kunt u helder uiteenzetten tot welke specifieke datavariabelen Huawei precies toegang had?

Antwoord 2, 3 en 4
Aanleiding van het artikel is een intern audit-rapport van KPN uit 2011 waarin KPN een reguliere audit doet naar de beveiliging van een destijds nieuw systeem van Telfort, toen onderdeel van KPN, waarop klant- en facturatiegegevens (zoals persoons- en verkeersgegevens) werden bewaard. KPN heeft ons gemeld dat het Amerikaanse bedrijf HP hoofdaannemer was voor de realisatie van het systeem en diverse onderaannemers gebruikte, waaronder

[1] Volkskrant, 29 maart 2021, «Huawei had onbeperkt toegang tot gegevens miljoenen Telfort-klanten», https://www.volkskrant.nl/nieuws-achtergrond/huawei-had-onbeperkt-toegang-tot-gegevens-miljoenen-telfort-klanten~b7248794/

ah-tk-20202021-2801
ISSN 0921 - 7398
's-Gravenhage 2021

Huawei, voor de bouw en het beheer. Uit dat rapport zou blijken dat beveiligingsmaatregelen niet op orde waren, zoals logging en monitoring van wie toegang heeft tot het systeem en wie wat met de gegevens doet. Uit het rapport kwam een groot aantal verbeterpunten waarvan de meeste waren gericht aan HP als hoofdaannemer. Volgens KPN zijn alle verbetermaatregelen in de jaren erna opgevolgd. Huawei had als leverancier toegang tot het systeem voor reguliere beheer- en onderhoudsactiviteiten. Ons is niet bekend of via deze beheertoegang klantgegevens zijn ontvreemd. Navraag bij KPN leert dat dit KPN niet is gebleken. Het systeem is in het voorjaar van 2018 vervangen.

Vraag 5
Is het denkbaar dat de Chinese autoriteiten op deze manier, via Huawei, de Oeigoerse diaspora of andere specifieke groepen in beeld konden brengen of konden volgen?

Antwoord 5
Het is ons niet bekend of, voor zover sprake is geweest van ontvreemding van klantgegevens, Chinese autoriteiten op deze manier Oeigoerse diaspora of andere groepen in beeld konden brengen of konden volgen. In algemene zin is bekend dat statelijke actoren zich richten op het vergaren van (onder meer) persoonsgegevens voor het monitoren en profileren van doelwitten. Daarbij is bekend dat de inlichtingen- en beïnvloedingsactiviteiten van China zich mede op zijn diaspora richten. Ongewenste buitenlandse beïnvloeding en inmenging hebben de aandacht van het kabinet en de inlichtingen- en veiligheidsdiensten in het bijzonder. Op het moment dat concrete activiteiten in dat verband worden waargenomen, wordt bezien of passende maatregelen nodig en mogelijk zijn.

Vraag 6, 7 en 8
Welke acties zijn ondernomen in 2019 toen medewerkers van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en specialisten van KPN een verborgen toegangspad naar klantgegevens ontdekten waar alleen Huawei bij kon?
Is het bestaan van dat toegangspad destijds gemeld bij de Autoriteit Persoonsgegevens? Zo nee, waarom niet?
Is destijds bij Huawei om opheldering gevraagd over het ontdekte toegangspad? Zo ja, door wie, en wat was de reactie? Zo nee, waarom niet? Op welke wijze is het toegangspad gesloten? In hoeverre is het aanbrengen van geheime toegangspaden in strijd met de wet?

Antwoord 6, 7 en 8
Het kabinet doet in het openbaar geen uitspraken over het kennisniveau of de activiteiten van de Nederlandse inlichtingen- en veiligheidsdiensten.
In het algemeen kan gesteld worden dat de Telecommunicatiewet sinds 2012 een zorgplicht kent die ertoe strekt dat aanbieders van openbare telecommunicatienetwerken en -diensten passende technische en organisatorische maatregelen dienen te nemen om de risico's voor de veiligheid en de integriteit van hun netwerken en diensten te beheersen. In het kader van die zorgplicht past het niet dat er toegangspaden tot een netwerk en diensten bestaan die niet zijn geautoriseerd of gecontroleerd door de desbetreffende aanbieder van openbare telecommunicatienetwerken en -diensten. Het ongeautoriseerd aanbrengen van geheime toegangspaden kan daarnaast een verdenking opleveren van een misdrijf als bedoeld in de artikelen 350c Sr en/of 138ab Sr.

Vraag 9
Klopt het dat het bewuste klantsysteem momenteel niet meer in gebruik is? Tot wanneer was het systeem wel in gebruik?

Antwoord 9
Het klopt dat dit bewuste klantsysteem, uit het audit rapport van 2011, momenteel niet meer in gebruik is. Het betreft hier een oud klantsysteem van Telfort. Het systeem was in gebruik tot voorjaar 2018.

Vraag 10 en 11
Kunt u uitsluiten dat Huawei op dit moment dergelijke toegang heeft tot klantgegevens van Nederlandse burgers? Hoe wordt voorkomen dat dit weer kan gebeuren? In hoeverre is de logging van toegang tot klantgegevens van telecombedrijven nu verplicht?
Deelt u de mening van hoogleraar Bas Jacobs, tevens lid van de Cyber Security Raad, dat het interne KPN-rapport ook iets zegt over de wijze waarop Huawei in het algemeen haar producten aanlevert, dat het bedrijf zichzelf een plek diep in de geleverde systemen verschaft? Zo ja, is het dan verantwoord om Huawei een rol te laten spelen in het aanleggen van 5G-netwerken? Zo nee, waarom niet?

Antwoord 10 en 11
Wij kunnen aan de hand van een intern KPN-rapport uit 2011 geen conclusies verbinden over hoe Huawei in het algemeen producten aanlevert. Het kabinet neemt actief maatregelen om de weerbaarheid van telecommunicatienetwerken te verhogen en misbruik via leveranciers van producten en diensten tegen te gaan. In 2019 heeft de Taskforce Economisch Veiligheid (TFEV), met medewerking van de drie mobiele netwerk operators (KPN, T-Mobile en VodafoneZiggo) een risicoanalyse naar de kwetsbaarheid van de netwerken voor dergelijk misbruik uitgevoerd. Uw Kamer is op 1 juli 2019 geïnformeerd over de uitkomsten hiervan. Op basis van deze analyse heeft het kabinet besloten tot het nemen van de volgende drie maatregelen:
1) Mobiele netwerk operators worden bij ministeriële regeling verplicht om aanvullende technische en organisatorische beveiligingsmaatregelen te nemen om de weerbaarheid van de mobiele telecomnetwerken te verhogen.
2) Mobiele netwerk operators worden bij beschikking verplicht om in de kritieke onderdelen van hun netwerk uitsluitend gebruik te maken van producten en diensten van vertrouwde leveranciers.
3) De werkwijze van de Taskforce Economische Veiligheid wordt bestendigd in een structureel proces waarbinnen betrokken overheidsorganisaties en telecomaanbieders doorlopend dreigingsinformatie delen en op basis daarvan risicobeoordelingen uitvoeren waar nodig.

Voor de eerste twee genoemde maatregelen is een grondslag gecreëerd in het Besluit veiligheid en integriteit telecommunicatie, met daarin nadere regels met betrekking tot de in het antwoord op vraag 6–8 genoemde zorgplicht voor telecomaanbieders krachtens de Telecommunicatiewet. De derde maatregel is essentieel om de telecomnetwerken ook in de toekomst veilig te houden.
De standaarden op het gebied van veiligheid die in de praktijk in het kader van deze zorgplicht worden gehanteerd door telecomaanbieders, en worden getoetst door de toezichthouder (Agentschap Telecom), zijn er mede op gericht te voorkomen dat onbevoegden in systemen kunnen komen. Specifieke eisen aan toegang tot systemen, zoals autorisatie, monitoring en logging, ongeacht de leverancier, zijn daar onderdeel van.

Vraag 12
Was u al op de hoogte van dit rapport, of is deze informatie nieuw voor u? In hoeverre waren de bevindingen van het rapport al meegenomen in het structurele proces ten aanzien van de risicobeoordeling van kwetsbaarheden van de netwerken van telecomaanbieders?

Antwoord 12
Wij waren niet op de hoogte van dit rapport. Van belang is om te realiseren dat het hier gaat om een bedrijfsintern rapport uit 2011. Het feit dat KPN dit type audits liet uitvoeren geeft inzage in de wijze waarop KPN invulling geeft aan de toetsing van haar eigen systemen. In de eerder benoemde risicoanalyse van de TFEV is het risico op ongeautoriseerde toegang tot systemen en data en hoe misbruik daarvan te voorkomen meegenomen.

Vraag 13
Deelt u de mening dat dit interne KPN-rapport laat zien dat het onverstandig is om gebruik te maken van andere dan volledig betrouwbare leveranciers in het telecomnetwerk, niet alleen in de kritieke delen van het netwerk, maar ook in het radio en antennenetwerk? Zo nee, waarom niet?

Antwoord 13
Op basis van de eerdergenoemde risicoanalyse van de TFEV is besloten om mobiele netwerk operators bij beschikking te verplichten om in kritieke onderdelen van hun netwerken enkel gebruik te maken van vertrouwde leveranciers. Het kabinet doet geen openbare uitspraken welke onderdelen als kritiek zijn aangemerkt. Er is op dit moment geen noodzaak om eenzelfde verplichting op te leggen voor het gehele netwerk. Eén van de maatregelen die het kabinet heeft genomen naar aanleiding van de eerder genoemde risicoanalyse van de TFEV in 2019 is het inrichten van een structureel proces, waarin nieuwe informatie over dreiging en technologie wordt beoordeeld door overheid en de telecomsector samen. Als daar aanleiding toe is, kunnen er op basis van dit structurele proces aanvullende veiligheidsmaatregelen genomen worden.