Ministerie van Economische Zaken
en Klimaat

> Retouradres Postbus 20401 2500 EK Den Haag

De Voorzitter van de Tweede Kamer
der Staten-Generaal
Prinses Irenestraat 6
2595 BD DEN HAAG

Datum 30 augustus 2022
Betreft Onderzoek Agentschap Telecom bij KPN

Geachte Voorzitter,

Tijdens het plenair debat van 29 juni 2021 over buitenlandse spionage in telecomnetwerken heeft de toenmalige staatssecretaris van Economische Zaken toegezegd de Kamer te informeren over de uitkomst van een onderzoek van het Agentschap Telecom (AT) bij KPN. Met deze brief kom ik aan deze toezegging tegemoet.

Aanleiding voor het onderzoek door AT was een artikel in de Volkskrant van 17 april 2021. Daarin werd, op basis van een rapport uit 2010, gesuggereerd dat er 'ongeautoriseerde, ongecontroleerde en ongelimiteerde' toegang was tot de mobiele netwerken van KPN. In de bijlage treft u het persbericht van AT aan met de belangrijkste bevindingen van haar onderzoek. Naast dit persbericht publiceert AT op haar website[1] nadere informatie over de aanpak en bevindingen van het onderzoek.

Het is van groot belang dat onze telecomnetwerken veilig en integer zijn. Dit principe ligt verankerd in de zorgplicht die is opgenomen in de Telecommunicatiewet. De zorgplicht stelt dat aanbieders passende technische en organisatorische maatregelen moeten nemen om hun risico's te beheersen. Hierbij is een grote eigen verantwoordelijkheid bij de aanbieders neergelegd hoe zij dat precies invullen. Zij hebben immers het beste zicht op hun systemen en de

[1] https://www.agentschaptelecom.nl/

dagelijkse risico’s waar zij mee van doen krijgen. Het AT houdt toezicht op de naleving van die zorgplicht.

Vanuit de toegenomen zorg over spionage in de telecomsector is de afgelopen jaren onder leiding van de Taskforce Economische Veiligheid gewerkt aan aanvullende maatregelen om risico’s die samenhangen met ongeautoriseerde toegang door derden beter te beheersen (Kamerstuk 30821, nrs. 92 en 143). Hiermee worden zwaardere eisen gesteld aan de beveiliging van onze telecomnetwerken. In het verlengde daarvan zijn meer middelen beschikbaar gesteld aan het AT voor bijpassend geïntensiveerd toezicht.

Deze nieuwe wettelijke instrumenten vormen samen met de bestaande bepalingen uit de Telecommunicatiewet en een versterkt AT belangrijke stappen om de weerbaarheid van de telecomsector te versterken tegen actuele dreigingen.

Desgewenst kunt u een vertrouwelijke briefing krijgen waarin de aanpak en bevindingen van het AT onderzoek nader kunnen worden toegelicht.

M.A.M. Adriaansens
Minister van Economische Zaken en Klimaat

Directoraat-generaal
Bedrijfsleven & Innovatie

Ons kenmerk
DGBI / 21239754

Bijlage 1: Persbericht AT

Tekortkomingen in beveiliging van aftapvoorziening KPN

Agentschap Telecom heeft diepgaand onderzoek gedaan naar de veiligheid van het aftapsysteem van KPN. Hieruit blijkt dat de beveiliging niet op alle onderdelen aan de wettelijke vereisten voldeed. Agentschap Telecom legt daarom een boete op aan KPN van 450.000 euro. KPN geeft aan dat zij de geconstateerde tekortkomingen inmiddels heeft verholpen.

Aanleiding
Aanleiding voor het onderzoek was een artikel in de Volkskrant van 17 april 2021. Daarin werd -op basis van een rapport uit 2010- gesuggereerd dat er 'ongeautoriseerde, ongecontroleerde en ongelimiteerde' toegang was tot de mobiele netwerken van KPN.

Het onderzoek
Agentschap Telecom heeft diepgaand technisch onderzoek gedaan naar de huidige beveiliging van de aftapvoorziening van KPN. Dit is het systeem dat informatie bevat over personen die 'getapt' worden. Tappen is het meeluisteren met telefoongesprekken die personen voeren of het meelezen met berichten (bijvoorbeeld via sms of mails). De Officier van Justitie, de AIVD of MIVD kunnen daarvoor opdracht geven op basis van hun eigen wettelijke taken.

Resultaten
Uit het onderzoek blijkt dat KPN onvoldoende zorg heeft gedragen voor het treffen van noodzakelijke beveiligingsmaatregelen om kennisneming van aftapgegevens door onbevoegden te voorkomen. Ook blijkt uit het onderzoek dat KPN voor haar systemen gebruik maakt van diverse leveranciers. Het beheer doet KPN echter zelf. De zogenoemde derdelijns ondersteuning komt van leveranciers, hetgeen gebruikelijk is en ook is toegestaan. Omdat er bij de tapvoorziening ook staatsgeheime informatie in het geding kan zijn, worden aan de beheerders strenge eisen gesteld. Alles wat ze doen moet nauwkeurig worden vastgelegd en alleen medewerkers met een Verklaring omtrent het Gedrag (VOG) en een geheimhoudingsverklaring mogen in aanraking komen met deze gegevens.
John Derksen, hoofd Toezicht van Agentschap Telecom: het onderzoek laat zien dat KPN 'de voordeur' tot haar systemen voldoende beveiligd heeft. Niemand anders dan KPN bepaalt wie er toegang krijgt tot de systemen. Het onderzoek laat echter ook zien dat een beperkte groep systeembeheerders die toegang had tot de systemen, niet over de vereiste Verklaring omtrent het Gedrag (VOG) en een geheimhoudingsverklaring beschikte. Deze personen hadden bovendien geen persoonlijk account. Daardoor konden hun individuele handelingen niet goed worden gevolgd en geregistreerd.

Problemen opgelost
KPN heeft volledig meegewerkt aan het onderzoek en tijdens het onderzoek maatregelen genomen om de veiligheid van het aftapsysteem op het vereiste niveau te brengen. KPN heeft aangegeven dat het autorisatieproces inmiddels is verbeterd en dat alle beheerders nu over de vereiste documenten beschikken.

Agentschap Telecom heeft essentiële delen van de verbeteringen gezien en de overige verbeteringen worden gecontroleerd in het reguliere inspectieproces onder de aangescherpte zorgplicht.

Weerbaarheid telecomsector

De veiligheid en integriteit van telecomnetwerken zijn van vitaal belang voor onze maatschappij en onze economie. Hiervoor zetten de medewerkers van het agentschap zich dagelijks in. De afgelopen jaren is onder leiding van de Taskforce Economische Veiligheid gewerkt aan wettelijke mogelijkheden om risico's te mitigeren. Onder andere het Besluit veiligheid en integriteit telecommunicatie en de daaruit volgende beschikkingen en ministeriële regeling geven een juridische basis om risico's die samenhangen met ongeautoriseerde toegang door derden beter te beheersen. Deze wettelijke instrumenten vormen samen met de bestaande bepalingen uit de Telecommunicatiewet de basis om de telecomsector voldoende weerbaar te maken tegen de actuele dreigingen en de basis voor het toezicht daarop door het agentschap.