Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres: Postbus 20010 2500 EA Den Haag

Ministerie van Justitie en Veiligheid
T.a.v. de Minister van Justitie en Veiligheid
Postbus 20301
2500 EH Den Haag

Postbus 20010
2500 EA Den Haag
www.aivd.nl

Contact

T 079 320 50 50
F 070 320 07 33

Ons kenmerk
907bf75c-or1-3.0

Uw kenmerk

Bijlagen
0

Datum 4 februari 2019
Betreft Nationale veiligheid en veiling 5G

Mijnheer de Minister,

De AIVD heeft als taak om dreigingen te onderkennen en de nationale veiligheid en de belangen van Nederland te beschermen, dit doen wij in nauwe samenwerking met de MIVD. Met deze brief informeer ik u, mede namens de MIVD, over de relevante ontwikkelingen op het gebied van digitale dreigingen, met betrekking tot het vraagstuk 5G en maatregelen voor de telecomsector.

Dreiging
In de afgelopen jaren ziet de AIVD een toename van het aantal *'supply chain attacks'* door statelijke actoren. Bij *supply chain attacks* worden dienstverleners, zoals internet service providers, telecomproviders en managed service providers, ingezet als springplank om doelwitorganisaties te infiltreren. Er wordt dan misbruik gemaakt van de hard- en software van deze dienstverleners om zo toegang te krijgen tot het netwerk van doelwitorganisaties.

Het misbruiken van de hard- en software van deze dienstverleners is interessant voor statelijke actoren, omdat het omvangrijke, diepgravende en structurele toegang geeft tot data(stromen) in de netwerken van de doelwitorganisaties. Dit biedt spionagemogelijkheden door zo op grote schaal persoons-, technisch-wetenschappelijke, financieel-economische, militaire en politiek-bestuurlijke gegevens van zowel publieke, militaire en private organisaties te vergaren.

De AIVD heeft vastgesteld dat infiltratie van de dienstverleners door statelijke actoren niet alleen spionage faciliteert, maar ook zorgt voor innesteling in de Nederlandse vitale infrastructuur voor mogelijke sabotagedoeleinden. Hierdoor kunnen de aan het internet gekoppelde besturings- en controlesystemen van vitale infrastructuren, zoals drinkwatervoorziening, elektriciteitsdistributie en betalingsverkeer, verstoord worden.

Daar bovenop komt dat diverse landen nationale wet- en regelgeving hebben om dienstverleners te dwingen tot medewerking aan inlichtingenactiviteiten. Er wordt dan door statelijke actoren gebruik gemaakt van de legitieme toegang die de dienstverlener heeft binnen de netwerken van doelwitorganisaties, waardoor preventie en detectie van misbruik bemoeilijkt wordt.

De risico's voor de nationale veiligheid worden significant vergroot als deze dienstverleners ook nog eens afkomstig zijn uit landen die een offensief cyberprogramma voeren tegen de Nederlandse belangen.

Belang 5G-technologie
De introductie van 5G-technologie (5G) brengt door de aard van de technologie enorm veel kansen met zich mee en vormt een kantelpunt ten opzichte van de huidige telecom infrastructuur. Iedere sector zal door de introductie van de technologie een innovatieve impuls krijgen. 5G faciliteert naar verwachting een significante toename van de aan het internet gekoppelde hard- en software in de persoonlijke levenssfeer van burgers, het bedrijfsleven, de vitale infrastructuur, Defensie en de (Rijks)overheid. Daardoor zal het goed functioneren van de Nederlandse maatschappij steeds meer afhankelijk zijn van 5G.

De keerzijde van deze afhankelijkheid is dat we als gehele Nederlandse samenleving in toenemende mate kwetsbaar zijn bij potentieel misbruik door digitale spionage en sabotage. Hierdoor creëert de introductie van 5G substantiële risico's voor de privacy van burgers en voor de vertrouwelijkheid van gevoelige bedrijfs- en overheidsinformatie. Specifiek kan ten aanzien van de telecomsector gedacht worden aan het vergaren van klant-, geolocatie- en telefonieverkeersgegevens.

Daarnaast is de continuïteit en beschikbaarheid van het bedrijfsleven en de vitale infrastructuur en de dienstverlening van de (Rijks)overheid in het geding. In potentie zal misbruik ertoe kunnen leiden dat grote delen van de Nederlandse samenleving kunnen uitvallen.

Advies
De inlichtingen- en veiligheidsdiensten vinden het onwenselijk dat Nederland voor de uitwisseling van gevoelige informatie en/of vitale processen afhankelijk is van IT-producten en -diensten uit landen waarvan is vastgesteld dat ze een offensief cyberprogramma tegen Nederlandse belangen voeren. Dit standpunt is in lijn met de criteria[1] die eerder door het kabinet zijn opgesteld.

Gegeven dit standpunt, de hierboven genoemde toekomstige afhankelijkheid van 5G en de geschetste dreiging geeft de AIVD onderstaande adviezen. Bij de uitwerking van deze maatregelen door de verschillende overheidspartijen is overleg met telecomproviders noodzakelijk gegeven de grote verschillen in technische infrastructuur.

1. Bij de veiling van 5G eisen en waarborgen ten aanzien van bepaalde hard- en software op te nemen ten behoeve van de nationale veiligheid en strategische onafhankelijkheid.
2. De kritieke belangen ('de kroonjuwelen') binnen de telecom infrastructuur te identificeren.
3. Een aanpak te formuleren voor het uitfaseren van bepaalde hard- en software binnen de kritieke belangen in de bestaande telecom infrastructuur (2G, 3G, 4G) afkomstig van dienstverleners uit landen met een offensief cyberprogramma.
4. Het voorkomen van nieuwe afhankelijkheden in de toekomstige 5G infrastructuur ten aanzien van de kritieke belangen, door bepaalde hard- en software van dienstverleners uit landen met een offensief cyberprogramma selectief te weren.
5. Te bezien welke aanvullende mitigerende maatregelen nodig zijn om de huidige en nieuwe infrastructuur te beveiligen.
6. Indien telecomproviders deze mitigerende maatregelen niet zelf treffen, deze maatregelen - al dan niet met wetgeving - af te dwingen.
7. Het inrichten van vernieuwd toezicht, passend bij het huidige dreigingsbeeld.

1 De volgende criteria zijn gehanteerd:
1. Het land van herkomst heeft een offensief cyberprogramma gericht op de Nederlandse belangen
2. Het land van herkomst heeft wetgeving die bedrijven verplicht medewerking te verlenen aan inlichtingendiensten
3. De software of hardware heeft verregaande toegang tot de infrastructuur

8. De (technische) expertise ten aanzien van nieuwe technologie zoals 5G binnen de Rijksoverheid op te bouwen, gezien de geconstateerde beperkte beschikbaarheid.

Zonder bovenstaande maatregelen is er onvoldoende sprake van risicobeheersing ten aanzien van de nationale veiligheid.

De AIVD en MIVD zijn gaarne bereid ondersteuning te bieden om dit verder vorm te geven.

Deze brief is ook verstuurd aan de staatssecretaris Economische Zaken en Klimaat, de directeur-generaal Bedrijfsleven en Innovatie, de directeur Digitale Economie, de Nationaal Coördinator Terrorismebestrijding en Veiligheid en de leden van de Raad voor Veiligheids- en Inlichtingendiensten.

Hoogachtend,
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties,

H.W.M. Schoof
Directeur-generaal van de Algemene Inlichtingen- en Veiligheidsdienst