Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

Aanhangsel van de Handelingen

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

1401

Vragen van de leden **Rajkowski** en **Minhas** (beiden VVD) aan de Staatssecretaris van Infrastructuur en Waterstaat en de Minister van Justitie en Veiligheid over *het bericht «ProRail dumpt Chinese bewakingscamera's, de NS laat ze hangen»* (ingezonden 22 november 2022).

Antwoord van Staatssecretaris **Heijnen** (Infrastructuur en Waterstaat) en van Minister **Yeşilgöz-Zegerius** (Justitie en Veiligheid) (ontvangen 31 januari 2023). Zie ook Aanhangsel Handelingen, vergaderjaar 2022-2023, nr. 1011.

Vraag 1
Herinnert u zich uw antwoorden op de schriftelijke vragen van 12 september jl. over het bericht «ProRail dumpt Chinese bewakingscamera's, de NS laat ze hangen»?[1]

Antwoord 1
Ja, wij herinneren ons deze antwoorden.

Vraag 2
Kunt u concreet aangeven hoe de aanwijzing van het proces van vervoer van personen en goederen over de (hoofd)spoorweginfrastructuur als vitaal proces zich verhoudt tot de aanwezigheid van Chinese camera's in treintoestellen, gegeven dat de Chinese overheid een offensieve cyberstrategie gericht tegen Nederland voert? Hoe beoordeelt u daarmee de aanwezigheid van Chinese camera's binnen een Nederlandse vitale sector, kijkend naar de veiligheidsrisico's waar onder andere de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) al eerder voor gewaarschuwd heeft? Kunt u dit toelichten?

Antwoord 2
Het proces van vervoer van personen en goederen over de (hoofd)spoorweginfrastructuur is aangewezen als vitaal proces. In dit proces zijn vitale aanbieders op basis van de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) verplicht tot het nemen van passende en evenredige technische en organisatorische maatregelen om de risico's voor de beveiliging van hun netwerk- en informatiesystemen te beheersen (zorgplicht). Daarnaast dienen zij inzicht te hebben in de risico's die hun dienstverlening kunnen raken. Vitale aanbieders zijn daarbij zelf verantwoordelijk voor het nemen van

[1] Aanhangsel Handelingen, vergaderjaar 2022-2023, nr. 476.

ah-tk-20222023-1401
ISSN 0921 - 7398
's-Gravenhage 2023

maatregelen tegen de risico's voor de nationale veiligheid. De Inspectie Leefomgeving en Transport houdt binnen de spoorsector toezicht op de manier waarop Aanbieders van Essentiele Diensten (AED's) invulling geven aan deze zorgplicht.

Ook dienen nationale veiligheidsoverwegingen te worden meegewogen bij het inkopen van producten en diensten. Hiervoor zijn er instrumenten ontwikkeld die organisaties, waaronder vitale aanbieders, helpen bij het nemen van passende maatregelen. Vitale aanbieders zijn zelf verantwoordelijk voor de toepassing van deze instrumenten en het meewegen van nationale veiligheidsrisico's. Hierbij kan het Rijk gevraagd en ongevraagd advies en ondersteuning bieden.

Dat een bepaald product of dienst, in dit geval camera's, binnen een vitale sector afkomstig is van een Chinese aanbieder is niet per definitie onwenselijk. Uitgangspunt bij het beoordelen van risico's is dat altijd een afweging plaatsvindt op de hierboven genoemde punten. Zoals ook eerder aan uw Kamer gemeld[2], is het daarbij van belang na te gaan of de partij die de dienst of het product levert banden heeft met of onder controle staat van landen met een offensief inlichtingenprogramma of specifieke verplichtende wetgeving kent. Daarnaast is van belang te onderzoeken waar de partij toegang toe kan verkrijgen via de dienst of het product en of er beheersmaatregelen mogelijk en realiseerbaar zijn.
Op een zeer zorgvuldige en case-by-case-basis dienen deze risico's te worden onderzocht.
In algemene zin is het dus mogelijk om binnen vitale sectoren apparatuur uit China te gebruiken, als dit zorgvuldig wordt afgewogen, er voldoende rekening wordt gehouden met de risico's en eventuele noodzakelijke maatregelen worden genomen om mogelijke risico's te beheersen.

Vraag 3
Gegeven dat bij de aanschaf en implementatie van gevoelige apparatuur rekening wordt gehouden met eventuele risico's in relatie tot de leverancier, waaronder in het bijzonder het hebben van een offensief cyberprogramma gericht tegen Nederland en gegeven het feit dat de leverancier in kwestie daadwerkelijk over een offensief cyberprogramma beschikt, in hoeverre zijn bovenstaande omstandigheden geïntegreerd in het meewegen van de nationale veiligheidsrisico's door de NS? Kunt u de overwegingen hierbij toelichten?

Antwoord 3
Zoals ook geschetst in het antwoord op vraag 2 van de schriftelijke vragen van 12 september jl. over het bericht «ProRail dumpt Chinese bewakingscamera's, de NS laat ze hangen?», heeft NS laten weten dat zij diverse maatregelen heeft genomen zodat (statelijke) actoren niet van buitenaf bij de inhoud of de besturing van de camera's kunnen komen. Dat geldt niet alleen voor de Chinese camera's, maar voor álle camera's.

Het gaat onder andere om de volgende maatregelen:
- Camera's zijn qua netwerk gescheiden van andere apparaten.
- Camera's zijn niet direct verbonden met het internet.
- Standaard toegangsrechten, zoals aanwezig bij aflevering, zijn aangepast.
- Ethische hackers testen de geïmplementeerde veiligheidsmaatregelen periodiek.

NS heeft mij laten weten dat zij menen dat door het toepassen van risicobeperkende maatregelen de risico's beheersbaar zijn. Daarnaast heeft NS aangegeven gebruik te maken van de adviezen van de rijksoverheid, zoals ook geschetst in antwoord op vraag 2. Hierop houdt de toezichthouder toezicht.

[2] Kamerstuk 25 124, nr. 96.

Vraag 4
In hoeverre acht u de mitigerende maatregelen die door de NS zijn genomen zoals vastgesteld op 24 oktober jl. toereikend? Kunt u dit toelichten? Zo nee, waarom niet?

Antwoord 4
Vitale aanbieders, zoals de NS, zijn zelf verantwoordelijk voor de toepassing van de instrumenten die de rijksoverheid aanbiedt en het meewegen van nationale veiligheidsrisico's (zoals genoemd in antwoord op vraag 2). NS heeft laten weten dat zij een risicoanalyse heeft doorlopen waarbij cyberrisico's zijn meegewogen. Naar aanleiding daarvan heeft NS diverse maatregelen genomen om de kans op/gevolgen van deze risico's te beheersen (zie ook antwoord op vraag 3).

Vraag 5
Bent u het ermee eens dat het wenselijk kan zijn voor de nationale veiligheid om het Nationaal Cyber Security Centrum (NCSC) advies te laten geven over individuele producten en diensten wanneer deze worden afgenomen door aanbieders werkzaam binnen een vitale sector? Zo ja, bent u bereid om het NCSC onderzoek te laten doen naar de camera's van Chinese makelij die de NS in bezit heeft? Zo nee, waarom niet?

Antwoord 5
Vitale aanbieders, zoals de NS, zijn zelf verantwoordelijk voor de toepassing van instrumenten die de rijksoverheid aanbiedt en het meewegen van nationale veiligheidsrisico's (zie ook antwoord op vraag 2). Organisaties zoals NS hebben eigen expertise in huis en weten zelf het beste hoe bepaalde producten en diensten worden toegepast, waar de te beschermen belangen en risico's zitten en welke maatregelen mogelijk zijn om risico's te verminderen. Het NCSC geeft geen advies over individuele producten of diensten, maar adviseert vitale aanbieders om risicomanagement te organiseren.