Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

Aanhangsel van de Handelingen

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

1233

Vragen van het lid **Six Dijkstra** (Nieuw Sociaal Contract) aan de Minister van Justitie en Veiligheid over *het artikel «Veiligheidsregio gebruikte jarenlang Chinese apparatuur ondanks spionagerisico's»* (ingezonden 3 januari 2024).

Antwoord van Minister **Yeşilgöz-Zegerius** (Justitie en Veiligheid), mede namens de Minister van Binnenlandse Zaken en Koninkrijksrelaties (ontvangen 13 maart 2024).

Vraag 1
Bent u bekend met het bericht «Veiligheidsregio gebruikte jarenlang Chinese apparatuur ondanks spionagerisico's»?[1]

Antwoord 1
Ja, ik ben bekend met het bericht «Veiligheidsregio gebruikte jarenlang Chinese apparatuur ondanks spionagerisico's.

Vraag 2
Deelt u de opvatting dat het vanuit het perspectief van nationale veiligheid onverantwoord is om Chinese routers en switches te gebruiken binnen het netwerk van vitale instellingen?

Antwoord 2
Zoals eerder is aangegeven in onder meer het Cybersecuritybeeld Nederland[2] en het Dreigingsbeeld Statelijke Actoren 2[3] is in algemene zin bekend dat statelijke actoren gebruik maken van supply-chain aanvallen via toeleveranciers, digitale dienstverleners of veelgebruikte software. Er kunnen aanvullende risico's zijn als dergelijke toeleveranciers, dienstverleners en software afkomstig zijn uit landen met een offensief cyberprogramma tegen Nederland. Het is echter niet per definitie zo dat het gebruik van hard- en software uit deze landen risico's met zich meebrengt. Om dit te kunnen beoordelen is onder meer het proces waarvoor de hard- en software wordt gebruikt relevant en bijvoorbeeld ook de manier waarop dit binnen organisaties

[1] Follow the Money, 27 december 2023, «Veiligheidsregio gebruikte jarenlang Chinese apparatuur ondanks spionagerisico's» (www.ftm.nl/artikelen/veiligheidsregio-verwijdert-huawei#:~:text=Ondanks%20waarschuwingen%20van%20veiligheidsdiensten%20voor,apparatuur%20in%20alle%20stilte%20vervangen.).
[2] Kamerstuk 28 665
[3] Kamerstuk 30 821, nr. 175

ah-tk-20232024-1233
ISSN 0921 - 7398
's-Gravenhage 2024

gebruikt wordt. Routers en switches zijn onderdeel van de netwerkinfrastructuur van organisaties en om eventuele risico's van het gebruik hiervan te kunnen duiden, prioriteren en beheersen is het van belang te bepalen welke rol de routers en switches hebben in deze infrastructuur. De risico's zijn bijvoorbeeld mogelijk groter als ze onderdeel zijn van de data/informatieverwerking van de organisatie of specifieke (vitale) processen ondersteunen. Ook is relevant of het land waar de leverancier uit afkomstig is wetgeving kent die burgers en bedrijven verplichten mee te werken met de overheid. Een solide risicoanalyse en risicomanagementproces zijn nodig om eventuele passende maatregelen te kunnen nemen.
Het is in dat verband van belang dat organisaties zich bewust zijn van mogelijke risico's in de toeleveringsketen, dit meenemen in hun inkoop- en aanbestedingsprocessen en waar nodig een risicoanalyse uitvoeren. Het kabinetsbeleid schrijft daarom voor dat nationale veiligheidsoverwegingen meegewogen worden bij de inkoop en het gebruik van producten en diensten bij de Rijksoverheid, lokale overheden en vitale aanbieders. In de Kamerbrief *Uitvoering moties Rajkowski* van 17 april 2023 wordt dit beleid nader toegelicht[4]. Het uitgangspunt is bij iedere inkoopopdracht risico's voor de nationale veiligheid in kaart te brengen en hier waar nodig gepaste maatregelen op te treffen. Ter ondersteuning van dit beleid is in 2018 en 2019 instrumentarium ontwikkeld dat organisaties mogelijkheden biedt bij het maken van een risicoanalyse en het treffen van maatregelen. Dit instrumentarium is recent geactualiseerd[5]. Deze instrumenten worden beschikbaar gesteld voor en actief verspreid onder vitale aanbieders. Tevens wordt doorlopend ingezet op bewustwording bij vitale aanbieders over het signaleren van risico's in het inkoopproces.
Daarnaast kunnen organisaties gebruik maken van de handreiking *Omgaan met risico's in de toeleveringsketen* van het Nationaal Cyber Security Centrum. Deze publicatie geeft publieke en private organisaties handvatten om zicht en grip te krijgen op risico's die voortvloeien uit de toeleveringsketen, ook in relatie tot leveranciers uit landen met een offensief cyberprogramma. Overheidsorganisaties kunnen ook gebruikmaken van de Inkoopeisen Cybersecurity Overheid wizard (ICO-wizard) die is opgesteld door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) samen met EZK. Deze inkooptool is ontwikkeld om veilig inkopen te vergemakkelijken. Met de ICO-wizard kunnen eisenpakketten worden geselecteerd die aansluiten op verschillende typen aan te besteden of in te kopen producten en/of diensten.

Vraag 3 en 4
Heeft u zicht op welke Chinese netwerkapparatuur door de veiligheidsregio's is gebruikt sinds de inwerkingtreding van het Besluit veiligheid en integriteit telecommunicatie in 2019?
Heeft u zicht op welke Chinese netwerkapparatuur momenteel wordt gebruikt door de veiligheidsregio's?

Antwoord 3 en 4
Nee. Ik heb geen volledig zicht op welke netwerkapparatuur wordt gebruikt door veiligheidsregio's. Het is aan de besturen van veiligheidsregio's zelf om bij de aanschaf en ingebruikname van ICT-producten en diensten zich bewust te zijn van mogelijke risico's in de toeleveringsketen, dit mee te nemen in hun inkoop- en aanbestedingsprocessen en waar nodig een risicoanalyse uit te voeren.

Vraag 5
Zo nee, bent u bereid dit (3 en 4) in kaart te brengen?

Antwoord 5
Veiligheidsregio's spelen een belangrijke rol in de crisisbeheersing en nationale veiligheid van Nederland. In algemene zin is het conform bestaand beleid (zie onder meer de beantwoording op vraag 2 en 4) aan de besturen

[4] Kamerstuk 26 643, nr. 1007
[5] Toolbox veilig inkopen (2024), online toegankelijk via https://www.nctv.nl/onderwerpen/economische-veiligheid/toolbox-veilig-inkopen

van veiligheidsregio's zelf om afwegingen te maken daar waar het gaat om het gebruik van (netwerk-)apparatuur.
Meer specifiek is digitale weerbaarheid voor de veiligheidsregio's een belangrijk onderwerp. De 25 veiligheidsregio's werken in een gezamenlijk meerjarig programma informatievoorziening aan hun eigen weerbaarheid. Ik zal de komende tijd met de veiligheidsregio's het gesprek aangaan over dit onderwerp en met hen bespreken of aanvullende stappen nodig zijn.

Vraag 6
Wordt er bij het aanbestedingsbeleid van de Rijksoverheid ook specifiek gekeken of er geschikte Europese alternatieven voor netwerkapparatuur beschikbaar zijn?

Antwoord 6
Het kabinet voert zoals aangegeven in het antwoord op vraag 2 een landenneutraal beleid. Dit betekent dat leveranciers uit specifieke landen door de aanbestedende dienst niet op voorhand categorisch worden uitgesloten, maar dat dit *per casus* op basis van een risicoafweging wordt bepaald. Hierbij kan per casus tevens door de organisatie zelf een marktanalyse worden uitgevoerd, waarbij in kaart kan worden gebracht of Europese aanbieders bij een inkoop- en aanbestedingstraject kunnen worden betrokken.
Het heeft de prioriteit van het kabinet om in samenwerking met alle departementen het veilig inkopen en aanbesteden in onderlinge samenhang verder te verbeteren en te versterken. Er is stevig ingezet op het sterker benutten van de huidige mogelijkheden binnen de Aanbestedingswetgeving en op het vergroten van de bewustwording ten aanzien van nationale veiligheidsrisico's. Tevens vindt meer voorlichting en communicatie plaats over de (juridische) mogelijkheden ten aanzien van veilig inkopen en aanbesteden. Ook wordt een regeling opgezet (genaamd Algemene Beveiligingseisen Rijksoverheid Opdrachten of afgekort ABRO) voor aanbestedingen van de Rijksoverheid en de Politie die de nationale veiligheid raken. De nieuwe regeling zal eisen stellen aan opdrachtnemers op het gebied van fysieke beveiliging, (digitale) informatiebeveiliging en cybersecurity, (wijzigingen in) eigendomsstructuren, economische veiligheid, screening van personeel en procedures bij incidenten.