Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019 **Aanhangsel van de Handelingen**

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

2525

Vragen van het lid **Bruins Slot** (CDA) aan de Minister en de Staatssecretaris van Defensie over *het tegengaan van ongewenste toegang tot het Netherlands Armed Forces Integrated Network (NAFIN)* (ingezonden 1 april 2019).

Antwoord van Minister **Bijleveld-Schouten** (Defensie), mede namens de Staatssecretaris van Defensie (ontvangen 3 mei 2019)

Vraag 1 en 2
Is het glasvezelnetwerk van Defensie, het Netherlands Armed Forces Integrated Network (NAFIN) van belang in het kader van de nationale veiligheid en dient dit zwaar beveiligd te zijn in het licht van de toenemende cyberdreiging?
Deelt u de mening dat het van belang is om voorzieningen te treffen om het NAFIN te vrijwaren van ongewenste statelijke en non-statelijke beïnvloeding, spionage en sabotage?

Antwoord 1 en 2
Ja. Het NAFIN wordt voortdurend aangepast naar de hedendaagse standaarden. De beveiliging tegen cyberdreigingen maakt hier onderdeel van uit.

Vraag 3
Hanteert u nog steeds het uitgangspunt dat over de middelen voor «command and control», waaronder de verbindingsstelsels, volledige beschikkingsmacht door Defensie vereist is en dat Defensie voor «command and control» niet afhankelijk van derden mag zijn?[1]

Antwoord 3
Ja. Defensie is autonoom in staat om «command and control» uit te voeren van het verbindingsstelsel NAFIN. Het beheer van het NAFIN wordt daarom volledig door Defensie uitgevoerd, onafhankelijk van derden. Voor andere verbindingsstelsels is het noodzakelijk gebruik te maken van diensten van civiele providers, waarbij Defensie maatregelen neemt op het gebied van onder andere encryptie, monitoring, beveiliging en redundantie om afhankelijkheid van deze derden tot het minimum te beperken.

[1] Kamerstuk 22 800 X, nr. 46

ah-tk-20182019-2525
ISSN 0921 - 7398
's-Gravenhage 2019

Vraag 4
Klopt het nog steeds dat het economisch eigendom van het NAFIN bij KPN ligt en dat u het eeuwig gebruiksrecht heeft?

Antwoord 4
KPN heeft het juridisch eigenaarschap van het NAFIN omdat Defensie zelf in vredestijd geen grondroerdersrechten heeft. Het economisch eigenaarschap en het eeuwige exclusieve gebruiksrecht ligt bij Defensie.

Vraag 5
Klopt het dat in de afgelopen jaren steeds meer medegebruik door tweeden en derden plaatsvindt van het NAFIN, zoals de politie, C2000 (voor vaste verbindingen in het kernnetwerk), het civiele KPN Telecom satelliet-grondstation in Burum en de vier rijksoverheidsdatacenters (opvolger van alle 64 datacenters van het Rijk), die een groot deel van alle rijksoverheid informatie opslaat en ook de Rijkscloud bevat en de Haagse Ring?

Antwoord 5
Ja. Vanwege het specifieke karakter van een strategische defensietoepassing als het NAFIN, is samenwerking met andere partijen binnen de rijksoverheid op het gebied van veiligheid en vitale processen passend. Zoals aangekondigd in de Defensie Cyber Strategie (33 321 Nr. 9, 12 november 2018) zal onderzocht worden welke Defensievoorzieningen kunnen worden ingezet om kritieke processen draaiende te houden wanneer er sprake is van maatschappij ontwrichtende ICT-uitval als gevolg van een digitale aanval. Voorzieningen als het NAFIN kunnen hierbij een rol spelen.

Vraag 6
Is de opsomming in vraag 5 van medegebruik door tweeden en derden volledig? Zo nee, welke organisaties of andere actoren missen in de opsomming?

Antwoord 6
Defensie levert ook NAFIN-diensten (of heeft het verzoek deze te gaan leveren) aan de NCTV, het Nationaal Cyber Security Centrum, de inlichtingen- en veiligheidsdiensten, de IND, het European Air Transport Command en de Kustwacht.

Vraag 7
Klopt nog steeds het uitgangspunt voor medegebruik dat «Defensie onder alle omstandigheden de volledige zeggenschap over het NAFIN behoudt»?[2] Zo nee, op welke onderdelen en in welke situaties is daar geen sprake meer van?

Antwoord 7
Ja.

Vraag 8
In hoeverre is er bij het medegebruik door tweeden en derden sprake van virtueel en/of gescheiden netwerken? Kunt u per medegebruiker aangeven of er sprake is van een virtueel gescheiden en/of fysiek gescheiden netwerk?

Antwoord 8
Bij medegebruik worden NAFIN glasvezels aangelegd naar de locatie van de medegebruiker waarop NAFIN apparatuur wordt aangesloten voor de levering van NAFIN diensten. Deze diensten zijn virtueel gescheiden in de NAFIN infrastructuur, zodat er geen vermenging van datastromen van verschillende organisaties en/of systemen kan optreden.

Vraag 9
In hoeverre is er op deze netwerken sprake van het verspreiden van gerubriceerde/geclassificeerde informatie? Kunt u een overzicht van welke gerubriceerde/geclassificeerde informatie over welke netwerken (NAFIN en de

[2] Kamerstuk 23 400 X, nr. 46

medegebruikers) verspreid kan/mag worden aan de Kamer toezenden? Klopt het nog steeds dat over het NAFIN tot en met geheim gerubriceerde e-mail kan worden verzonden?

Antwoord 9
Het NAFIN is gerealiseerd over glasvezels die alleen bovengronds komen op locaties van Defensie of ketenpartners in een daartoe ingerichte en beveiligde ruimte. Door aanvullende, strikte eisen aan netwerkapparatuur kan over het NAFIN informatie tot het niveau Departementaal Vertrouwelijk getransporteerd worden. Voor transport van hoger gerubriceerde informatie over het NAFIN worden aanvullende maatregelen genomen.

Vraag 10
Herinnert u zich de verkenning door PWC naar gescheiden ICT-netwerken en -diensten in Nederland?[3] Bent u het met PWC eens, dat een deel van de kwetsbaarheid van ICT-netwerken zich bevinden in:
a. de oorsprong van de keten van ontwerp en bouw van het netwerk;
b. de upgrades van het netwerk: welke kwetsbaarheden zijn, al dan niet bewust, in componenten ingebouwd?
c. het beheer en het onderhoud van het netwerk: wie hebben toegang tot een netwerk via beheer en onderhoud en met welke intenties?[4]

Antwoord 10
Defensie houdt maximaal rekening met deze ketenrisico's door het NAFIN als zogenaamd *militairy owned and controlled* infrastructuur te beschouwen. Dat betekent dat het netwerk door medewerkers van Defensie is ontworpen en dat Defensie zelf de netwerkapparatuur installeert en configureert. Daarnaast garandeert de leverancier dat de netwerkapparatuur voor het NAFIN voldoet aan de Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408). Toegang tot technische ruimtes en NAFIN-apparatuur is alleen voor geautoriseerde medewerkers van Defensie en eventueel voor medewerkers van de leverende marktpartijen, echter uitsluitend onder aansturing en begeleiding van Defensiemedewerkers. Tot slot wordt het beheer en onderhoud van het NAFIN door Defensie zelf uitgevoerd, waar nodig in samenwerking met gescreende leveranciers. Bewaking van het NAFIN vindt vierentwintig uur per dag plaats. Er zijn geen beheerkoppelingen naar de leverende marktpartijen en onderhoud wordt door Defensie zelf uitgevoerd vanaf Defensielocaties.

Vraag 11
Op welke wijze hebt u rekening gehouden met deze ketenrisico's (zoals het mogelijk schenden van de vertrouwelijkheid van de inhoud van de communicatie) bij het NAFIN en de medegebruikers van het netwerk?

Antwoord 11
De richtlijnen van Defensie zoals verwoord in de reactie op vraag 10 zijn ook van toepassing voor medegebruik NAFIN op locaties buiten defensie. Het NAFIN verzorgt het ongeschonden transport van de aangeboden data; de eindgebruiker is verantwoordelijk voor de inhoud van de communicatie.

Vraag 12
Welk restrisico accepteert u voor NAFIN en het medegebruik? Wat is nodig om dit restrisico te mitigeren?

Antwoord 12
De topologie van het NAFIN is zo opgesteld dat de hoofdroutes van het NAFIN uitsluitend naar Defensielocaties gaan. Locaties van medegebruikers worden separaat aangesloten op deze hoofdroutes. In geval van een dreiging die zijn oorsprong kent in een locatie van een medegebruiker kan Defensie op afstand de poorten dichtzetten of zelfs de volledige locatie isoleren van het NAFIN. Hierdoor kunnen risico's voortkomend uit medegebruik van het NAFIN zoveel mogelijk worden gemitigeerd.

---

[3] Kamerstuk 26 643, nr. 337
[4] PWC, Verkenning naar gescheiden ICT-netwerken en -diensten in Nederland, september 2014

Vraag 13
Wie doet op dit moment of gaat in de toekomst het ontwerp, bouw, upgrades, beheer en onderhoud van het NAFIN en de medegebruikers zoals C2000, de Rijksdatacenters, de Haagse Ring, de Rijkscloud en overige medegebruikers doen? Kunt u een overzicht van NAFIN en per medegebruiker maken? In hoeverre is hier sprake van Nederlandse dan wel buitenlandse bedrijven?

Antwoord 13
Deze activiteiten worden volledig onder regie van Defensie uitgevoerd, waarbij het merendeel van de activiteiten ook door Defensie zelf worden uitgevoerd. Aanvullende inzet van medewerkers van de leverende marktpartijen vindt uitsluitend plaats onder aansturing en begeleiding van Defensiemedewerkers. Defensie maakt gebruik van twee marktpartijen voor het NAFIN: KPN voor de infrastructuur en Nokia Nederland (voorheen Alcatel-Lucent) voor de netwerkapparatuur. Beide partijen zijn ABDO getoetst.

Vraag 15
Hoe wordt voorkomen dat via ontwerp, bouw, upgrades, beheer en onderhoud van de medegebruikers van het NAFIN door buitenlandse bedrijven (bijvoorbeeld Chinese bedrijven) toegang wordt verkregen tot het militaire deel van het netwerk en dat daarmee de nationale veiligheid in gevaar kan komen? Kunt u de maatregelen apart benoemen voor de categorie ontwerp, bouw, upgrades, beheer en onderhoud?

Antwoord 15
Het NAFIN wordt alleen gekoppeld met externe netwerken door tussenkomst van een sterk beveiligd koppelvlak om te voorkomen dat derden toegang krijgen. Zie voorts het antwoord op vraag 13.

Vraag 16
Bent u bereid om, door middel van een risicoanalyse van het NAFIN en het medegebruik, de kans en impact van dreigingen in kaart te brengen om hier vervolgens mitigerende maatregelen aan te koppelen en over de kans en impact van dreigingen en de genomen en te nemen maatregelen de Tweede Kamer voor de zomer van 2019 te informeren? Zo nee, waarom niet?

Antwoord 16
Een risicoanalyse is onderdeel van het bestaande informatiebeveiligingsplan van het NAFIN. Dit leent zich niet voor openbaarmaking. Ik verwijs u voorts naar het antwoord op vraag 1 en 2.