Ministerie van Defensie

> Retouradres Postbus 20701 2500 ES Den Haag

de Voorzitter van de Tweede Kamer
der Staten-Generaal
Bezuidenhoutseweg 67
2594 AC Den Haag

Ministerie van Defensie
Plein 4
MPC 58 B
Postbus 20701
2500 ES Den Haag
www.defensie.nl

Onze referentie
2024031990

Bij beantwoording, datum, onze referentie en onderwerp vermelden.

Datum	30 september 2024
Betreft	Kamerbrief beantwoording vragen van het lid Olger van Dijk (NSC) aan de minister van Defensie over het bericht 'Zwaarbeveiligd Defensie-netwerk wist even niet meer hoe laat het was'

Geachte voorzitter,

Hierbij ontvangt u de antwoorden op de schriftelijke vragen van het lid Olger van Dijk (NSC) aan de minister van Defensie over het bericht 'Zwaarbeveiligd Defensie-netwerk wist even niet meer hoe laat het was'. Deze vragen werden aangeboden bij brief van 9 september 2024 met kenmerk 2024Z13160.

Hoogachtend,

DE STAATSSECRETARIS VAN DEFENSIE

Gijs Tuinman

Antwoorden op de schriftelijke vragen van het lid van Dijk (NSC) aan de minister van Defensie over het bericht 'Zwaarbeveiligd Defensie-netwerk wist even niet meer hoe laat het was' (ingezonden 9 september 2024, kenmerk 2024Z13160)

Vraag 1

Heeft u kennisgenomen van het artikel, getiteld "Zwaarbeveiligd Defensie-netwerk wist even niet meer hoe laat het was"?

Ja.

Vraag 2

In uw brief aan de Kamer van 28 augustus 2024 heeft u toegezegd dat Defensie, gezamenlijk met andere betrokkenen, de storing en de weerbaarheid van de desbetreffende IT-systemen zal evalueren; kunt u inmiddels aangeven wat precies de oorzaak is geweest van de fout in de softwarecode die u in uw brief aan de kamer van 28 augustus 2024 aanmerkt als de oorzaak van de storing van het NAFIN-Netwerk? Of zijn er inmiddels andere oorzaken gevonden?

Vraag 3

In uw brief aan de Kamer heeft u tevens aangegeven dat er vooralsnog geen indicatie is dat de storing door een kwaadwillende partij zou zijn veroorzaakt; is dat nog altijd het geval en op basis van welke informatie bent u tot deze conclusie gekomen?

In zijn brief van 28 augustus 2024 schreef de minister van Defensie dat door een fout in de softwarecode een probleem was ontstaan in de tijdsynchronisatie op het NAFIN-netwerk en dat hierdoor het niet mogelijk was om verbinding te maken met dit netwerk. De foute softwarecode zat in een redundant uitgevoerde netwerkcomponent die Defensie als standaardproduct van een leverancier inzet. Defensie heeft geen zicht op hoe deze softwarefout in dit standaardproduct bij de leverancier is ontstaan. De leverancier heeft een nieuwe versie van de software geleverd waarin dit probleem is opgelost. Defensie evalueert nog hoe deze fout tot deze grote storing heeft kunnen leiden. Er is geen indicator gevonden die duidt op betrokkenheid van een kwaadwillende partij. Dit betreft een voorlopige conclusie.

Vraag 4

Hoe beoordeelt u de kwetsbaarheid van het NAFIN-netwerk door sabotage, zoals het verstoren van de klok van het netwerk, *time spoofing*?

Vraag 5

Hoe is de redundantie van het NAFIN-netwerk? Zijn er voor bijvoorbeeld de aangesloten civiele overheidsdiensten noodvoorzieningen beschikbaar en zo nee, wordt dit naar aanleiding van dit incident overwogen?

Het NAFIN-netwerk kent bescherming tegen *time spoofing* en een hoge mate van redundantie. Vanwege veiligheidsredenen verstrekt Defensie echter geen nadere inhoudelijke informatie over het al dan niet aanwezig zijn van kwetsbaarheden. Defensie zorgt voor voortdurende evaluatie van de staat van het netwerk en het doorvoeren van wijzigingen waar nodig. Voorts onderzoekt de

Algemene Rekenkamer periodiek de mate van weerbaarheid van het NAFIN-netwerk tegen zowel fysieke en cyberaanvallen, hierbij worden tevens aanbevelingen meegegeven.

Verstoringen, zoals door fouten in de software, kunnen nooit volledig uitgesloten worden. Defensie onderhoudt het netwerk dagelijks en evalueert en verbetert gevonden kwetsbaarheden. Wat betreft noodvoorzieningen hebben Defensie en de andere gebruikers van het NAFIN-netwerk een gezamenlijke verantwoordelijkheid voor de beschikbaarheid en veiligheid van de NAFIN-gerelateerde systemen. We helpen elkaar in deze verantwoordelijkheid.

Vraag 6

Kunt u toelichten waarom het bijna 15 uur duurde voordat de oorzaak van de storing werd ontdekt en verholpen? Deelt u de mening dat dit onacceptabel is, gegeven de grote gevolgen zoals bijvoorbeeld de impact op het civiele luchtvaartverkeer van vliegveld Eindhoven? In hoeverre hebben de vele aansluitingen op het netwerk van andere overheidsdiensten invloed gehad op dit proces?

Ik heb volledig begrip dat voor gedupeerden vijftien uur te lang heeft geduurd. De eerste meldingen over verstoringen werden gedaan in de late avond van 27 augustus 2024. In de ochtend van 28 augustus 2024 werd de omvang van de verstoring volledig zichtbaar. Omdat de richting van de problemen en de gevolgen niet op voorhand bepaald kon worden, is er stap voor stap naar de oorzaak gezocht, inclusief naar indicaties van activiteiten van kwaadwillenden. Echter, de falende netwerkcomponent belemmerde ook de analyse- en herstelwerkzaamheden. Bij deze storing had het aantal aansluitingen op het netwerk van andere overheidsdiensten geen invloed op de hersteltijd van het NAFIN-netwerk. Na het herstel van het NAFIN-netwerk moesten IT-systemen, die gebruik maken van het NAFIN-netwerk, opnieuw worden opgestart. Dit dient veilig te gebeuren, waarbij veiligheidseisen en protocollen gevolgd worden. Dit kost extra tijd. Defensie evalueert de directe oorzaak, de gevolgen en het hele proces om het netwerk weer te herstellen. Een onderdeel van de evaluatie zal gericht zijn om te onderzoeken of de oplossing van deze verstoring sneller had gekund.

Vraag 7

Kunt u toelichten of en zo ja welke concrete maatregelen inmiddels zijn genomen om te voorkomen dat dergelijke storingen zich in de toekomst opnieuw voordoen?

Vraag 8

Kunt u toelichten of en zo ja welke concrete maatregelen inmiddels zijn genomen om te verzekeren dat bij een storing in het NAFIN-netwerk de storing sneller opgespoord en verholpen wordt?

Defensie heeft een tijdelijke wijziging doorgevoerd in de configuratie van netwerkcomponenten die betrokken zijn bij tijdsynchronisatie. Daardoor is de kans op herhaling van deze specifieke verstoring van de tijdsynchronisatie geminimaliseerd. Deze wijziging heeft echter weer andere nadelen waar ik vanwege veiligheidsredenen geen details over kan verstrekken. Onderdeel van de evaluatie is het heroverwegen wat het optimale ontwerp is van de configuratie van de netwerkcomponenten. Als uit het onderzoek blijkt dat aanvullende maatregelen nodig zijn zal Defensie deze doorvoeren.

Vraag 9

Kunt u aangeven of er scenario's ontwikkeld zijn voor het opvangen van de effecten bij systeemuitval? Zo ja, hoe worden deze scenario's getest en voorbereid om de impact van dergelijke storingen te minimaliseren?

Defensie heeft scenario's en crisisstructuren indien systemen uitvallen. Defensie moet zich namelijk voorbereiden op een scenario waarbij IT-diensten niet beschikbaar zijn. Deze scenario's worden meegenomen in de evaluatie die Defensie momenteel uitvoert.

Vraag 10

Kunnen de toegezegde vervolgbrief met de nadere evaluatie alsook de antwoorden op de afzonderlijke vragen binnen 3 weken aan de Kamer worden toegestuurd?

Gelet op de diepte en breedte van de evaluatie verwacht ik de finale oplevering hiervan niet voor het einde van dit jaar. Voor de informatie van de Kamer en ter aanvulling wijs ik erop dat de Algemene Rekenkamer binnenkort een onderzoek zal publiceren over het NAFIN-netwerk. De beoogde oplevering van dit onderzoek is op 7 november aanstaande.