Ministerie van Defensie

Aan	STASDEF
Van	CIO
Afgestemd met	CDS, DGB, DJZ, HDFC, DCO
In afschrift aan	MINDEF

TER BESLISSING

Datum
13 maart 2025

Onze referentie
D2025-000744

Opgesteld door

[redacted]
KD:Ambtelijke leiding
T 06[redacted]
[redacted]@mindef.nl

Aantal bijlagen
3

Nota

Evaluatie NAFIN storing

Aanleiding

Op 28 augustus heeft zich een technische storing voorgedaan als gevolg van een softwarefout op het Netherlands Armed Forces Integrated Network (NAFIN) van Defensie. Zowel Defensie als andere aangesloten organisaties hebben hiervan hinder ondervonden. Het COT Instituut voor Veiligheids- en Crisismanagement (hierna: COT) en Strict hebben een evaluatie uitgevoerd. De bevindingen zijn vastgelegd in bijgevoegde twee rapporten met daarop een gezamenlijke oplegger.

Op 9 april 2025 is het commissiedebat NAFIN ingepland. Met bijgevoegde brief informeert u de Kamer voorafgaand aan dit debat over de aanbevelingen van COT en Strict en de maatregelen die Defensie neemt om invulling te geven aan de aanbevelingen. Beide rapporten zijn departementaal vertrouwelijk gemerkt en worden vertrouwelijk met de Kamer gedeeld.

Geadviseerd besluit

U wordt geadviseerd akkoord te gaan met bijgevoegde brief en deze aan de Kamer te verzenden.

Kernpunten

Het COT en Strict geven aan dat ondanks de bestaande preventieve maatregelen die Defensie heeft getroffen, deze storing niet had kunnen worden voorkomen. Dit incident benadrukt de complexiteit van onze IT-omgeving, en de uitdagingen die gepaard gaan met het waarborgen van robuuste en veerkrachtige systemen.

COT en Strict concluderen dat Defensie onvoldoende voorbereid was op een dergelijke verstoring. De conclusies gaan vooral over voorbereidende maatregelen en plannen om de impact van storingen, incidenten of rampen te minimaliseren en de continuïteit te garanderen. Daarnaast heeft Defensie te weinig aandacht gehad voor bredere maatschappelijke implicaties en partijen die op NAFIN zijn aangesloten. Zowel de communicatie naar deze externe partijen als de interne informatiestroom zijn niet goed verlopen. Tot slot was er onvoldoende aandacht voor cybersecurity risico’s en zijn experts op dit gebied niet op tijd in staat gesteld goed genoeg onderzoek te kunnen doen.

De aanbevelingen uit beide rapporten zijn als volgt samen te vatten:

- Zorg voor een grondige herziening van continuïteitsplannen.
  Zet zwaarder in op continuïteitsplannen. Verbeterde continuïteitsplannen zijn belangrijk om de impact van storingen, incidenten of rampen te minimaliseren en de continuïteit te garanderen.
- Zorg voor een duidelijk opschalingskader die ook voor partijen aangesloten op NAFIN navolgbaar is.
  Een opschalingskader is een stappenplan dat bepaalt hoe een organisatie reageert als er een groot cyber of IT-incident is. Het geeft aan wanneer en hoe de crisisaanpak opgeschaald

wordt, bijvoorbeeld wanneer meer experts, bestuurders of externe partijen betrokken moeten worden. Een dergelijk kader voor cyber en IT-storingen als deze ontbreekt.

- Denk bij een storing ook na over de bredere maatschappelijke implicaties en neem dit perspectief mee in oefeningen.
  Defensie wordt aangeraden om de scope te verbreden van het bestuurlijk team dat verantwoordelijk is voor de coördinatie van crisesmanagement, en om deze bredere scope mee te nemen in oefeningen.
- Maak bij het afhandelen van verstoringen geen onderscheid tussen IT- en cybersecurity incidenten.
  Defensie heeft op dit moment voor de afhandeling van IT- en cybersecurity incidenten verschillende plannen en procedures. Echter is het type storing in de eerste fase vaak nog niet duidelijk.
- Stel een crisiscommunicatieplan op waarin vastligt op welke manier en wanneer informatie gedeeld wordt tijdens storingen, zowel intern als met externe partners.
  Met een duidelijk crisiscommunicatieplan kunnen zowel interne als externe partijen sneller en beter worden geïnformeerd.
- Communiceer regelmatig, ook bij onvolledige informatie, over de stand van zaken, genomen maatregelen en verwachte hersteltermijnen.
  Mede door het uitvallen van de reguliere communicatielijnen, kwam de informatiestroom moeilijk op gang. Daarnaast werd er bewust gekozen om enkel via officiële kanalen te communiceren.
- Oefen regelmatig met calamiteitenoefeningen.
  Evalueer na elke oefening de effectiviteit van de maatregelen en werk het plan bij op basis van de bevindingen. Ook communicatie moet als expliciet onderdeel van calamiteitenoefening getraind worden.
- Herijk de uitgangspunten bij een dergelijke verstoring van de prioritering van systemen.
  Dit is nodig voor het waarborgen van de bedrijfscontinuïteit en het verder minimaliseren van de impact op de organisatie. Een goed bedrijfscontinuïteitsplan helpt om vitale processen te identificeren en prioriteit te geven aan herstelwerkzaamheden, zodat de meest kritieke systemen als eerste worden hersteld. In het geval van Defensie kan dit per crisis verschillen.

Op basis van de evaluaties wordt gewerkt aan een actieplan om in de toekomst beter voorbereid te zijn op dergelijke storingen. De conclusies en aanbevelingen van COT en Strict vormen hiervoor een belangrijke basis. Een deel van de maatregelen is al bekend en opgenomen in de brief.

Toelichting

Eerdere ontwikkelingen:

- Op 7 november 2024 heeft de Algemene Rekenkamer het rapport ‘De Kracht en Kwetsbaarheid van Digitale Krijgsmachtnetwerk NAFIN’ gepubliceerd. Naar aanleiding van dit rapport zijn tijdens de vaste commissie voor Defensie op 9 december feitelijke vragen gesteld.
- De storing van 28 augustus 2024 heeft geen relatie heeft met de geconstateerde bevindingen. De aanbevelingen van de Algemene Rekenkamer richtten zich namelijk niet op de digitale werking van het netwerk, maar op de fysieke beveiliging en positionering van het netwerk. Wel komt een van de aanbevelingen van COT en Strict overeen met een aanbeveling van de Algemene Rekenkamer, namelijk dat er onderzoek nodig is naar de wenselijkheid van het vervlechten van militaire middelen met publieke diensten.

Financiële overwegingen

De verzending van deze brief kent geen financiële consequenties.

Juridische overwegingen
De verzending van deze brief kent geen juridische consequenties.

Communicatie
Er wordt in samenwerking met DCO een communicatielijn opgesteld ter voorbereiding op mogelijke media aandacht.

Informatie die niet openbaar wordt gemaakt
De persoonsgegevens van de steller zijn gelakt.