Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 1229

BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 28 oktober 2024

Recente incidenten zoals de Crowdstrike-storing maken de impact van digitale verstoring zichtbaar. Digitale incidenten hebben grote (fysieke) consequenties: vertraging op de vliegvelden, ziekenhuizen kunnen de zorg niet plannen en haperende communicatiesystemen van de hulpdiensten. Dit soort incidenten demonstreren dat complexe en sterk verwerven netwerk- en informatiesystemen kunnen leiden tot brede en onvoorspelbare uitval. De kans op verstoring neemt daarnaast nog steeds toe, niet alleen door technische problemen maar ook door de huidige geopolitieke spanningen. Zo voeren statelijke actoren cyberaanvallen uit om politieke, economische en militaire doelen te bereiken. Ook zien we wereldwijd opererende en steeds geavanceerdere criminelen die grof geld verdienen aan cybercriminaliteit. Dit beeld wordt ondersteund door het *Cybersecuritybeeld Nederland (CSBN) 2024: Turbulente tijden, onvoorziene effecten*. Het verhogen van onze digitale weerbaarheid is daarom een prioriteit. Dit kabinet bouwt voort op de *Nederlandse Cybersecuritystrategie 2022–2028 (NLCS)*. Met deze brief bied ik u namens het kabinet het CSBN 2024 en de voortgangsrapportage NLCS 2024 aan, en ga ik in op verschillende toezeggingen en ontwikkelingen binnen het cybersecuritydomein. In de bijgevoegde voortgangsrapportage ga ik in op de impact van deze toezeggingen en ontwikkelingen op de realisatie van de NLCS.

Het kabinet focust de komende periode in het bijzonder op het bestrijden van de digitale criminaliteit en de weerbaarheid tegen militaire en hybride dreigingen.

Zij intensiveert de aanpak van cybercriminaliteit en gedigitaliseerde criminaliteit. Onder andere door het versterken van de digitale rechtshandhaving, door gerichte investeringen in de politie en strafrechtketen en het verbeteren van de toegang tot digitale gegevens voor de opsporing.

Daarnaast ontvangt uw Kamer voor het einde van het jaar een Kamerbrief over de maatschappij brede aanpak voor de weerbaarheid tegen militaire

kst-26643-1229
ISSN 0921 - 7371
's-Gravenhage 2024

en hybride dreigingen. De NLCS draagt voor het digitale domein in grote mate bij aan de weerbaarheid tegen dit type dreigingen. Het verhogen van de digitale weerbaarheid is noodzakelijk van MKB tot vitale infrastructuur om de continuïteit van de samenleving te borgen. Het doel is om het ongestoord functioneren van netwerk- en informatiesystemen te borgen. Tegelijkertijd kunnen we incidenten nooit volledig uitsluiten. Het is daarom ook van belang dat organisaties zich dusdanig organiseren dat mocht een incident zich voordoen de dienstverlening snel hersteld kan worden of dat er (analoge) terugvalopties beschikbaar zijn.

Nederlandse Cybersecuritystrategie 2022–2028

De NLCS is in 2022 opgesteld en zet uiteen hoe de betrokken publieke, private en wetenschapspartijen in zes jaar gezamenlijk toewerken naar een digitaal weerbaar Nederland. Deze inzet is concreet gemaakt in een onderliggend actieplan. Op 8 februari 2024 is de nulmeting met uw Kamer gedeeld.[1] Deze nulmeting maakt inzichtelijk wat de uitgangssituatie was voordat er met de strategie werd gestart. De nulmeting vormt de basis voor de evaluatie van de NLCS. Er is een tussentijdse evaluatie in 2026 en een eindevaluatie in 2028 voorzien. In de tussentijd wordt de Kamer geïnformeerd over de voortgang van de acties middels de voortgangrapportages van de Nederlandse Cybersecuritystrategie.

Voortgangsrapportage 2024

Het afgelopen jaar is de inzet op de acties die bijdragen aan het realiseren van de NLCS groot geweest. Zo is 23 mei 2024 de visie op het Cyberweerbaarheids-netwerk (CWN) gepubliceerd. Het Cyberweerbaarheidsnetwerk is de doorontwikkeling van het Landelijk Dekkend Stelsel (LDS) voor cybersecurity samenwerkingsverbanden. Het doel van het Cyberweerbaarheidsnetwerk is om met publieke en private organisaties gecoördineerd samen te werken en gezamenlijk de vijf functies van het CWN te realiseren. Een sterke verbreding ten opzichte van het LDS, wat zich voornamelijk richtte op informatiedeling. De vijf functies van het CWN zijn: (i) informatiedeling; (ii) doelwit- en slachtoffernotificatie; (iii) incidentafhandeling; (iv) kennisuitwisseling; en het (v) organiseren en/of faciliteren van opleidingen, trainingen en oefeningen. Deze samenwerking binnen het CWN zal publieke en private organisaties binnen Nederland in staat stellen om hun cyberweerbaarheidsniveau te verhogen. De visie wordt momenteel vertaald naar een bouwplan.

Daarnaast is er op verschillende manieren aandacht voor het beschermen van burgers tegen digitale risico's. Zo wordt nauw samengewerkt aan publiekscampagnes op het gebied van cybercriminaliteit en cybersecurity, om de bewustwording rondom digitale risico's onder burgers te vergroten.

Ook de voorbereidingen voor de implementatie van de herziene Europese Netwerk en Informatiebeveiligingsrichtlijn (NIS2-richtlijn) in de Cyberbeveiligingswet (Cbw) is in volle gang. De consultatie hiervoor is afgerond en de verwachting is dat het wetsvoorstel in het eerste kwartaal van 2025 bij uw Kamer wordt ingediend. In afwachting van de inwerkingtreding hiervan kunnen de organisaties die onder de nieuwe wet zullen vallen zich al vanaf oktober 2024 vrijwillig registreren zodat zij relevante dreigingsinformatie van het Nationaal Cyber Securitycentrum (NCSC) kunnen ontvangen.[2] Hiernaast is op 1 oktober de Wet bevorderen digitale weerbaarheid bedrijven in werking getreden. De wet versterkt de

[1] Kamerstukken II, 2023–2024 26 643, nr. 1128
[2] Kamerstukken II, 2024–2025 22 112, nr. 3968

wettelijke basis van het Digital Trust Center (DTC) om informatie over digitale dreigingen en kwetsbaarheden te delen met alle niet-vitale bedrijven, waaronder het mkb. De transitie naar de vernieuwde cybersecurityorganisatie is daarbij in volle gang. De integratie van het DTC, het cybersecurity incidentresponsteam voor digitale dienstverleners (CSIRT-DSP) en het NCSC wordt op dit moment verder geïntensiveerd en de vernieuwde organisatie krijgt daarmee steeds verder vorm.

Dankzij de succesvolle publiek-private oefening ISIDOOR IV zijn er waardevolle inzichten opgedaan op het gebied van crisispreparatie. De evaluatie van de oefening is reeds aan uw Kamer verzonden. De evaluatie biedt onder andere aanknopingspunten voor de doorontwikkeling van het Cyberweerbaarheidsnetwerk en voor een volgende actualisering van het Landelijk Crisisplan Digitaal.

Het kabinet wil de dreiging afkomstig van landen met een offensief cyberprogramma gericht tegen Nederlandse belangen zoveel mogelijk tegengaan, en waar mogelijk aan de voorkant ontmoedigen. Dat heeft het afgelopen jaar onder andere geleid tot publicatie over geavanceerdere malware die door China werd gebruikt om te spioneren op computernetwerken van het Ministerie van Defensie. In samenwerking met het NCSC werd een analyse over de werking van deze malware gedeeld, net als diverse beveiligingsmaatregelen. Dit is in lijn met de motie Erkens.[3]

Tenslotte zijn er stappen gezet ten aanzien van de krappe arbeidsmarkt. In opdracht van het Ministerie van Economische Zaken (EZ) is een onderzoek uitgevoerd. Uw Kamer is op 15 mei jl. geïnformeerd over het rapport en de eerste vervolgstappen.[4]

In de bijgevoegde voortgangsrapportage vindt u het uitgebreide overzicht van de voorgang op de verschillende acties.

Recente ontwikkelingen

Cybersecuritybeeld Nederland (CSBN) 2024

Het Cybersecuritybeeld Nederland 2024 (CSBN 2024) biedt inzicht in de digitale dreiging, de belangen die daardoor kunnen worden aangetast, de digitale weerbaarheid en digitale risico's. De focus ligt daarbij op de nationale veiligheid.

In het CSBN 2024 wordt geconcludeerd dat de digitale dreiging voor Nederland groot en divers is, en dat cyberaanvallen voornamelijk afkomstig zijn van statelijke en criminele actoren. Er is sprake van turbulente geopolitieke tijden, en te midden hiervan intensiveren statelijke actoren hun activiteiten en verbreden zij hun capaciteiten. Daarbij maken zij gebruik van een bredere gereedschapskist, waar cyberaanvallen «slechts» een onderdeel van zijn. Statelijke actoren kunnen cyberaanvallen uitvoeren met andere, ook niet-digitale, middelen. Ook kunnen individuele cyberaanvallen in samenhang met elkaar worden ingezet. Die combinaties kunnen grote impact hebben. Criminele actoren voeren op grote schaal aanvallen uit en handelen daarbij opportunistisch. Grootschalige uitval van digitale processen door technische problemen vormt eveneens een dreiging, zoals bijvoorbeeld het recente Crowdstrike incident demonstreert.

[3] Kamerstuk 36 410-X, nr. 46
[4] Kamerstuk 26 643, nr. 1164.

Verder wordt in het CSBN 2024 geconcludeerd dat digitale risico's om een brede manier van beheersing vragen. Digitale risico's staan namelijk niet op zichzelf, maar zijn dynamisch en worden beïnvloed door vele verschillende factoren. Het bredere digitale ecosysteem, met daarbinnen monoculturen, en de hoge mate van digitalisering zorgen ervoor dat risico's met elkaar verbonden raken. Een incident bij een organisatie kan doorwerken naar vele andere organisaties. En niet-vitale organisaties kunnen voor kwaadwillenden een aantrekkelijke springplank zijn naar vitale organisaties.

Verder kunnen ontwikkelingen die ogenschijnlijk niets met cybersecurity van doen hebben, blijvend van invloed zijn op de digitale dreiging en weerbaarheid. Dat geldt bijvoorbeeld voor geopolitieke of technologische ontwikkelingen. Zo vormt een toekomstige krachtige kwantumcomputer, een technologische ontwikkeling, nu al een risico voor de nationale veiligheid. Versleutelde data die nu onderschept en opgeslagen wordt, kan namelijk mogelijk op een later moment ontsleuteld worden met een kwantumcomputer. Een voorbeeld van een niet-digitale factor die van invloed is op digitale risico's, is de mondiale datahandel. Verschillende databedrijven handelen wereldwijd in persoonsgevoelige data van burgers en medewerkers van organisaties. Sommige bedrijven veredelen verkregen persoonsgevoelige data met andere data, stellen profielen op van gebruikers en verkopen deze. De grootschaligheid en precisie van die datahandel en mogelijk misbruik daarvan, kan de nationale veiligheid schaden. Ook criminelen vergaren persoonsgevoelige data, en veredelen en verkopen die aan andere criminelen. Zo worden waardevolle slachtofferprofielen opgesteld, klaar voor gebruik voor allerlei vormen van criminaliteit.

Digitale processen vormen het zenuwstelsel van de maatschappij, en veiligheid van die processen is essentieel. Digitale veiligheid is daardoor onlosmakelijk verbonden met de nationale veiligheid.

Samenhangend Inspectiebeeld cybersecurity vitale processen 2023

Het Samenhangend Inspectiebeeld is opgesteld door de toezichthouders van de Wet beveiliging netwerk- en informatiesystemen (Wbni) en beschrijft de staat van de cybersecurity van vitale aanbieders en vitale processen. In 2023 lag de focus van de toezichthouders op het meerjarige thema risicomanagement. De toezichthouders zien ruimte voor verbetering op het gebied van risicomanagement op bestuursniveau en wijzen op de noodzaak om vanuit risico-oogpunt actuele ontwikkelingen zoals artificiële intelligentie en kwantumcomputers, te volgen. De bevindingen worden betrokken bij het toezicht op de Wbni en op termijn de Cbw.

Cybersecurityraad

De Cybersecurityraad (CSR) heeft als taak het kabinet te adviseren over de uitvoering en uitwerking van de Nederlandse Cybersecuritystrategie. De CSR constateert dat in het huidige geopolitieke klimaat de digitale dreiging toeneemt. De CSR blijft daarom terecht wijzen op het belang van digitale weerbaarheid. Hierbij is vooral het delen van informatie en kennis essentieel, daarom verdient de doorontwikkeling van het Cyberweerbaarheidsnetwerk het komende jaar de aandacht. Temeer omdat dit een oplossing is voor de door de CSR geconstateerde weerbaarheidskloof in het MKB. De CSR-leden vragen daarnaast aandacht voor o.a. de opkomst en ontwikkeling van nieuwe technologieën, zoals kwantum en AI, aandacht voor operationele technologie (OT) en het belang van de implementatie van nieuwe wet- en regelgeving. Daarnaast wijst de CSR op het feit dat voldoende cybersecurityspecialisten voorwaardelijk zijn om

de acties uit de Nederlandse Cybersecuritystrategie te kunnen verwezenlijken. De CSR onderstreept tenslotte het belang van publiek-private samenwerking. Om de doelstellingen uit het actieplan te behalen is samenwerking tussen overheid, bedrijfsleven en wetenschap een voorwaarde om in te kunnen spelen op het snel veranderende speelveld.

Overige moties en toezeggingen

- Motie 36 200-VII-61 van het lid Rajkowski c.s. (VVD) verzoekt de regering om in samenwerking met het Digital Trust Center (DTC), brancheorganisaties en regionale partners een structurele cyberoefenagenda te ontwikkelen met daarin cyberoefeningen specifiek gericht op niet-vitale bedrijven. Op de DTC website kunnen ondernemers aan de slag met de toegezegde cyberoefening die partijen zelf – zonder begeleiding – kunnen uitvoeren.[5] Ik beschouw deze motie als afgedaan.
- De Minister van EZ heeft aan het lid Rajkowski (VVD) toegezegd (TZ202405-001) dat in de voortgangsrapportage van de NLCS zal worden ingegaan op de verschillende punten met betrekking tot de samenwerking en het delen van informatie bij acute dreigingen bij bedrijven. In de voortgangsrapportage ga ik op pagina 9 in op de doorontwikkeling van het Cyberweerbaarheidsnetwerk en Cyclotron waar dit onderdeel van is. Ik zal de Kamer hier in de komende voortgangsrapportages over blijven informeren. Ik beschouw de toezegging hiermee als afgedaan.
- Het Centraal Bureau voor de Statistiek (CBS) zal voor de uitvoering van motie 36 270-9 van het lid Kathmann (PvdA-GL) in de jaarlijkse Cybersecuritymonitor onderzoeken hoeveel bedrijven hun digitale hulpverlening hebben ingericht en op welke manier. In verband met de doorlooptijd van de metingen van het CBS zal dit vraagstuk terugkomen in de Cybersecuritymonitor van 2025. Het DTC heeft op haar website informatie opgenomen over op welke manieren bedrijven digitale hulpverlening in hun organisatie kunnen vormgeven. Het DTC brengt deze informatie actief onder de aandacht bij ondernemers. Hiermee is de motie opgenomen in de staande werkprocessen van het CBS en het DTC.
- Toezegging TZ202405-052 van de Minister van EZ om in de volgende voortgangsrapportage van de NLCS de conclusies en aanbevelingen uit het rapport van Dialogic *Evaluatiekader en nulmeting Nederlandse Cybersecuritystrategie* mee te nemen. De conclusies van Dialogic zijn waar relevant meegenomen in de voortgangsrapportage en zullen betrokken worden bij de evaluaties in 2026 en 2028. Ik beschouw deze toezegging als afgedaan.
- Toezegging TZ202405-053 van de Minister van EZ dat in de volgende voortgangsrapportage van de NLCS een voorbeeld casus wordt opgenomen naar aanleiding van de genoemde punten van het lid Six Dijkstra (NSC), met betrekking tot de risico's van het gebruik van mogelijk onveilige apparaten verbonden met het internet, zoals routers en security first, bij aanbestedingen. Deze voorbeeld casus is opgenomen in de voortgangsrapportage op pagina 11. De toezegging beschouw ik hiermee als afgedaan.
- Toezegging TZ202405-054 van de Minister van EZ dat voortaan in de voortgangsrapportage van de NLCS het bestuurlijk convenant digitale veiligheid wordt meegenomen. Deze is opgenomen in de voortgangsrapportage op pagina 14. De toezegging beschouw ik hiermee als afgedaan.
- De Minister van EZ zegt toe (TZ202405-058) om bij de voortgangsrapportage NLCS te reflecteren op de vraag van het lid Six Dijkstra met

[5] https://www.digitaltrustcenter.nl/oefen

betrekking tot de (de)centralisatie aangaande cybersecurityorganisaties. In Nederland zijn (wettelijke) taken op het gebied van cybersecurity belegd bij verschillende organisaties, zodat aansluiting kan worden gezocht bij bestaande expertise. Een voorbeeld hiervan is het nationale coördinatiecentrum NEXIS, dat Europese subsidies voor cybersecurity innovaties verstrekt en voortbouwt op bestaande expertise binnen de Rijksdienst voor Ondernemend Nederland. Tegelijkertijd kunnen er in sommige gevallen schaalvoordelen worden behaald, bijvoorbeeld als er sprake is van tijdsdruk zoals bij het informeren van organisaties over dreigingen en kwetsbaarheden. Het kabinet heeft er daarom in de NLCS voor gekozen om te bouwen aan een nationaal CSIRT, waarin het NCSC, het DTC en het CSIRT DSP samen gaan. Tegelijkertijd hecht het kabinet ook aan het opbouwen en behouden van sectorale expertise waar dit functionele voordelen biedt, zodat cybersecurity een breed gedragen opgave blijft. De toezegging beschouw ik hiermee als afgedaan.

- Toezegging van de Minister van JenV aan het lid Six Dijkstra (NSC) over kwantumproof vitale sectoren in het Commissiedebat op 4 juni 2024 (Kamerstuk 30 821, nr. 233). Op pagina 13 van de voortgangsrapportage wordt ingegaan op de ontwikkelingen om de risico's van post-quantumcomputing te beheersen. Ik beschouw de toezegging hiermee als afgedaan.
- De ontwikkelingen rondom kunstmatige intelligentie (AI) gaan snel en dat biedt kansen en risico's voor cybersecurity. Om die reden heeft het Ministerie van EZ een verkenning laten uitvoeren naar de raakvlakken van cybersecurity en AI door TNO. In het bijgevoegde verkenningsrapport worden het belang, de kansen, uitdagingen en kwetsbaarheden van het gebruik van AI voor cybersecurity beschreven.

De Minister van Justitie en Veiligheid,
D.M. van Weel