Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 1072 **BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 9 oktober 2023

Een digitaal weerbare samenleving is essentieel voor een veilig en welvarend Nederland. Digitale weerbaarheid is een prioriteit voor dit kabinet. De digitale dreiging is onverminderd groot, de afhankelijkheid van digitalisering neemt toe en het organiseren van digitale weerbaarheid binnen organisaties is nog steeds niet de norm. Ook afgelopen jaar hebben zich tal van incidenten voorgedaan die de noodzaak tot het nemen van maatregelen onderstrepen. Denk hierbij aan de DDOS-aanvallen, geclaimd door de pro-Russische hacktivisten van Killnet, op de websites van verschillende ziekenhuizen in Nederland of de aanzienlijke economische schade als gevolg van de ransomware-aanval op de stad Antwerpen op 6 december 2022. Het herstel hiervan zal de stad minstens 95 miljoen euro gaan kosten.[1] In het Cybersecuritybeeld Nederland 2023 (CSBN2023) dat op 3 juli 2023 met uw Kamer is gedeeld worden deze en vele andere incidenten verder toegelicht (Kamerstuk 26 643, nr. 1045). Wat dit ons vooral laat zien is dat de digitale dreiging voor de Nederlandse samenleving onverminderd groot is en dat er nog altijd complicaties bestaan voor risicobeheersing. We moeten gezamenlijk stappen zetten om onze digitale weerbaarheid te verhogen.

In oktober 2022 heeft het kabinet de Nederlandse Cybersecuritystrategie (NLCS) gepubliceerd (Kamerstuk 26 643, nr. 925). In deze strategie staan de ambities en plannen voor een digitaal weerbaar Nederland voor de komende zes jaar beschreven. Met deze brief bied ik, mede namens het kabinet, de voortgangsrapportage 2023 aan waarin uiteen is gezet welke resultaten afgelopen jaar zijn behaald. Daarnaast zal in deze brief de appreciatie van het kabinet worden gegeven van het CSBN2023, het Inspectiebeeld Cybersecurity 2022 en andere relevante ontwikkelingen op het cybersecurityterrein en de impact hiervan op de strategie en het actieplan. Tenslotte ontvangt u een update rond de doorontwikkeling van de monitoring en governance van de NLCS.

[1] Gazet van Antwerpen, https://www.gva.be/cnt/dmf20230616_92935237, 16 juni 2023.

kst-26643-1072
ISSN 0921 - 7371
's-Gravenhage 2023

Afgedane moties en toezeggingen

Met deze brief doe ik de volgende moties en toezeggingen af:

- Toezegging van de Minister van de Minister van Justitie en Veiligheid aan de vaste commissie voor Digitale Zaken dat de Minister de Kamer jaarlijks informeert over de voortgang van de NLCS en het inzichtelijk maken van de structuur rond cybersecurity. Met de voortgangsrapportage wordt voor 2023 voldaan aan de toezegging. Daarnaast wordt met het bijgevoegde overzicht van strategieën en beleidsnota's aangaande cybersecurity inzicht geboden in de structuur van het stelsel.
- Toezegging van de Minister van Economische Zaken en Klimaat aan dhr. van der Staaij (SGP) om een overzicht te geven van het kabinetsbeleid tegen digitale aanvallen van statelijke dreigingen en het bieden van inzicht in de effectiviteit hiervan. De NLCS en de voortgangrapportage bieden dit overzicht. Het overzicht zal de komende jaren worden uitgebreid. In deze brief wordt daarnaast uiteen gezet op welke wijze op termijn inzicht wordt gegeven in de effectiviteit van de strategie.
- Tijdens het commissiedebat Cybercrime van 30 maart jl. (Kamerstukken 26 643 en 29 911, nr. 1015) heb ik toegezegd aan de Vaste Kamercommissie Justitie en Veiligheid de Kamer te informeren over bestaande meldplichten bij ransomware aanvallen. In bijlage III bij deze brief vindt u een overzicht van de meldplichten die raken aan het fenomeen ransomware.
- Motie van het lid Slootweg aan de Staatssecretaris van Koninkrijksrelaties en Digitalisering om medeoverheden zo snel mogelijk duidelijkheid te geven over de scope van NIS2, hen te betrekken bij de nadere uitwerking van de richtlijn en te ondersteunen bij implementatie van de richtlijn. De Staatssecretaris van Koninkrijksrelaties en Digitalisering verschaft de koepels duidelijkheid met een brief over de gevolgen van NIS2 voor medeoverheden. Met deze brief wordt invulling gegeven aan de motie van het lid Slootweg.[2]

Voortgangsrapportage 2023

De NLCS is nu een jaar in gebruik. Afgelopen jaar is het kabinet samen met het brede veld aan publieke en private partijen aan de slag gegaan om de doelstellingen van de strategie te realiseren door het uitvoeren van het actieplan van de NLCS. Zo is er dit jaar gestart met de integratie van het Nationaal Cyber Security Centrum (NCSC), het Digital Trust Center (DTC) en het Computer Security Incident Response Team voor digitale dienstverleners (CSIRT-DSP) tot de vernieuwde nationale cybersecurityorganisatie. Door het bundelen van de krachten ontstaat één helder aanspreekpunt voor organisaties in Nederland en daarbuiten. Vanuit dit informatieknooppunt worden deze organisaties, groot of klein, publiek of privaat, vitaal en niet-vitaal, van passende informatie en kennis voorzien op het gebied van cybersecurity. In aanvulling daarop bieden enkele sectorale CSIRT's binnen het stelsel maatwerk ondersteuning aan hun specifieke sectoren. Ook is in december 2022 het Landelijk Crisisplan Digitaal gepubliceerd, dit plan biedt de basis voor de landelijke crisisaanpak voor digitale incidenten. Daarnaast is op Nederlands initiatief in het onderhandelingsmandaat van de Raad van de EU voor de Cyber Resilience Act opgenomen dat de zorgplicht voor fabrikanten en leveranciers moet gelden voor de gehele levensduur van digitale producten. Dit draagt bij aan een veiliger digitaal ecosysteem, en aan meer vertrouwen onder consumenten en bedrijven. Deze en andere ontwikkelingen worden nader beschreven in de voortgangsrapportage NLCS 2022–2023.

[2] Kamerstuk 26 643, nr. 1049.

Naast een terugblik op het afgelopen jaar biedt de aanbieding van de jaarlijkse voortgangsrapportage ook de mogelijkheid om acties aan te passen of uit te breiden. Het aan de NLCS onderliggende actieplan is zo opgesteld dat indien er zich tijdens de doorlooptijd van de strategie ontwikkelingen voordoen die relevant zijn voor het uitvoeren van de strategie het kan worden actieplan aangepast. De belangrijkste ontwikkelingen 2022–2023 zijn beschreven in het CSBN2023 en het inspectiebeeld cybersecurity 2023. Daarnaast is ook de Cyber Security Raad (CSR) gevraagd om aan te geven of zij ontwikkelingen zien die vragen om een aanpassingen van het actieplan.

Ontwikkelingen 2022–2023: inzet cybersecurity onverminderd nodig

Cyber Security Beeld Nederland 2023 – «Verwacht het onverwachte»

Het CSBN2023 onderschrijft de noodzaak voor onze blijvende inzet ten aanzien van cybersecurity.[3] De digitale dreiging in Nederland is onverminderd groot. Het CSBN2023 constateert dat er sprake is van geopolitieke verharding wat zich weerspiegeld ziet in het digitale domein. De Russische oorlog tegen Oekraïne is hierin het meest prominente voorbeeld en laat zien dat statelijke actoren naar cyberaanvallen grijpen als middel om hun belangen te behartigen.
Ook wordt de toenemende specialisatie onder cybercriminelen beschreven waardoor zij steeds afhankelijker worden van elkaars (online) diensten in het kader van cybercrime-as-a-service. Deze afhankelijkheid geldt ook voor het afnemen van legale diensten, zoals webhosting en communicatiediensten als VPN of domeinregistraties.
Daarnaast wordt in het CSBN2023 gewezen op het feit dat cybersecurityrisico's zich voordoen over de hele breedte van de organisaties en hun leveranciersketens niet alleen de digitale. Een voorbeeld hiervan is een incident uit 2023 waarbij verschillende grote organisaties, waaronder de NS en Vodafone, getroffen werden door een indirecte datalek. Deze organisaties huurde onderzoeksbureaus in voor klantonderzoek. Die onderzoeksbureaus maakten gebruik van dezelfde softwareleverancier. Toen zich bij die softwareleverancier een datalek voordeed als gevolg van een ransomware aanval, kwamen de gegevens van naar schatting rond de twee miljoen Nederlanders in de openbaarheid. Klanten van de getroffen organisatie werden slachtoffer van een datalek bij de IT-leverancier van de dienstverlener van de organisatie, oftewel in de derde lijn. Dit vraagt, aldus het CSBN2023, om een andere en bredere blik op risicomanagement bij organisaties.
Er wordt ook geconstateerd dat ondanks alle weerbaarheid verhogende maatregelen die organisaties nemen, het niet altijd mogelijk is om incidenten te voorkomen. Daarom is het voorbereiden op incidenten van groot belang.
Het voorgaande CSBN2022 benoemt tenslotte strategische thema's die (mede) de grondslag vormen voor de geformuleerde NLCS doelstellingen en acties. Deze onderliggende strategische thema's zijn nog steeds actueel en zorgen nog altijd voor complicaties voor risicobeheersing. Wel constateert het CSBN2023 enkele ontwikkelingen binnen deze thema's, zoals het onder druk komen te staan van de verzekerbaarheid van digitale risico's, de ontwikkeling van generatieve artificiële intelligentie (AI) maakt het uitvoeren van digitale aanvallen makkelijker en de groeiende kwetsbaarheid van de beveiliging van operationele technologie (OT).

[3] Cybersecuritybeeld Nederland 2023, https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland.

Samenhangend Inspectiebeeld

Het Samenhangend Inspectiebeeld is gezamenlijk 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.[4] Het inspectiebeeld is 3 juli jl. met uw Kamer gedeeld.[5]

De belangrijkste rode draad uit het rapport betreft het onderwerp risicomanagement. Net als in het jaar 2021 besteedden alle toezichthouders in 2022 aandacht aan dit onderwerp. De toezichthouders zien dat het risicomanagementproces bij vitale aanbieders is verbeterd – mede als gevolg van de inspectiewerkzaamheden – en dat organisaties ook op bestuursniveau steeds meer betrokken raakten bij dit onderwerp. Daarnaast hebben vitale aanbieders steeds meer aandacht voor de steeds complexere digitale dreigingen in de leverancierskketens. Op basis van de inspectieresultaten zien de toezichthouders dat er ruimte is om de cyberhygiëne (de basismaatregelen voor cybersecurity) te verbeteren en het risicomanagementproces naar een hoger niveau te tillen.

Stevige inzet op het blijven versterken van de digitale veiligheid van vitale aanbieders zal noodzakelijk zijn en toezicht speelt hierin een belangrijke rol. Deze rol zal de komende jaren alleen maar toenemen als er na de implementatie van de NIS2-richtlijn duizenden nieuwe organisaties in Nederland onder toezicht komen te staan. Het rapport is aangeboden aan alle bewindspersonen betrokken bij het toezicht op de Wbni, met als doel hen in staat te stellen waar nodig maatregelen te nemen en aanbevelingen op te volgen.

Cybersecurityraad

De Cyber Security Raad (CSR) heeft als taak het kabinet te adviseren over de uitvoering en uitwerking van de Nederlandse Cybersecuritystrategie. De CSR wordt gevraagd om periodiek te adviseren over de ontwikkelingen die meegewogen moeten worden in de herijking van het actieplan. De Cyber Security Raad (CSR) geeft aan dat er, in lijn met het CSBN2023, toenemende zorgen zijn over de mate van verwevenheid binnen het digitale ecosysteem. Tegelijkertijd constateert de raad dat het actieplan van de NLCS een breed scala aan acties bevat die een goede basis bieden om de digitale veiligheid van Nederland te vergroten. De CSR adviseert daarom primair in te zetten op realisatie van de al opgenomen activiteiten en slechts beperkt in te zetten op extra activiteiten. Wel vraagt de CSR extra aandacht voor de inzet op het gebied van (generatieve) AI, operationele technologie (OT) en blijvende aandacht voor innovatie.

Gevolgen voor actieplan

De hierboven beschreven ontwikkelingen passen binnen het huidige actieplan. In de voortgangsrapportage is beschreven hoe er binnen de huidige acties wordt omgegaan met bovenstaande recente ontwikkelingen. Het kabinet onderschrijft in het bijzonder de grote impact van technologische ontwikkeling van generatieve AI en werkt daarom aan het uitvoeren van het actieplan AI dat eind 2019 is gepubliceerd, hierin is ook aandacht voor cybersecurity en AI.[6] Technologische ontwikkelingen zoals

[4] Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS), Autoriteit Persoonsgegevens (AP), De Nederlandsche Bank (DNB), Inspectie Gezondheidszorg en Jeugd (IGJ), Inspectie Leefomgeving en Transport (ILT) Inspectie Justitie en Veiligheid (IJenV) en Rijksinspectie Digitale Infrastructuur (RDI).

[5] Kamerstuk 26 643, nr. 1046.

[6] Kamerstuk 26 643, nr. 604.

AI of kwantumtechnologie hebben gevolgen voor cybersecurity op organisatieniveau onder andere omdat de methode van aanvallen en verdedigen veranderen. Daarnaast kunnen criminelen op grotere schaal automatische aanvallen zoals phishing uitvoeren op burgers en bedrijven. De komende periode moeten deze ontwikkelingen nauwgezet gevolgd worden. Het kabinet start daarom met een onderzoek waarin de samenhang tussen AI en cybersecurity nader wordt onderzocht, met nadruk op te verwachte ontwikkelingen, potentiële kwetsbaarheden en mogelijkheden om de digitale veiligheid van Nederland te waarborgen, in een wereld waar AI technologie een steeds grotere rol zal gaan spelen in de maatschappij.

Governance NLCS

Monitoring en rapportagestructuur

De voortgangsrapportage in dit eerste jaar is compact. Veel trajecten zijn nog volop in ontwikkeling of gaan pas in de komende jaren van start. Dit maakt dat nog niet op alle trajecten voortgang te rapporteren is. Daarnaast is de uiteindelijke monitoringsstructuur nog in ontwikkeling. Het streven is om per doelstelling inzichtelijk te maken of de beoogde actie zijn uitgevoerd, of dit volgens plan gebeurde en wat de verandering is ten aanzien van de beginsituatie. Om deze beginsituatie te bepalen wordt momenteel een nulmeting uitgevoerd door een onafhankelijk onderzoeksbureau.[7] Uit de evaluatie van de vorige strategie, de Nederlandse Cybersecurity Agenda (NCSA), bleek dat het moeilijk was om de voortgang en effectiviteit van de maatregelen te bepalen. Mede omdat er geen referentiekader was waaraan de voortgang getoetst kon worden voor de NLCS wordt daarom de nulmeting uitgevoerd. Het uitvoeren van de nulmeting voor de NLCS is een tijdsintensief proces en het rapport met de resultaten wordt begin 2024 verwacht. Deze nulmeting vormt de basis voor de uiteindelijke monitoringsstructuur. De eerste voortgangsrapportage op basis van deze monitoringsstructuur volgt in het najaar 2024.

Naast de jaarlijkse voortgangsrapportage die meer gericht is op de vraag of de geplande acties daadwerkelijk zijn uitgevoerd hebben de tussentijdse (2025) en eindevaluatie (2028) als doel vast te stellen of de doelstellingen van de NLCS zijn bereikt en in welke mate de acties en hun output bij hebben gedragen aan het bereiken van de doelstellingen. Deze evaluaties worden via het WODC door een onafhankelijk onderzoeksbureau uitgevoerd.

Tenslotte wordt er gewerkt aan een brede effectiviteitsmeting van het cybersecuritybeleid in Nederland. Beleid ten behoeve van het verhogen van de digitale weerbaarheid van Nederland is een relatief nieuw domein. Het is belangrijk om de ontwikkeling van de digitale weerbaarheid en de impact van het overheidsbeleid hierop zo goed als mogelijk in kaart te brengen en te meten. Dit draagt bij aan de onderbouwing van toekomstige beleidskeuzes.

Beschikbare middelen

Tijdens het Wetgevingsoverleg van de Vaste Kamercommissie Digitale Zaken op 13 juni 2023 heeft uw Kamer verzocht om een overzicht van de besteding van de verschillende departementen aan het uitvoeren van de NLCS. Ik heb toegezegd om samen met de betrokken vakministers en het Ministerie van Financiën uit te zoeken wat de mogelijkheden zijn en zal dit

[7] Nulmeting Nederlandse Cyber Security Strategie (NLCS) | Welk onderzoek doen we? | WODC – Wetenschappelijk Onderzoek- en Documentatiecentrum.

betrekken bij de departementale jaarverslagen 2024 (Kamerstukken 36 360 VI en 36 360 VII en 36 360 XIII, nr. 22). De gesprekken hierover zijn door het Ministerie van Justitie en Veiligheid opgepakt.

NLCS in samenhang met verschillende digitaliseringsstrategieën

De NLCS is een kader aan de hand waarvan bewaakt wordt dat het cybersecuritybeleid zich op alle niveaus samenhangend en gestructureerd ontwikkelt. De NLCS vormt de cybersecurityinput voor bredere strategieën zoals de «Werkagenda Waardengedreven Digitalisering» of de «Strategie Digitale Economie». Vakdepartementen vertalen dit generieke kader daarnaast naar sectorspecifieke kaders en regelgeving voor de organisaties en processen waar zij een systeemverantwoordelijkheid voor dragen zoals de «Internationale Cybersecurity Strategie». Deze aanpak is nodig omdat digitalisering en daarmee cybersecurity inmiddels onderdeel zijn van vrijwel elk beleidsterrein waardoor het onmogelijk is om alles in een strategie te vangen. Bij de lezer kan dit echter leiden tot verwarring over de samenhang van het digitaliseringsbeleid van het kabinet. Zie daarom bijlage II voor een overzicht van de verschillende strategieën en de samenhang daar tussen.

De Minister van Justitie en Veiligheid,
D. Yeşilgöz-Zegerius