Voortgangsrapportage 2024 Nederlandse Cybersecuritystrategie

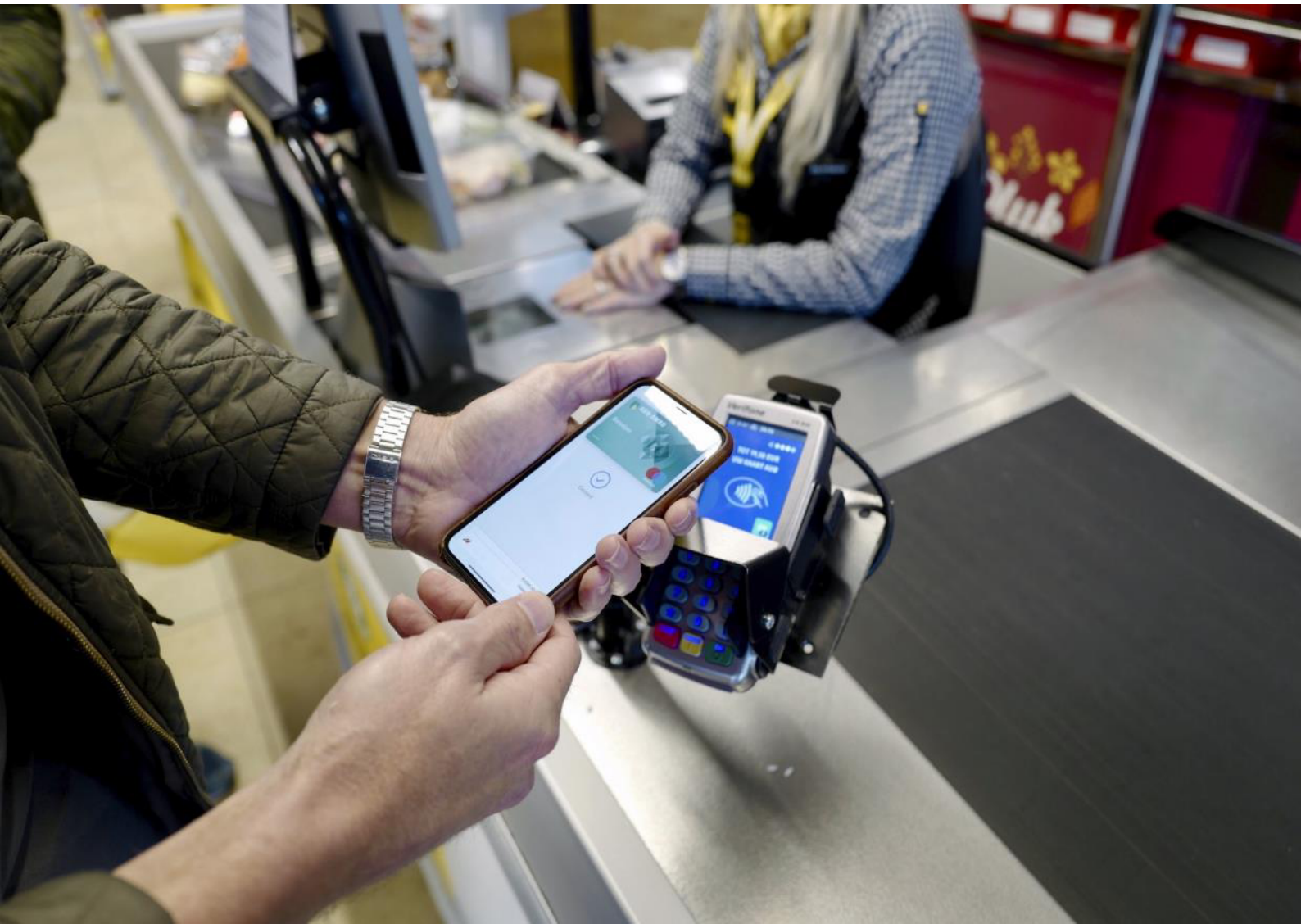

Foto omslag:

We gebruiken steeds minder contant geld. Tegenwoordig gebeurt 81% van de betalingen aan de kassa zelfs contactloos. Dat maakt het nog belangrijker dat ons betalingsverkeer veilig en betrouwbaar is en blijft.

Voortgangsrapportage 2024 Nederlandse Cybersecuritystrategie

Leeswijzer

- De voortgang wordt beschreven op het niveau van de actieclusters uit het actieplan. Dit biedt de mogelijkheid om de acties in samenhang te bespreken. De nummers uit het actieplan corresponderen met de nummers in de voortgangsrapportage.
- De focus ligt bij de onderwerpen die in 2024 moeten worden afgerond en waar belangrijke ontwikkelingen over te melden zijn.
- Wanneer een bepaald onderwerp niet is opgenomen verloopt de uitvoering volgens de planning zoals beschreven in het actieplan.
- Om de voortgangsrapportage overzichtelijk te houden worden de onderwerpen beperkt inhoudelijk ingeleid. De voortgangsrapportage is daarom het beste te lezen in combinatie met de NLCS en het actieplan.

Inhoudsopgave

Digitalisering is een belangrijke stap om zorg voor iedereen toegankelijk te houden en de druk op zorgprofessionals te verminderen. Het maakt het mogelijk om zorg op afstand te verlenen, maar biedt ook sneller toegang tot informatie.

Pijler I

Digitale weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties

Het verhogen van de weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties is een opgave die een vergaande publiek-private samenwerking vergt. Onder pijler I van de Nederlandse Cybersecuritystrategie (NLCS) worden verschillende acties uitgevoerd die deze samenwerking verdiepen en uitbreiden. Deze acties dragen bij aan het realiseren van de ambitie van het kabinet om alle organisaties binnen Nederland in staat te stellen om hun weerbaarheidsniveau te verhogen.

Doel 1: Organisaties hebben zicht op cyberincidenten, -dreigingen en -risico's en hoe hiermee om te gaan.

I.1.1: Herziening van het stelsel

De vernieuwde NCSC organisatie

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) ligt op schema. De samenwerking tussen het DTC, het CSIRT voor digitale diensten en het NCSC wordt op dit moment geïntensiveerd en de vernieuwde NCSC-organisatie krijgt daarmee steeds verder vorm. De verwachting is dat fase 1 van de samenvoeging (NCSC met het CSIRT voor digitale diensten) dit jaar zo veel als mogelijk zal zijn voorbereid, in afwachting van de inwerkingtreding van de Cyberbeveiligingswet in 2025. De verdere samenvoeging tussen het DTC en het NCSC staat voor 2025 op het programma. Dit behelst naast de organisatorische samenvoeging ook een goede doelgroep- en merktransitie: van drie organisaties en doelgroep benaderingen, inclusief bijbehorende merken naar één. Vanaf begin 2026 dienen alle doelgroeporganisaties vanuit één vernieuwde NCSC-organisatie te worden bediend. De vernieuwde NCSC-organisatie voert vanaf 2026 integraal vier hoofdtaken uit: die van Nationaal CSIRT, Sectoraal CSIRT voor specifieke sectoren onder de Cyberbeveiligingswet, Uitvoeringscoördinator en Kennis- en adviescentrum.

De te integreren organisaties werken ondertussen al nauw samen. Op twee terreinen is dat al goed zichtbaar. In de eerste plaats betreft dit intensieve samenwerking tussen het CSIRT-DSP en het NCSC om, in voorbereiding op de invoering van de Cyberbeveiligingswet (Cbw), te komen tot de integratie van de producten, zoals bijvoorbeeld de vijf basisprincipes [1]. Ook wordt er gekeken naar de integratie van diensten en bijbehorende processen van beide organisaties. In de tweede plaats wordt er intensief samengewerkt in een multidisciplinair team bestaande uit medewerkers vanuit zowel het NCSC, het CSIRT voor digitale diensten en het DTC om doelwitten en slachtoffers van dreigingen en incidenten te notificeren. Er wordt door dit team gewerkt aan een technische oplossing die het mogelijk maakt om dreigingsinformatie sneller te verwerken en direct terecht te laten komen bij de doelgroeporganisaties.

[1] De 5 basisprincipes van veilig digitaal ondernemen | Digital Trust Center (Min. van EZ)

Cyclotron

Het afgelopen jaar is er door publieke en private organisaties actief bijgedragen aan de ontwikkeling van het programma Cyclotron. Het programma Cyclotron verbindt hoog volwassen partijen en realiseert de uitwisseling van (ruwe) data tussen deze partijen. Hierdoor is het mogelijk om collectief analyses tot stand te brengen om efficiënter en doeltreffender te handelen bij het bestrijden van cyberdreigingen en incidenten. Partijen kunnen unieke inzichten delen en een dieper begrip ontwikkelen van de methoden, technieken en doelstellingen van cyberaanvallers. Daarnaast zijn de functionele en technische eisen voor het samenwerkingsplatform vastgesteld en worden de eerste versies hiervan voor het einde van het jaar opgeleverd waaronder juridische vereisten, geïdentificeerd voor de doorontwikkeling van deze samenwerking. Intussen zijn er meer dan 10 partijen die via use-cases periodiek data met elkaar uitwisselen en invulling geven aan dit publiek-private samenwerkingsverband. Om goede publiek-private samenwerking te stimuleren en te bouwen aan een trusted community is de governance en sturing van het programma ingericht. Dit bestaat uit een stuurgroep en een publiek-private governance board.

I.1.2: Versterken Landelijk Dekkend Stelsel van cybersecurity samenwerkingsverbanden (LDS)

In 2024 is er met het publiceren van de toekomstvisie voor het Cyberweerbaarheids-netwerk (CWN) een belangrijke stap gezet naar het verdiepen en uitbreiden van publiek-private samenwerking op het gebied van cybersecurity. [2] Hiermee wordt het huidige Landelijk Dekkend Stelsel (LDS) uitgebouwd om te komen tot het CWN. De naam LDS wordt daarmee vervangen door CWN. Het doel van het CWN is om met een brede set groep (publieke en private) organisaties gecoördineerd samen te werken en gezamenlijk de verantwoordelijkheid te dragen en daarmee de digitale weerbaarheid van het Koninkrijk der Nederlanden te vergroten. Met de visie is de actie om te komen tot een communicatieplan LDS afgedaan. Na het publiceren van de toekomstvisie is het opstellen van een bouwplan een belangrijke actie voor de verdere ontwikkeling van het Cyberweerbaarheidsnetwerk. In het bouwplan worden ook de randvoorwaarden voor aansluiting op het CWN geformuleerd, en wordt duidelijkheid geschept over de reikwijdte van het netwerk. Het bouwplan is naar verwachting halverwege 2025 gereed. In samenhang met het bouwplan worden de overige LDS (vanaf nu CWN) acties uitgevoerd.

Het afgelopen jaar zijn stappen gezet ten aanzien van het wijzigen van het wettelijk kader voor cybersecurity informatiedeling door de introductie van de Wet bevordering digitale weerbaarheid bedrijven (Wbdwb). Deze wet zet de taken en bevoegdheden van de minister van Economische Zaken uiteen op het terrein van digitale weerbaarheid van niet-vitale bedrijven in Nederland, zoals het verwerken en verspreiden van informatie over kwetsbaarheden, dreigingen en incidenten en het samenwerken met andere bestuursorganen en organisaties. Deze wet vormt een grondslag om vanuit de overheid niet-vitale Nederlandse bedrijven te kunnen waarschuwen over digitale kwetsbaarheden, cyberdreigingen en beveiligingslekken.

I.1.3: Uitbreiden schakelorganisaties binnen het CWN

Op 14 december 2023 heeft het bestuur van het Interprovinciaal Overleg (IPO) in aanwezigheid van de toenmalig staatssecretaris voor Koninkrijksrelaties en Digitalisering het besluit genomen om zich in 2024 aan te sluiten bij het CSIRT van het Nationaal Cyber Security Centrum (NCSC) en op die manier invulling te geven aan de actie I-1.3.2 in de NLCS. In het kader van de Cyberbeveiligingswet (voortvloeiend uit de NIS2-richtlijn) krijgen provincies en IPO hiermee toegang tot actuele dreigingsinformatie over cyberaanvallen en ondersteuning bij incidenten. Het NCSC zal tevens fungeren als sectoraal CSIRT voor de provinciale bestuurslaag. Momenteel geven het NCSC en de provincies nadere uitwerking aan hoe deze dienstverlening eruit komt te zien. Het CERT watermanagement is daarnaast versterkt door Infrastructuur en Waterstaat door nauw samen te werken met de Unie van Waterschappen, Rijkswaterstaat en andere stakeholders.

Het afgelopen jaar is het Computer Emergency Response Team (CERT) voor het funderend onderwijs van start gegaan. In de proeffase is een aantal scholen aangesloten voor dreigingsinformatie en hulp bij cyberaanvallen. Komende periode zal het CERT verder verankerd worden.

I.1.4: Nationaal Detectie Netwerk

Middels het Nationaal Detectie Netwerk (NDN) werken overheidsorganisaties samen om geavanceerde digitale aanvallen beter waar te nemen. Het afgelopen jaar is het project om de laatste relevante rijksoverheidsorganisaties aan te sluiten op het NDN afgerond. [3]

Voor het NDN wordt een meerjarenplan ontwikkeld om het netwerk te moderniseren. Het NDN is meer dan 10 jaar geleden opgericht. De veranderingen in wetgeving (Cbw) en technische uitdagingen maken het nodig om de samenwerking in dreigingsdetectie en monitoring tussen het NCSC, de AIVD, de

[2] Kamerstukken II, 2023–24, 26 643, nr. 1176.
[3] Kamerstukken II, 2023–2024, 31 490, nr. 338

MIVD en aangesloten partners te herijken en door te ontwikkelen. Het meerjarenplan is in 2025 gereed.

I.1.5: Doelwit- en Slachtoffernotificatie

Het onderzoek om vast te stellen op welke manier bedrijven en burgers die doelwit dreigen te worden of slachtoffer zijn van digitale incidenten geïnformeerd kunnen worden is afgerond. Hierbij is een visie voor doelwit- en slachtoffernotificatie geformuleerd die geoperationaliseerd wordt door het NCSC. Gezamenlijk wordt er op deze manier gewerkt om alle organisaties en burgers (via netwerkeigenaren zoals bijvoorbeeld internet service providers of managed service providers) in Nederland te waarschuwen in het geval ze doelwit of slachtoffer zijn van een cyberdreiging. Hierbij werkt de overheid nauw samen met publiek-private partners, ook binnen het toekomstige CWN. Daar waar voorheen structureel over 24 soorten cyberdreigingen werd genotifieerd is dit inmiddels opgeschaald naar 55 urgente dreigingen. De verwachting is dat het NCSC eind 2024 over alle soorten cyberdreigingen kan notificeren.

Daarnaast worden de mogelijkheden voor notificatie uitgebreid als gevolg van de komende implementatie van de Cbw/NIS2-richtlijnen de uitbreiding taakstelling van de vernieuwde NCSC-organisatie. Ook wordt ingezet op waar mogelijk meer structurele informatie-uitwisseling met het Openbaar Ministerie en de politie. De beoogde aanpassing van het Besluit Politiegegevens stelt de politie in staat slachtoffer- en dreigingsinformatie structureel te delen met NCSC. De beoogde datum van de inwerkingtreding van deze wet is januari 2025.

Doel 2: Organisaties zijn goed beschermd tegen digitale risico's, en nemen hierin hun belang voor de sector en andere organisaties in de keten mee.

I.2.1: Digitale weerbaarheid vitale infrastructuur

NIS2-richtlijn

Zoals eerder aan de Tweede Kamer is medegedeeld zal de NIS2-richtlijn niet in 2024 worden geïmplementeerd. [4] De Cyberbeveiligingswet (Cbw), die deze richtlijn zal implementeren is inmiddels in consultatie geweest. De verwachting is dat het wetsvoorstel in Q4 2024 aan de Afdeling Advisering van de Raad van State kan worden aangeboden. In de op 17 oktober 2024 verstuurde Kamerbrief zet de minister van Justitie en Veiligheid uiteen hoe wordt omgegaan met de overgangsperiode tussen de implementatiedeadline van de richtlijn en de inwerkingtreding van de Cbw.

De wetsvoorstellen voor de Cbw en de Wet weerbaarheid kritieke entiteiten (Wwke), die de Europese richtlijn weerbaarheid kritieke entiteiten (CER-richtlijn) implementeert, zijn parallel aan elkaar opgesteld en op elkaar afgestemd. Beide wetten kennen dezelfde structuur en hetzelfde tijdspad. Sinds 2023 zijn er door verschillende instanties en overheidsorganisaties communicatieproducten opgesteld om organisaties te informeren over hun nieuwe status onder de Cbw en Wwke en hen te helpen bij de voorbereidingen om te voldoen aan de aankomende wetgeving.

De verkenning naar een centraal NIS2-meldloket is afgerond en het NCSC ontwikkelt als opvolging een centrale meldfunctionaliteit in samenwerking met de toezichthouders, de vakdepartementen en de andere beoogde CSIRTs. De verwachting is dat deze in oktober 2024 beschikbaar is, zodat vrijwillige meldingen van incidenten, voor zover nodig onder de Cbw, al via deze functionaliteit kunnen worden gedaan.

Het NCSC past haar dienstverlening aan om tegemoet te komen aan de uitbreiding van het aantal doelgroeporganisaties. In 2024 is het dienstverleningsportaal van het NCSC beschikbaar gekomen voor de eerste groepen gebruikers. Via dit portaal worden kennisproducten en datagedreven informatieproducten beschikbaar gesteld.

Het voornemen bestaat om de zorgplicht vanuit de Cbw voor de sector overheid in te vullen via wettelijke verankering van de Baseline Informatiebeveiliging Overheid (BIO). Aanvullende eisen worden zover mogelijk meegenomen in actualisatie van de BIO (BIO2). De publieke consultatie van de BIO2 is in augustus 2024 afgerond. De BIO2 is voorzien om eind 2024 van kracht te worden. Wanneer de Cyberbeveiligingswet in werking is getreden, zal deze ook wettelijk verankerd kunnen worden.

Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) heeft het afgelopen jaar gewerkt aan het in kaart brengen van mogelijke acties om de cyberweerbaarheid voor de Openbare Lichamen binnen het Koninkrijk te versterken. Dit gaat onder meer om het opzetten van awareness trainingen, een inventarisatie van de huidige juridische kaders en bepalingen voor digitale weerbaarheid bij de openbare lichamen en een verkenning naar ondersteuning voor implementatie normenkaders zoals ISO2700x of de BIO. Daarnaast is gewerkt aan de aansluiting van de Openbare Lichamen op de Informatiebeveiligingsdienst (IBD).

[4] Kamerstukken II, 2023–2024 51 936 nr.78

Aanpak vitale infrastructuur

Het instrumentarium van de cyclus vitaal is in 2023 geactualiseerd. De beleidsverantwoordelijke departementen worden geacht om periodiek (en minimaal vierjaarlijks) de cyclus vitaal te doorlopen voor hun vitale processen. Dit omvat het uitvoeren van een vitaalbeoordeling, een weerbaarheidsanalyse en een actieprogramma.

Om informatie-uitwisseling over relevante dreigingen en risico's binnen de cyclus vitaal te structuren en stimuleren, zet de NCTV in samenwerking met de inlichtingen- en veiligheidsdiensten en het NCSC eind 2024/2025 een aantal initiatieven op.

Op het gebied van satellietsystemen GNSS/PNT [5] heeft de AIVD op nationaal en internationaal niveau geadviseerd over weerbaarheid verhogende maatregelen in relatie tot Galileo. De AIVD levert vanuit de c-taak voor verschillende sectoren structureel bijdragen ten bate van realistische dreigingsscenario's en effectieve en efficiënte maatregelen. De dienst participeert eveneens actief in projecten ter bescherming van de vitale infrastructuur. De AIVD investeert extra in bestuurlijk overleg met sectoren. De AIVD participeert in verschillende (transitiegerelateerde) cybersecuritytrajecten in de energiesector met toelichting op dreiging vanuit AIVD -taakvelden en als sparringspartner voor maatregelen. Voor deze en andere vitale processen zijn dreigings-, weerbaarheids- of risicoanalyses opgesteld. Verder bracht de AIVD brochures en producten uit als de "position paper Quantum Key Distribution''.

Risicomanagement inkoop door vitale aanbieders

Tijdens het Tweede Kamerdebat 'Online Veiligheid en Cybersecurity' van de vaste Kamercommissie Digitale Zaken op 11 april 2024 is door de minister van Economische Zaken en Klimaat aan lid Six Dijkstra toegezegd dat er in de voortgangsrapportage van de NLCS een voorbeeld van een casus wordt opgenomen onder welke omstandigheden het gebruik van met het internet verbonden apparatuur afkomstig uit landen met een offensief cyberprogramma binnen een vitale organisatie verantwoord kan plaatsvinden. Dit om een schets te geven van hoe het kabinet in dit type casuïstiek aanstuurt op risicomanagement binnen de (inkoop)keten. Het kabinet voert een landenneutraal beleid i.r.t. aanbestedingstrajecten. Daarbij wordt er, vanwege de geopolitieke situatie, continue aandacht besteed aan mogelijke dreigingen vanuit landen met een offensief cyberprogramma gericht tegen Nederlandse belangen. Dat betekent dat het inzichtelijk maken van onze afhankelijkheden van toeleveranciers uit het buitenland de prioriteit heeft binnen het Rijk maar ook bij vitale aanbieders. Dit doen we met de versteviging van risicomanagement o.a. binnen de (inkoop)keten. [6]

Vitale aanbieders dienen bij het in gebruik nemen van producten en diensten goed risicomanagement uit te voeren. Het analyseren van mogelijke risico's is gestoeld op het in kaart brengen van (1) de te beschermen belangen, (2) de dreiging tegen deze belangen te identificeren en (3) de bestaande weerbaarheid van de organisatie te definiëren. (4) Op basis van deze analyse kunnen aanvullende maatregelen getroffen worden om de risico's te beheersen. Het doel is om uiteindelijk tot een passend niveau van weerbaarheid te komen en de mate van risicoacceptatie te bepalen.

Een situatie of casus waarbij aan het internet verbonden apparaten uit landen met een offensief cyberprogramma verantwoord gebruikt kunnen worden is er een waarbij vastgesteld kan worden dat de te beschermen belangen niet geraakt worden of in voldoende mate beschermd zijn. Deze situatie kan zich in de praktijk op verschillende manieren voordoen. Zo kan het zijn dat het te beschermen belang niet in contact staat of in contact kan komen met dergelijke apparaten of kan het zijn dat bestaande of aanvullende weerbaarheidsmaatregelen voldoende waarborg geven voor het verantwoord in gebruik nemen van dergelijke apparaten.

Het bij voorbaat weren van partijen uit landen met een offensief cyberprogramma neemt cyberrisico's niet weg, omdat de risico's afhankelijk zijn van verschillende factoren. Een typerend voorbeeld in deze is het COATHANGER-incident. Er werd spionage-software aangetroffen op aan het internet verbonden apparaten bij het ministerie van Defensie (DEF). Deze apparaten waren juist niet afkomstig uit een land met een offensief cyberprogramma gericht tegen Nederland. Het stelselmatig uitsluiten van apparatuur zou in deze situatie niet gezorgd hebben voor een verhoogde beveiligingswaarde. Statelijke actoren kunnen namelijk andere middelen inzetten om toegang te krijgen tot het netwerk. Het is daarom belangrijk om per casus de juiste, proportionele beveiligingsmaatregelen te treffen en daarbij ook oog te hebben voor andere belangen, zoals nut en noodzaak, beschikbaarheid, prijs en kwaliteit van alternatieven.

I.2.2: Digitale weerbaarheid MKB en bedrijfsleven

Het NCSC en het DTC hebben het afgelopen jaar diverse kennis- en adviesproducten ontwikkeld over cybersecurity in het risicomanagementproces, crisispreparatie en incidentrespons. Het gaat daarbij niet alleen om producten die relevant zijn voor organisaties die onder het toepassingsbereik van Cbw vallen, maar ook andere organisaties. Daarnaast is er door het NCSC en het DTC een nieuwe set cybersecurity basisprincipes geschreven. [7]

---

5 GNSS is de afkorting voor «Global Navigation Satellite System» en staat voor de verzameling van satellietsystemen voor positie, navigatie- en tijdsbepaling. In veel gevallen maken (vitale) processen gebruik van plaats- en tijdbepaling met GNSS (hierna «PNT»).

6 Cybercheck: ook jij hebt supply chain risico's! | Publicatie | Nationaal Cyber Security Centrum (ncsc.nl)

7 https://www.ncsc.nl/documenten/publicaties/2023/december/01/infosheet_basismaatregelen

Om in publiek/privaatverband nog sneller en beter samen te werken heeft het NCSC gewerkt aan het digitaliseren van onder andere de kwetsbaarheden. Hierbij wordt gebruik gemaakt van kwetsbaarheidsregisters om zo organisaties snel van advies te kunnen voorzien. Dit gebeurt mede in samenhang met het programma Cyclotron.

De Cyber Security Raad (CSR) heeft op 4 juni jl. het adviesrapport 'Verkleinen van de cyberweerbaarheidskloof' overhandigd aan de toenmalig minister van Economische Zaken en Klimaat. Deze kloof gaat over de grote verschillen tussen bedrijven die hun cyberweerbaarheid op orde hebben, ook wel de voorlopers genoemd en achterblijvers bij wie dit nog niet het geval is. Het advies richt zich met name op het midden- en kleinbedrijf (mkb), omdat in die groep relatief veel achterblijvers blijken te zijn. Het adviesrapport bevat concrete aanbevelingen aan de Rijksoverheid om samen met brancheorganisaties, ICT-leveranciers en het mkb de cyberweerbaarheidskloof te verkleinen. De adviezen zijn herkenbaar en worden in publiek-privaat verband verder uitgewerkt.

I.2.3: Digitale weerbaarheid onderwijs

In 2024 is het normenkader voor informatiebeveiliging en privacy binnen het funderend onderwijs geactualiseerd om beter aan te sluiten bij de beleving van scholen. Met het nieuw ontwikkelde groeipad kunnen scholen stap voor stap werken aan hun informatiebeveiligingsnormen. Het groeipad is opgeknipt in fases: gaandeweg wordt gewerkt aan het behalen van het juiste niveau. [8]

Schoolbesturen in het funderend onderwijs zijn vanaf 2024 verplicht om het onderwerp informatiebeveiliging en privacy als maatschappelijk thema op te nemen in het bestuursverslag. De verwachting is dat deze rapportages vanaf 2025 tot een verbeterd inzicht zullen leiden.

Ook is er het afgelopen jaar in de gehele onderwijssector ingezet op het verhogen van de bewustwording van digitale risico's doormiddel van oefeningen, bijeenkomsten en weerbaarheids-testen van het primair tot het wetenschappelijk onderwijs.

In juni 2024 is het sectorbeeld digitale veiligheid gepresenteerd voor het mbo, hbo en wo. Hier hebben bijna alle instellingen aan meegedaan. Het sectorbeeld is opgesteld op basis van het gezamenlijke toetsingskader wat ook de basis vormt voor de externe audit op alle instellingen die uitgevoerd zal worden in de periode 2024 en 2025.

Het merendeel van de instellingen in het mbo, hbo en wo is inmiddels aangesloten op een Security Operations Center (SOC). Tegelijkertijd wordt de bestaande centraal georganiseerde SOC doorontwikkeld (SOC2.0) die aangepast wordt naar de aangescherpte eisen en behoeften van de instellingen.

I.2.4: Digitale weerbaarheid zorginstellingen

Zorgaanbieders zijn op grond van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) verplicht om te voldoen aan de NEN-7510 norm. Deze norm voor informatie-beveiliging in de zorgsector in Nederland wordt eind 2024 herzien[9]. In 2025 start de Stichting Koninklijk Nederlands Normalisatie Instituut (NEN) met de ontwikkeling van implementatietools op basis van de nieuwe versie van de norm. Deze tools worden gratis beschikbaar gesteld.

De open-source Kwetsbaarheden Analyse Tool (OpenKAT) is een tool die door alle zorginstellingen gebruikt kan worden om actief te scannen op kwetsbaarheden in hun eigen systemen. In 2024 is ingezet op het verder uitwerken van de basisscanfunctionaliteit en compliancy tools van OpenKAT. Z-CERT is voornemens vanaf oktober 2024 OpenKAT te gaan inzetten voor het scannen van online omgevingen van een groot aantal zorginstellingen. Daarnaast zet Z-CERT zich in voor het stapsgewijs uitbreiden van het aantal aangesloten zorgsectoren en worden in 2024 de ambulancezorg, gehandicaptenzorg en de verpleeg-, verzorgings-huizen en thuiszorg aangesloten. Het programma Informatieveilig gedrag in de zorg voorziet zorginstellingen van manieren om informatieveilig gedrag te bevorderen. Het aantal zorgorganisaties dat aan de slag gaat met deze methode groeit. [10]

In 2024 heeft Z-CERT samen met de Nederlandse Bank en CIO-Rijk het Advanced Red Teaming framework ontwikkeld dat gebruikt kan worden voor het uitvoeren van testactiviteiten binnen de zorgsector. Deze nieuwe systematiek wordt ook toegepast op het ZORRO programma. [11] ZORRO staat voor "ZOrg Redteaming Resilience Oefeningen". In deze Red Teamtests worden mensen, processen en systemen van zorginstellingen getest met behulp van tools en technieken van actuele dreigingsactoren die binnen en buiten onze sector actief zijn geweest. Daarnaast levert Z-CERT ook (bestuurlijke) crisisoefeningen, zo zijn van 1 januari tot 1 juli 2024 zes van deze bestuurlijke crisisoefeningen uitgevoerd.

8 Het juiste niveau is gebaseerd op de bestaande normen van de Nederlandse Beroepsorganisatie van Accountants
9 Publieke consultatie NEN 7510 gestart. Consultatie loopt tot 22 september 2024.
10 Stand van zaken juli 2024: aantal Linkedin volgers (855, met groei van 27,8% sinds januari 2024), aantal inschrijvingen op nieuwsbrief (476). Het aantal deelnemers aan activiteiten van juni tot juli 2024 (352), met uitzondering van workshops en lezingen op externe events.
11 https://z-cert.nl/zorro

I.2.5: Digitale weerbaarheid sectoren infrastructuur en waterstaat

Binnen de sectoren infrastructuur en waterstaat zijn verschillende ontwikkelingen gaande. Er wordt gewerkt aan het versterken van de digitale weerbaarheid van sectoren waarvoor het ministerie van IenW een systeemverantwoordelijkheid heeft, zoals drinkwater, keren en beheren, luchtvaart, maritiem, chemie, nucleair, spoorwegen en plaats- en tijdbepaling. Binnen de sectoren drinkwater, luchtvaart, maritiem zijn al weerbaarheids-programma's actief. De weerbaarheidsprogrammmering binnen het ministerie van Infrastructuur en Waterstaat (IenW) is in 2023 uitgebreid met de mobiliteitssector (weg- en spoorvervoer).

De weerbaarheid van de sectoren wordt versterkt door samen te werken met de sector en o.a. kennisproducten op te leveren. Denk hierbij aan het opstellen van handreikingen, geven van trainingen en workshops. In 2024 heeft IenW een cyberweerbaarheids-conferentie georganiseerd waar kennis tussen de vitale aanbieders van IenW en overheid is uitgewisseld.

I.2.6: Digitale weerbaarheid Rijksoverheid

De digitale weerbaarheid van de Rijksoverheid is van essentieel belang omdat burgers en bedrijven erop moeten kunnen vertrouwen dat de Rijksoverheid betrouwbaar haar taken uitvoert en zorgvuldig omgaat met hun (persoons)gegevens. De versterking van de digitale weerbaarheid van de Rijksoverheid wordt uiteengezet in de I-strategie Rijk en de bijbehorende routekaart. Over de voortgang op de routekaart en de mijlpalen die zijn behaald is de Tweede Kamer regelmatig geïnformeerd via de verzamelbrief digitaliseringen en de jaarrapportage Bedrijfsvoering Rijk. [12] [13]

Versterken SOC Stelsel Rijk-programma

Om digitale dreigingen op de netwerken van de Rijksoverheids-organisaties te kunnen detecteren wordt er binnen de Rijksoverheid gebruik gemaakt van Security operations Centers (SOCs) die de computer- en netwerkactiviteiten in een Rijksoverheidsorganisatie monitoren. Het Versterken SOC Stelsel Rijk-programma (VSSR) richt zich daarom op het versterken van en ondersteunen bij het inrichten van SOC's bij rijksoverheids-organisaties door het ontwikkelen van generieke aanpakken en kennisproducten. Op 8 februari 2024 heeft het VSSR-programma haar productenportaal met de eerste drie producten gelanceerd. Het gaat hierbij om een uitwisseling van inhoudelijke informatie die gebruikt wordt in detectie en monitoring, een aanpak voor het meten van de volwassenheid van een SOC en een beschrijvend document voor een risico gebaseerde SOC-aanpak. Het VSSR-programma zal kennisproducten ontwikkelen op het gebied van monitoring en detectie, dreigingsinformatie, kwetsbaarheden-management en dashboarding, incidentenmanagement en het samenwerken en delen van informatie.

Red Teaming testen binnen de Rijksoverheid

Op de meest kritieke onderdelen binnen de Rijksoverheid implementeert de Rijksoverheid de TIBER-methodiek voor Red Teaming testen. TIBER staat voor Threat Intelligence Based Ethical Red-teaming. Bij deze methodiek worden Rijksoverheids-organisaties getest op hun weerbaarheid tegen geavanceerde cyberaanvallen. Dit gebeurt met testaanvallen, die zijn gebaseerd op realistische dreigingen. De eerste TIBER-testen binnen het Rijk zijn in 2023 gestart en in 2024 is het aantal testen verder uitgebreid. Binnen CIO Rijk is er een centraal team ingericht om het toenemend aantal TIBER-testen te kunnen begeleiden.

Quantumcomputing

Om de risico's van quantumcomputing in relatie tot cryptografie te beheersen moet de Rijksoverheid de komende jaren stappen zetten. Deze stappen zijn opgenomen in het programma Quantumveilige Cryptografie Rijk dat zich focust op het verhogen van het bewustzijn en het kennisniveau, het introduceren van nieuw beleid en nieuwe kaders, en het bieden van praktische ondersteuning. In 2024 wordt het rijksbrede beleidskader voor cryptografie vastgesteld en komt er een training voor IT specialisten beschikbaar zodat deze doelgroep over voldoende kennis en handelingsperspectief beschikt. Daarnaast breidt de doelgroep van het programma Quantumveilige Cryptografie Rijk zich in 2025 uit van Rijksoverheidsorganisaties naar mede-overheden en kritieke en vitale infrastructuren.

Ook heeft het kabinet in 2024 een BNC-fiche over een gecoördineerde routekaart voor de transitie naar Post Quantum cryptografie gepubliceerd naar aanleiding van de aanbeveling van de Europese Commissie. [14] Hierin stelt het kabinet dat Quantumveilige Cryptografie Rijk invulling zal geven aan de aanbeveling vanuit de Commissie.

Verplichte basisopleiding digitale weerbaarheid

Omdat het belangrijk is dat medewerkers van de Rijksoverheid over voldoende kennis en vaardigheden beschikken om goed en zorgvuldig om te gaan met informatie is er sinds 2024 beleid voor de verplichting om een basisopleiding digitale weerbaarheid te volgen. Voor organisaties die niet zelf een basisopleiding kunnen aanbieden komt er een centrale e-learning beschikbaar die eind 2024 wordt opgeleverd door het ministerie van Binnenlandse Zaken.

[12] Kamerstukken II, 2023–2024, 26 643, nr. 1197
[13] Kamerstukken II, 2023–2024, 31 490, nr. 338
[14] Kamerstukken II, 2023-2024, 22112 nr. 3945

I.2.7: Digitale weerbaarheid overheid en Bestuurlijk convenant

In 2024 is op verschillende manieren inhoudelijke voortgang geboekt op de drie systeemuitdagingen voor digitale veiligheid op lokaal niveau die onderdeel zijn van het bestuurlijk convenant digitale veiligheid gemeenten. Deze drie systeemuitdagingen gaan over (1) het digitale veiligheidsstelsel, (2) de informatiepositie van gemeenten en (3) structurele financiering voor uitvoering van de NLCS.

Om meer duidelijkheid te krijgen over het stelsel, de rollen en de verantwoordelijkheden zijn onder andere cyberoefendriehoeken georganiseerd en hebben verschillende gemeenten cybercrisisoefeningen gedaan. Voor de informatiepositie heeft de G4 afgelopen jaar, met behulp van de informatiemodellen uit het programma Cyclotron, een eerste verkenning gedaan naar de informatiebehoefte op digitale veiligheid van gemeente. Wat betreft financiering is door de Vereniging Nederlandse Gemeenten (VNG) en G4 een eerste interne inventarisatie gedaan van de benodigde middelen en de VNG en G4 gaan hierover in gesprek met BZK en JenV.

Voor de verdere uitwerking van het convenant zijn in 2024 twee projectleiders, een aan de gemeentezijde en een aan de Rijkszijde, gestart. Ook heeft er een eerste evaluatiemoment plaatsgevonden met als resultaat dat de onderlinge samenwerking tussen de convenantpartners BZK, JenV, de VNG en de gemeente Den Haag namens de G4 op de drie systeemuitdagingen de komende tijd verder wordt versterkt.

I.2.8: Digitale weerbaarheid sectoren met operationele technologie- en procesautomatiseringssystemen

De aanpak om de beveiliging van Industrial Automation and Control Systems (IACS) te verhogen wordt versterkt doormiddel van de IACS Coalitie. [15] Gezamenlijk wordt gewerkt aan het publiceren van IACS-security kennisproducten om de weerbaarheid van deze systemen te verhogen. Deze vijf themawerkgroepen zijn (1) Risicomanagement, (2) Awareness, Opleidingen en Trainingen, (3) Monitoring, Detectie en Respons, (4) Crisismanagement en (5) Onderzoek. Ook werkt de IACS Coalitie aan community building, o.a. door middel van het organiseren van kennisevenementen.

I.2.9: Zicht op digitale weerbaarheid van overheid en bedrijfsleven

De Nederlandse beroepsorganisatie van IT-auditors (NOREA) heeft een generiek format voor een IT-jaarverslag en een IT-auditverklaring ontwikkeld als onderdeel van het NOREA Reporting Initiative (NRI). Er worden pilots uitgevoerd binnen de overheid om te onderzoeken welke toegevoegde waarde het IT-verslag en IT-auditverklaring heeft voor de efficiënte en effectieve sturing op digitale weerbaarheid binnen de overheid. De eerste pilot is gestart en de verwachting is dat deze pilots zullen doorlopen in 2025.

De naleving van beveiligingsstandaarden wordt op basisbeveiliging.nl gemeten en gepubliceerd, waarbij continu nieuwe meetwaarden, zoals recent online tracking cookies, worden toegevoegd. De metingen zijn breed toepasbaar over alle branches heen, waarbij steeds meer organisaties worden gemonitord. Waaronder nu ook alle onderwijsinstellingen inclusief het basisonderwijs.

Doel 3: Organisaties reageren, herstellen en leren snel en adequaat op en van cyberincidenten en –crises.

I.3.1: Incident- en crisispreparatie en I.3.2: Oefenen

Evaluatie ISIDOOR IV

De evaluatie van ISIDOOR IV wordt interdepartementaal opgevolgd. Binnen de reikwijdte van de NLCS zullen meerdere acties worden ondernomen voor de opvolging van aanbevelingen. De NCTV en het NCSC zullen een visie ontwikkelen ten aanzien van een toekomstige ISIDOOR, waarin vraagstukken rondom deelnemersaantal, vorm, frequentie en omvang worden beantwoord. Vanwege de uitbreiding van de doelgroep die onder de implementatie van de Cbw zal volgen, zal er aandacht worden besteed aan de ondersteuning van deze (nieuwe) partijen gedurende (cyber)crisisvoorbereidingen en oefeningen. Daarnaast streeft de NCTV om in 2025 een nieuwe versie van het LCP Digitaal te publiceren, in lijn met de inwerkingtreding van de Cbw en de stelselwijzigingen die als gevolg hiervan plaatsvinden. De aanbevelingen uit de ISIDOOR evaluatie zullen worden meegenomen in de actualisatie. De evaluatie wordt tevens meegenomen in de uitwerking van het bouwplan het Cyberweerbaarheidsnetwerk, wat wordt vormgegeven door het NCSC. Onderdeel van de doorontwikkeling is dat heldere rol- en taakverdeling tussen CSIRTs, schakelorganisaties en ISACs worden vastgelegd, waaronder werkwijzen tijdens crises en incidenten,

[15] https://www.versterkencyberweerbaarheid.nl/onderwerpen/iacs-coalitie

inclusief oefeningen. Volgens het huidig ISIDOOR ritme wordt iedere ca. 2 jaar een oefening georganiseerd. Gezien de wetsimplementatie van de Cbw en de daaraan gekoppelde nodige herijking van de opzet van de ISIDOOR oefening, alsook de benodigde tijd voor om de lessen voortvloeiend uit de evaluatie te realiseren, zal de frequentie van 2 jaarlijkse ISIDOOR oefeningen naar verwachting niet gehaald worden. In aanvulling op ISIDOOR IV zal het ministerie van Volksgezondheid Welzijn en Sport in januari 2025 een departementale crisisoefening organiseren op gebied van digitale ontwrichting in de zorg.

Crisisplannen en oefenen

Naar aanleiding van de aankomende implementatie van de Cyberbeveiligingswet (Cbw) en de evaluatie van ISIDOOR IV zal het Landelijk Crisisplan Digitaal worden geactualiseerd. Het streven is om in 2025 een vernieuwd LCP Digitaal te publiceren.

Ook regionale crisisplannen sluiten steeds beter aan op het Landelijk Crisisplan Digitaal en worden doorlopend doorontwikkeld. Zo zetten de Veiligheidsregio's zich in om de expertise en werkwijzen voor cybercrises te versterken, o.a. door middel van themadagen en tabletop-oefeningen. Daarnaast wordt in samenwerking met het Nederlands Instituut Publieke Veiligheid (NIPV) een opleidingsmodule voor leiding en coördinatie bij cybercrises ontwikkeld, het streven is om dit ook in 2025 gereed te hebben.

Lokaal bestuur oefent per regio in de cyberoefendriehoeken op verschillende scenario's [16]. Tijdens de oefendag van de VNG, het OM en de politie doorlopen de burgemeesters, officieren van justitie, politiechefs en teamleiders van de verschillende veiligheidsregio's samen een aantal scenario's, van signalen van cybercrime, uitval van kritieke voorzieningen tot een ransomware-aanval op meerdere organisaties. Aanvullend biedt de VNG een cyberoefenpakket, toolboxen en interactieve cyberoefeningen en ondersteunt de IBD gemeenten bij tabletop ofeningen binnen de eigen organisaties[17].

Daarnaast oefenen overheden (Rijksoverheid, provincies, gemeenten en waterschappen) in de Overheidsbrede Cyberoefening jaarlijks aan de hand van een gesimuleerde hackaanval. Daarnaast zijn er gedurende het hele jaar online webinars en masterclasses georganiseerd met als doel het delen van kennis over allerlei ontwikkelingen rond cybersecurity.

Nederland heeft actief bijgedragen aan de doorontwikkeling van het Europese cyber crisis liaison netwerk (EU-CyCLONe) en deelgenomen aan verschillende oefeningen van de Europese Unie (EU) en de Noord-Atlantische Verdragsorganisatie (NAVO) waaronder edities van Cyber Europe, Cyber Storm, Locked-Shields, PACE, CMX en BlueOLEx, en streeft naar een intensievere jaarlijkse deelname.

Moderniseren (staats)noodrecht

Er is verbinding gelegd tussen de actie in de NLCS en de modernisering van het (staats)nood en crisisrecht. Er wordt gezamenlijk en interdepartementaal opgetrokken in de inventarisatie van (nood)bevoegdheden bij cybercrises en het identificeren van mogelijke lacunes. De basis van de verkenning vormt het in 2021 gemaakte en aan de Tweede Kamer verzonden overzicht van wet- en regelgeving cybersecurity [18]. Momenteel wordt na een initiële verkenning een inschatting gemaakt van de opgave en bijbehorende omvang en tijdslijn.

Cybersolidariteitsverordening

In de EU is in maart 2024 overeenstemming bereikt over de Cybersolidariteitsverordening, de publicatie wordt in het najaar van 2024 verwacht. De Cybersolidariteitsverordening is gericht op de detectie, paraatheid en respons op grootschalige cyberincidenten binnen de Europese Unie. Om dit te realiseren bestaat de Cybersolidariteitsverordening uit drie onderdelen. Ten eerste zal een Europees Cybersecurity Alerteringssysteem worden opgezet, bestaande uit een netwerk van nationale en grensoverschrijdende 'Cyber Hubs' welke bijdragen aan detectie, situationeel bewustzijn en kennisdeling. Het tweede onderdeel bestaat uit de realisatie van een Cybernoodmechanisme, waaronder kritieke entiteiten worden getest, en een Cybersecurity Reserve, welke incidentresponsdiensten levert wanneer een cyberaanval zich voordoet. Als derde zal een Evaluatiemechanisme voor cyberincidenten worden opgericht voor het herzien en beoordelen van significante cyberincidenten en de respons hierop.

[16] https://vng.nl/sites/default/files/2024-03/stappenplan_cyberoefendriehoek.pdf
[17] https://vng.nl/artikelen/interactieve-cyberoefening
[18] kst-26643-738, 2020/2021

Het einde van de OV-chipkaart is nabij. Binnenkort is inchecken met een betaalpas of smartphone mogelijk in het openbaar vervoer. Dit moet zorgen voor meer reis- en betalingsgemak. Een dergelijke verandering is een behoorlijke operatie. Ruime 60.000 poortjes en kaartlezers moeten worden omgebouwd.

Pijler II

Veilige en innovatie digitale producten en diensten

Doel 1: Digitale producten en diensten zijn veiliger

II.1.1: Europese wetgeving voor digitale producten en diensten

Nederland heeft zich met resultaat ingezet voor een wettelijk vastgelegde verantwoordelijkheid van fabrikanten, importeurs en distributeurs ten aanzien van de cybersecurity van digitale producten. Deze producten zullen moeten voldoen aan essentiële cybersecurity-eisen om in de EU op de markt gebracht te mogen worden. Op grond van een gedelegeerde handeling in het kader van de Radioapparatenrichtlijn (Radio Equipment Directive, RED) gelden vanaf 1 augustus 2025 cybersecurityeisen voor alle radioapparaten die verbonden kunnen worden met het internet, en in lokale netwerken ook radioapparaten gebruikt voor kinderzorg, als kinderspeelgoed of "wearables".

In de periode daarna zal deze regelgeving worden uitgebreid. Eind 2023 is in de EU overeenstemming bereikt over de Cyber Resilience Act (CRA), publicatie wordt in het najaar van 2024 verwacht. Deze verordening bevat onder meer een zorgplicht voor fabrikanten, importeurs en distributeurs voor de cybersecurity van alle producten met digitale elementen (alle hard- en software en componenten) die vanaf medio 2027 in de EU op de markt komen. Deze zorgplicht geldt voor de gehele verwachte gebruiksduur van het product.

In de CRA is aandacht besteed aan een goede aansluiting op bestaande en toekomstige sectorspecifieke cybersecurityregulering, door producten die onder deze sectorspecifieke cybersecuritywetgeving vallen, uit te sluiten van de CRA en door certificaten verleend op grond van de Cyber Security Act (CSA) waar passend te accepteren als middel om de conformiteit met cybersecurityeisen in de CRA aan te tonen.

De cybersecurityeisen in de RED en de CRA worden uitgewerkt in Europese geharmoniseerde normen. Aan NEN is een subsidie toegekend voor het voeren van het secretariaat voor de werkgroepen binnen Europese standaardisatieorganisatie CEN/CENELEC die deze normen opstellen. Daarnaast dragen het ministerie van EZ, de Rijksinspectie Digitale Infrastructuur (RDI) en private partijen door deelname van experts aan deze werkgroepen bij aan de totstandkoming van deze normen.

II.1.2: Toezicht en handhaving op digitale producten en diensten

De RDI zal toezien op de toepassing van de cybersecurityeisen op producten vallend onder de RED en de uitbreiding van de eisen onder de CRA.

In aanloop naar de inwerkingtreding van deze eisen voert de RDI een actieve voorbereiding. Zo heeft zij capaciteit en een testlab ingericht. Ook heeft RDI, vooruitlopend op het van toepassing worden van de RED-cybersecurityeisen, onderzoek gedaan naar de kwetsbaarheid van een aantal producten in verschillende categorieën, waaronder omvormers voor zon-PV-installaties, om

fabrikanten aan te sporen zich beter voor te bereiden. De RDI voert daarnaast een actieve bewustwordingsstrategie richting fabrikanten en andere relevante marktspelers. Deze lijnen worden de komende jaren doorgezet voor het voorbereiden op de uitvoering van de taken die uit de bredere reikwijdte van de CRA voortkomen. Het hiervoor genoemde normalisatieproces voor de RED duurt door de inhoudelijke complexiteit en de zeer grote diversiteit aan producten die eronder vallen langer dan voorzien. Dit heeft geleid tot uitstel van de inwerkingtreding van de cybersecurityeisen onder de RED (van augustus 2024 naar augustus 2025). Ook met dit uitstel zal de tijdige toepassing van de betreffende normen een uitdaging vormen voor de markt. RDI houdt hier rekening mee door ook aandacht te besteden aan de dienstverlening van de conformiteitsbeoordelingsinstanties die hier een rol in spelen.

De Autoriteit Consument en Markt houdt toezicht op de verkopers van producten die verplicht zijn om beveiligingsupdates te verstrekken aan consumenten, zolang zij dit redelijkerwijs mogen verwachten. Dit is een structurele taak en daarom doorlopend. Ook werken de RDI en de ACM intensiever samen om handhaving en toezicht op het gebied van veilige producten en diensten te verbeteren, zo hebben zij samen onderzoek gedaan naar de informatieverstrekking over updates en de werking en de veiligheid van slimme apparaten. Uw kamer is daar reeds over geïnformeerd op 3 mei 2024.[19]

II.1.3: Certificering en standaarden

In het kader van de Europese CSA worden door de Europese Commissie samen met het Europese cyberagentschap ENISA diverse Europese cybersecurity certificatie schema's ontwikkeld. Elk schema is vrijwillig en heeft een eigen toepassingsgebied met een eigen set certificeringseisen om een breed scala aan producten, diensten en processen te kunnen certificeren.

Op basis van het werkprogramma 'Union Rolling Work Programme' (URWP) dat is opgesteld door de Europese Commissie, zijn de prioriteiten voor de ontwikkeling van cybersecurity certificerings schema's vastgesteld. Het eerste uitgewerkte schema, het EU European Common Criteria-based cybersecurity certification scheme (EUCC), is begin 2024 gepubliceerd. Door deze certificering krijgen bedrijven, organisaties en consumenten meer zekerheid over de veiligheid van IT-producten (zoals chips in een bankpas of paspoort, routers, besturingssystemen, slimme meters, wachtwoordmanagers of chips in mobiele telefoons) omdat ze door een onafhankelijke conformiteitsbeoordelende instantie uitgebreid zijn getest op cybersecurityeisen. Het tweede schema, het EU cybersecurity certification scheme on cloud services (EUCS), bevindt zich in de laatste fase van ontwikkeling. Het doel daarvan is om zowel het beveiligingsniveau tegen cyberdreigingen te verhogen, als ervoor te zorgen dat fabrikanten en dienstverleners niet in elke lidstaat afzonderlijk een certificaat hoeven te behalen. Dit certificeringssysteem is een relevant instrument dat de cloudgebruikers kan helpen de veiligheid van de clouddiensten van hun leveranciers te beoordelen en aan te tonen. Het EUCS-schema wordt naar verwachting in de tweede helft 2024 gepubliceerd.

Daarnaast zijn twee schema's voor EU5G en eIDAS in ontwikkeling en wordt nader onderzocht wat voor schema voor beheerde beveiligingsdiensten dient te worden opgesteld.

Op 8 april 2024 heeft de toenmalige minister van Economische Zaken en Klimaat het rapport "Onderzoek contractuele afspraken cybersecurity" naar de Tweede Kamer gezonden. Het onderzoek werd begeleid met een brief van de minister waarin de bevindingen en de adviezen worden besproken die in dit rapport zijn gegeven om afnemers en leveranciers beter in staat te stellen heldere contractuele afspraken over cybersecurity te maken. Op basis van dit onderzoek en de door een klankbordgroep gegeven input werd er geen noodzaak tot het starten van nieuwe initiatieven gezien. Er is in de brief geconcludeerd dat bestaande initiatieven toereikend zijn om bedrijven te ondersteunen in het maken van contractuele afspraken over cybersecurity. Er valt nog winst te behalen in het verder onder de aandacht brengen van deze initiatieven bij bedrijven.

In het kader van de uitvoering van de motie Rajkowski[20] wordt een keurmerk ontwikkeld voor ICT-dienstverleners ten behoeve van het mkb. Het keurmerk geeft afnemers (midden- en kleinbedrijf) een bepaalde mate van zekerheid dat de gekozen ICT-dienstverlener betrouwbaar is, kwaliteit levert bij implementatie van basismaatregelen en gekwalificeerd is om bij te dragen aan de vormgeving van het cybersecurity-beleid. Het doel is het gemiddelde niveau van cybersecurity bij het mkb te verhogen.

Het project wordt uitgevoerd door het Centrum voor Criminaliteitspreventie en Veiligheid (CCV). Daarbij wordt samengewerkt met ICT-dienstverleners, afnemers, het DTC, de VNG, verzekeraars en certificatie-instellingen. De ontwikkeling van het keurmerk loopt conform planning en wordt naar verwachting eind 2025 afgerond.

II.1.4: Algemene beveiligingseisen rijksoverheid (ABRO) en overheidsinkoopbeleid

De oplevering van het ABRO-voorschrift neemt meer tijd in beslag dan voorzien. De deadline van eind 2023 is niet gehaald. Dit is

[19] Kamerstuk 35 734, nr. 16.
[20] Kamerstuk 36200 VII, nr. 60.

onder meer het gevolg van vertraging in de bemensing van het programma en de benodigde inhoudelijke afstemming tussen departementen en de politie om te komen tot een gedragen resultaat. Verwacht wordt dat de eerste overheidsorganisaties vanaf het tweede kwartaal van 2025 met ABRO gaan werken.

Aan de doorontwikkeling van de tool inkoopeisen cybersecurity overheid (ICO-tool) wordt continu gewerkt. Het afgelopen jaar is procesautomatisering in een nieuw thema uitgewerkt en opgenomen in de tool. Daarnaast is de tool op verschillende manieren verbreed. Zo zijn de thema-uitwerkingen of inkoopsegmenten 'applicatieontwikkeling', 'toegangsbeveiliging' en 'middleware' vernieuwd.

Doel 2: Nederland heeft een sterke cybersecuritykennis- en innovatieketen.

II.2.1: Veilige cryptografie

De Nationale Cryptostrategie (NCS) is een strategie voor het versneld ontwikkelen van eersteklas informatiebeveiligings-producten voor hoog-gerubriceerde ('bijzondere') informatie en het stimuleren van kennisontwikkeling. In navolging daarop is in 2024 verder gewerkt aan het opstellen van een lange termijn cryptobehoefte van de Rijksoverheid. Hierdoor is het Rijk in staat om eensgezind het opdrachtgeverschap bij de cryptografische industrie in te vullen.

In de tweede helft van 2024 zullen gesprekken plaatsvinden met de crypto-industrie om te komen tot een samenwerkingsmodel dat voor de langere termijn de stabiliteit en continuïteit moet waarborgen van de cryptografische industrie voor High Assurance producten.

Er wordt in Nederland door universiteiten, kennisinstituten en bedrijven onderzoek gedaan dat op korte en langere termijn een bijdrage levert aan het tot stand komen van hoogwaardige beveiligingsproducten. In 2024 is als onderdeel van de NCS een start gemaakt met het opstellen van een lange termijn onderzoeksstrategie. Deze onderzoeksstrategie heeft tot doel om het onderzoek meer gestructureerd en efficiënter te laten plaatsvinden en beter te laten aansluiten op de daadwerkelijke behoefte aan deze producten. De onderzoeksstrategie komt tot stand door het raadplegen van specialisten uit de wetenschap en de cryptografische industrie en is naar verwachting in 2025 gereed.

Vanuit de Nationale Technologie Strategie Cybersecuritytechnologieën zijn ambities bepaald voor innovatie en onderzoek om veilige cryptografie óók in de toekomst te waarborgen. De komst van de quantumcomputer vormt een bedreiging voor de veiligheid van klassieke encryptiemethodes. Samen met kennisinstellingen en bedrijven, en in nauwe afstemming met het programma QVC Rijk en de Nationale Crypto Strategie worden onderzoeks- en innovatietrajecten ontwikkeld voor fundamenteel en toegepast onderzoek ter bevordering van kennis en innovatie rondom quantumveilige cryptografie.

II.2.2: Nationale samenwerking kennis- en innovatie-onderzoeks-samenwerking

Gerichte en structurele investeringen in cybersecurity kennis- en innovatieontwikkelingen zijn noodzakelijk. Deze helpen Nederlandse bedrijven om hoogwaardige en toekomstbestendige producten en diensten te leveren, het verdienvermogen te versterken en de cyberweerbaarheid van Nederland te verhogen. Om deze reden zet EZ een meerjarig investeringsplan op en doet structurele investeringen in de vorm van subsidiemogelijkheden middels instrumenten voor cybersecurity kennis- en innovatieontwikkeling. Middels deze bijdrage worden er in samenwerking met subsidiepartners, in de komende jaren meerdere instrumenten opengesteld om onderzoek en innovatie op het gebied van cybersecurity te stimuleren (voor zowel wetenschap als bedrijfsleven), gericht op verschillende fases in de innovatieketen. Dit meerjarige investeringsplan zal naar verwachting vanaf 2025 geoperationaliseerd worden.

In 2024 heeft EZ twee Small Business Innovation Research (SBIR) trajecten geopend waarmee in totaal € 3 miljoen beschikbaar is gesteld voor cybersecurity innovatie aan mkb'ers in Nederland. Het gaat hierbij om de onderwerpen 'autonome IT/OT beveiliging' en 'Autonoom delen van dreigingsinformatie'. In totaal hebben elf bedrijven subsidie ontvangen om een verkennend eerstefaseproject uit te voeren. In 2025 worden projecten geselecteerd om een tweedefaseproject uit te voeren waarin technologie demonstrators worden ontwikkeld.

In het Cybersecurity Innovatieprogramma CS4NL werken Topsectoren, NWO, universiteiten en hogescholen, en bedrijfsleven samen om de innovatiekracht van Nederlandse topsectoren op het gebied van cybersecurity te versterken. CS4NL wordt uitgevoerd door het cybersecurity samenwerkingsplatform dcypher. Het programma pakt cyberveiligheidsvraagstukken op die voortkomen uit grote maatschappelijke transities en organiseert publiek-private samenwerking, bijvoorbeeld via onderzoeksfinanciering. Zo is begin 2024 het onderzoekstraject Kennis- en Innovatieconvenant (KIC) van de Nederlandse Wetenschapsorganisatie (NWO) uitgezet voor 'Cybersecurity voor digitale weerbaarheid'. Ook staat een onderzoekscall open tot 25 oktober 2024 over 'Cyber resilience for critical chains and systems' van Topconsortium voor Kennis & Innovatie (TKI) voor in totaal € 2,5 miljoen.

De in 2024 geformaliseerde Cyber Innovation Hub (CIH) van Defensie werkt nauw samen met marktpartijen om innovaties te testen en, mede via militaire oefeningen, te valideren voor militair gebruik (*fast follower*). De activiteiten worden daarbij meer en meer uitgebreid naar het gezamenlijk innoveren met marktpartijen. Defensie houdt daarbij voeling met andere nationale initiatieven.

II.2.3: Europese onderzoeks-samenwerking en fondsen

In 2023 is een start gemaakt met de opzet van het Nationaal Coördinatiecentrum (NCC-NEXIS) bij de Rijksdienst voor Ondernemend Nederland (RVO). Het NCC moet de Nederlandse input richting het Europese Cybersecurity Competence Centrum (ECCC) vormgeven en nationale partijen helpen gebruik te maken van de beschikbare Europese subsidies op het gebied van cybersecurity. Inmiddels bestaat het NCC-NEXIS een jaar en is het volledig operationeel.

Organisaties uit de Nederlandse cybersecuritysector (waaronder het dcypher-netwerk) en onderzoekspartijen worden ondersteund via het Nationaal Coördinatie Centrum (NCC-NEXIS) in de voorbereiding en uitvoering van projecten uit Europese initiatieven en fondsen zoals Digital Europe en Horizon Europe. NCC-NL | NEXIS ondersteunt Nederlandse partijen bij het schrijven van hun voorstellen, door onder meer te reviewen en te helpen partners te vinden voor consortia.

NCC-NEXIS zorgt voor coördinatie van de Nederlandse onderzoeksbehoefte vanuit overheid en marktpartijen en borgt dat de nationale behoeften worden meegenomen naar het ECCC om de Nederlandse prioritaire innovatiethema's zo goed mogelijk te vertegenwoordigen bij de totstandkoming van de cybersecurity werkprogramma's van Digital Europe en Horizon Europe. Dit heeft geresulteerd in een hogere deelname van Nederlandse partijen aan EU subsidiemogelijkheden over verschillende cybersecurity thema's zoals inzet AI in cybersecurityoplossingen, in post quantum cryptografie (PQC), in het vraagstuk van cybersecurity arbeidsmarktkrapte en, hieraan gerelateerd, in het bevorderen van cybersecurity skills en talentontwikkeling.

Luchthavens proberen zich niet meer enkel te onderscheiden met service en aanbod. Ook digitalisering en data zijn terreinen waarop ze zich snel ontwikkelen. Zowel voor passagiers- als goederenverkeer betekent dit ook dat de afhankelijkheid en mogelijke kwetsbaarheid groeit.

Pijler III

Tegengaan van digitale dreigingen van staten en criminelen

Doel 1: Nederland heeft zicht op digitale dreigingen van staten en criminelen.

III.1.1: Zicht op statelijke actoren

De AIVD en de MIVD hebben de afgelopen tijd sterk geïnvesteerd in de inlichtingenonderzoeken. Dat heeft ertoe geleid dat er steeds meer zicht ontstaat op de huidige en voorstelbare digitale dreiging. De Inlichtingen- en Veiligheidsdiensten delen daarnaast structureel producten zoals inlichtingenberichten, cyberadviezen en risicoanalyses met de verschillende afnemers. Deze worden door de dienstafnemers vervolgens vertaald naar specifieke handelingsperspectieven.

De Inlichtingen-gebaseerde incidentencoördinatie vanuit de AIVD en de MIVD is daarnaast in 2024 verder uitgebouwd, onder andere via de samenwerking in de Cyber Intel/Info Cel (CIIC) en het cyberincident team van de AIVD en de MIVD dat de zogenaamde Intelligence Based Incident Coordination (IBIC) uitvoert. De Nederlandse overheid was in 2023 regelmatig doelwit van statelijke cyberactoren. IBIC-team heeft in 2023 verschillende organisaties, bedrijven en individuen in Nederland genotificeerd over geavanceerde en persistente digitale aanvallen van deze cyberactoren en advies gegeven over het mitigeren van deze concrete dreigingen. Bij het coördineren van cyberincidenten heeft het IBIC-team daar waar nodig samengewerkt met de CIIC, het NCSC en andere partners.

In de Defensiebegroting staat dat Defensie haar cybercapaciteit met onder meer 400 fte's gaat versterken om het delen van informatie sneller en veiliger te laten plaatsvinden en de reactiesnelheid bij kwetsbaarheden en incidenten te verhogen. Het is de bedoeling dat dit in vier jaar wordt gerealiseerd, waarbij een bestaand IT-programma van Defensie zorgt voor de benodigde technische hulpmiddelen. In de periode 2023-2024 is dit volgens plan verlopen.

In het actieplan NLCS is aangegeven dat er in 2022 zal worden gekeken naar de mogelijkheden om de effectieve inzet van de bijzondere bevoegdheden voor onderzoeken naar landen met een offensief cyberprogramma te vergroten. In 2022 is daaropvolgend een voorstel voor de Tijdelijke Wet onderzoeken AIVD en MIVD ingediend bij de Tweede Kamer. Deze wet is op 1 juli 2024 in werking getreden. De Commissie van Toezicht of de Inlichtingen- en Veiligheidsdiensten (CTIVD) heeft echter gemeld niet in staat te zijn om per 1 juli toezicht te houden op de Tijdelijke wet. Dit omdat er randvoorwaarden hiervoor ontbreken. Het betreft, volgens de Commissie, de bezetting van de Commissie en de staf, de huisvesting en de IT-omgeving. De AIVD en MIVD zijn in nauw overleg met de CTIVD om te kijken hoe het toezicht kan plaatsvinden.

De herziening van de Wet op de Inlichtingen- en Veiligheidsdiensten 2017 is dit jaar opgestart. De herziening is een traject van meerdere jaren, waarbij de effectieve inzet van de bevoegdheden en het verbeteren van de slagkracht van de diensten belangrijke uitgangspunten zijn en blijven. Hierover is op

26 juni 2024 een Kamerbrief gestuurd met daarin opgenomen wat dit voor de inwerkingtreding betekent.[21]

III.1.2: Onderzoeks- en opsporings-capaciteit cybercriminelen

De bestrijding van cybercriminaliteit middels onderzoeks- en opsporingscapaciteiten is een doorlopende actie voor de politie en het Openbaar Ministerie (hierna OM), tevens gewaarborgd in de Veiligheidsagenda. De Kamer is hierover op 28 juni 2024 geïnformeerd middels Kamerbrief over de voortgang van de integrale aanpak cybercrime en de bevoegdheden voor de opsporing in het digitale domein.[22] Hieronder een opsomming van enkele concrete interventies rondom deze (doorlopende) actie:

- Inzet van Google Ads. Bij deze preventieve maatregel krijgen mensen die in Google zoeken op termen die aan cybercrime zijn gerelateerd, een waarschuwing in beeld te zien om hen te waarschuwen voor de strafbaarheid van cybercrime.
- Met succes zijn op initiatief van het OM en de politie voor het eerst cybercriminelen op de Europese sanctielijst geplaatst. De inzet van sancties wordt gezien als nieuw aanvullend verstoringsmiddel in de aanpak van cybercriminaliteit.
- Het samenwerkingsverband Melissa, waar de politie en het OM aan deelnemen, heeft ook dit jaar weer zijn succes en meerwaarde bewezen in de aanpak van ransomware, wat zich onder meer heeft getoond in de gezamenlijke aanpak van Qakbot, Lockbit en recentelijk nog Cactus. Steeds meer partijen tonen interesse om deel te nemen aan het samenwerkingsverband.
- Met de Autoriteit Consument en Markt (ACM) wordt actief de samenwerking gezocht ten behoeve van een bestuursrechtelijke aanpak van aanbieders van tussenhandelsdiensten die zich niet houden aan de zorgvuldigheidsbeginselen die volgen uit de Digital Services Act.
- Door het OM is in afstemming met de politie en de rechtspraak een oefenrechtbank georganiseerd voor verschillende Kamerleden, waarbij onder andere complexe vraagstukken die spelen in cyberzaken onder de aandacht zijn gebracht.
- Het ministerie van Justitie en Veiligheid is primair deelnemer aan het CRI (Counter Ransomware Initiative). Daarnaast wordt ook door de politie, het OM en het ministerie van Buitenlandse Zaken actief bijgedragen aan het Counter Ransomware Initiatief.
- Er is een Cybercrime Beeld Nederland door de politie en het OM gepubliceerd in het tweede kwartaal 2024.
- Er is vanuit het Programma Cybercrime en Gedigitaliseerde Criminaliteit een opleidingsplan binnen het OM ontwikkeld. Op dit moment wordt er gewerkt aan de realisatie van het opleidingsplan. Hierbij wordt gefocust op het versterken van de basiskennis op het gebied van cybercrime en gedigitaliseerde criminaliteit binnen de gehele organisatie.

III.1.3: Versterken diplomatiek netwerk

De cyberdiplomaten zijn ten opzichte van de vorige voortgangsrapportage beter ingebed binnen ambassades en permanente vertegenwoordigingen, waardoor de cybercomponent sterker naar voren komt in het diplomatieke werk. Dit heeft geleid tot uitbreiding van het netwerk, het beter in kaart brengen van het 'cyberlandschap' in derde landen, en daaropvolgend een versterkt engagement richting deze landen. Ook vindt jaarlijks een aantal overheidsbrede cyberconsultaties plaats, met bijvoorbeeld India, Zuid-Korea, het Verenigd Koninkrijk, en de Verenigde Staten.

Het NCSC is gestart met de uitvoering van het cybercapaciteitsopbouwprogramma. Het cybercapaciteitsopbouwprogramma ondersteunt het opbouwen van cyberweerbaarheid in partnerlanden, stimuleert een wereldwijd digitaal ecosysteem en bevordert strategische allianties gericht op een stabiele en veilige cyberspace. Het NCSC biedt een leidende expertrol, o.a. bewerkstelligd door de opstelling van een trainersnetwerk van NCSC medewerkers.

Het ministerie van Defensie neemt daarnaast actief deel aan cyberinitiatieven op het gebied van cyber, onder meer binnen het Europees Defensiefonds en via PESCO-projecten en het innemen van een conceptueel leidende rol binnen de EU en de NAVO. Zo heeft het ministerie van Defensie meegedaan aan twee trajecten in het kader van het Europees Defensiefonds (ACTING en AINCEPTION), en is betrokken bij de oprichting van het Cyber and Information Domain Coordination Center (CIDCC). Defensie heeft in 2023 ook deelgenomen aan meerdere internationale (cyber)oefeningen.

Doel 2: Nederland heeft grip op digitale dreigingen van staten en criminelen

III.1.4: Attributie en respons

Voor het vergroten van onze cyberweerbaarheid zijn er plannen gemaakt voor de verdere ontwikkeling van attributie- en responsmogelijkheden. Deze plannen zijn uitgewerkt in de internationale cyberstrategie. Dit najaar wordt de Kamer apart geïnformeerd op de voortgang op deze strategie. Betrokken ministeries en diensten werken samen aan een meer 'proactieve omgang met cyberdreigingen'. Essentie van die inzet is dat

[21] Kamerstukken II, 2023-2024, 36263, nr.43, p. 2
[22] Kamerstukken II, 2023-2024, *5397428*

Nederland niet enkel reageert op cyberincidenten op het moment dat ze plaatsvinden, maar dat kwaadwillende activiteiten ook effectief worden ontmoedigd of gemitigeerd. Dat heeft bijvoorbeeld geleid tot een publicatie over de COATHANGER-malware en de zichtbare trend rondom het misbruiken van kwetsbaarheden in publiek benaderbare *edge devices.*[23]

Het kabinet werkt daarnaast in verschillende coalities aan strategieën om statelijke cyberdreigingen tegen te gaan. Nederland heeft het afgelopen jaar, samen met Polen, aan de basis gestaan van aanscherping van de zgn. *EU Cyber Diplomacy Toolbox* (het geheel aan maatregelen dat de EU tot zijn beschikking heeft om te kunnen reageren op cyberdreigingen). Dat heeft onder andere geleid tot nieuwe sancties onder het cybersanctieregime. Op Nederlandse voordracht zijn twee prominente Russische cybercriminelen gesanctioneerd[24]. Dit resultaat kwam tot stand door intensieve samenwerking tussen het ministerie van Buitenlandse Zaken, politie, OM en het ministerie van Justitie en Veiligheid. Daarnaast werden – eveneens naar Nederlands voorstel - verschillende bedrijven gesanctioneerd die als ICT-toeleverancier opereren voor de Russische inlichtingendiensten en zo kwaadwillende cyberoperaties mede mogelijk maken.[25]

De ontwikkeling van een gezamenlijke weerbaarheid tegen cyberdreigingen binnen de NAVO blijft daarnaast een uitdaging vanwege de vaak beperkte bereidheid informatie uit te wisselen en de soms uiteenlopende belangen van bondgenoten. Er wordt weliswaar veel gesproken over modaliteiten om informatie-uitwisseling te versterken maar daadwerkelijke implementatie blijft beperkt. Wel heeft Nederland een belangrijke bijdrage kunnen leveren aan de discussie over de cyberweerbaarheid van de NAVO en zijn bondgenoten door de organisatie van de Cyber Defence Pledge Conference in Den Haag in mei 2024. Op Nederlands initiatief is daarnaast ingezet op de herziening van de maatregelen die de NAVO tot zijn beschikking heeft om te kunnen reageren op cyberdreigingen. Deze werden tijdens de top in Washington formeel aangenomen.

Concluderend kan er worden gesteld dat Nederland zowel binnen de NAVO als binnen de EU een voortrekkersrol inneemt als het gaat om cyberbeleidsvorming en -ontwikkeling. Er wordt vanwege de capaciteit en expertise op het gebied van cyber binnen Nederland, veelvuldig naar Nederland gekeken.

III.1.5: Defensieve en offensieve cybercapaciteiten

Net als de fysieke wereld is ook de digitale wereld inmiddels het speelveld van strategische competitie, waarin conflicterende belangen en waarden in toenemende mate tot confrontaties leiden. Om deze reden heeft het ministerie van Defensie sterk geïnvesteerd in cybercapaciteiten, onder meer via het structureel borgen en vergroten van Cyber Rapid Respons Teams (CRRT's) en Multidisciplinaire Cyber Teams (MDCT) en het vergroten van de personele gereedheid via opleiding, training en oefening. Defensie is nu al in staat om de genoemde teams in te zetten, maar werkt nog aan een verbetering en versterking van de personele capaciteit en de hulpmiddelen.

Doel 3: Staten houden zich aan het normatief kader voor verantwoordelijk statelijk gedrag in de digitale ruimte

III.1.6: Normatief kader

Nederland heeft het afgelopen jaar een belangrijke rol gespeeld bij de opvolging van de met grote steun aangenomen VN-resolutie voor een Programme of Action (PoA)[26]. Het PoA moet de opvolger zijn van de huidige Open Ended Working Group (OEWG) en zal zich gaan richten op het bijstaan van VN-leden bij de implementatie van het bestaande normatief kader (o.a. bestaande uit 11 vrijwillige normen) voor verantwoord statelijk gedrag. Nederland heeft een prominente rol gespeeld in deze discussie, en heeft onder andere ideeën gepresenteerd over hoe capaciteitsopbouw tussen VN-lidstaten binnen het PoA zou moeten worden georganiseerd. Ondanks de grote geopolitieke tegenstellingen binnen de VN kon het jaarlijkse voortgangsrapport van de OEWG (Annual Progress Report 2024) ook afgelopen zomer weer worden aangenomen[27]. Daarnaast heeft Nederland met gelijkgezinde landen gepoogd om de discussie over toepassing van het internationaal recht in het cyberdomein verder te brengen. Dat is belangrijk omdat kwaadwillende landen daarmee uiteindelijk beter verantwoordelijk kunnen worden gehouden voor hun gedrag. De ruimte voor voortgang is vanwege de opstelling van met name Rusland en China echter zeer beperkt.

[23] Nieuwe malware benadrukt aanhoudende interesse in edge devices | Nieuwsbericht | Nationaal Cyber Security Centrum (ncsc.nl)
[24] EU sanctioneert voor het eerst cybercriminele kopstukken | Nieuwsbericht | Rijksoverheid.nl
[25] Europese Unie (EU) neemt twaalfde sanctiepakket aan tegen Rusland | Nieuwsbericht | Rijksoverheid.nl
[26] A/RES/78/16
[27] Third Annual Progress Report of the Open-ended working group on security of and in the use of information and communications technologies 2021-2025 (A/AC.292/2024/CRP.1)

III.1.7: Internet governance

De toegenomen geopolitieke spanningen manifesteren zich ook in een grotere strijd over het beheer van het internet. Landen als Rusland en China proberen hun controle op het beheer van het internet te vergroten in multilaterale organisaties, ten koste van de invloed van niet-statelijke actoren in deze discussie. De inzet van EZ en BZ op internet governance – gericht op behoud van een wereldwijd open, vrij en veilig internet – richt zich primair op de noodzaak voor het behoud van het multistakeholder-model waarbij alle belanghebbenden (statelijk en niet statelijk) op gelijke voet kunnen meekijken, praten en beslissen over ontwikkelingen van en wijzigingen in de publieke kern van het internet. Met dit doel hebben we onze inzet in internetorganisaties zoals ICANN en in de multilaterale VN-organisatie International Telecommunications Union (ITU) en de Freedom Online Coalition geïntensiveerd. Ook blijven we in gesprek met de stakeholders in de Nederlandse internet gemeenschap om hetzelfde te doen. Dit heeft o.a. geleid tot een aantal Nederlandse voorstellen voor workshops, die tijdens het VN Internet Governance Forum (IGF) in december 2024 zullen plaatsvinden.

Het proces om binnen VN verband een akkoord te bereiken op een “Global Digital Compact”, welke tijdens de VN Summit of the Future zal worden aangenomen, bevindt zich in de afrondende fase. De Nederlandse inzet, samen met de EU en lidstaten van de Freedom Online Coalition, heeft zich o.a. gericht op het borgen van het multistakeholder model voor internet governance. Binnenkort zullen ook de onderhandelingen starten over de 20 jaar review van de World Summit for the Information Society (WSIS+20). Deze summit vormt het fundament onder het multistakeholder model en wij zullen ons, samen met de Nederlandse internet gemeenschap, sterk maken om het succes van het multistakeholder model om de publieke kern van het internet te beheren, te benadrukken. Ook zetten we in op continuering en versterking van het Internet Governance Forum na 2025.

Toenemende digitalisering biedt het onderwijs veel kansen, bijvoorbeeld door het aanbieden van online colleges en voor het ontsluiten van kennis. Tegelijkertijd brengt deze grote afhankelijkheid van technologie risico's met zich mee. Verschillende universiteiten zijn de laatste jaren doelwit van ransomware geweest.

Pijler IV

Cybersecurity arbeidsmarkt, onderwijs en digitale weerbaarheid van burgers

Doel 1: Burgers zijn goed beschermd tegen digitale risico's

IV.1.1: Voorlichtingscampagnes

De ministeries van Binnenlandse Zaken en Koninkrijksrelaties (BZK), Economische Zaken (EZ) en Justitie en Veiligheid (JenV) werken nauw samen aan publiekscampagnes op het gebied van cybercriminaliteit en cybersecurity, om de bewustwording rondom digitale risico's onder burgers te vergroten. Er lopen inmiddels drie publiekscampagnes: '*Laat je niet interneppen*'; '*Dubbel beveiligd is dubbel zo veilig*'; en '*Doe je updates*'.

Er is naast deze publiekscampagnes ook aandacht besteed aan het aanbieden van handelingsperspectieven om slachtofferschap te voorkomen. Van alle campagnes zijn toolkits beschikbaar die vrij kunnen worden gebruikt door andere partijen om de campagnes te ondersteunen, waaronder gemeenten.

In het kader van de City Deal Lokale Weerbaarheid Cybercrime zijn er innovatieve projecten ontwikkeld voor de jeugd, het midden- en kleinbedrijf, senioren en laaggeletterden. De City Deal loopt eind 2025 af. Er wordt om deze reden gekeken naar de waarborging van deze projecten vanaf 2026.

IV.1.2: Beveiligingsadvies burgers

Om burgers beter te voorzien van informatie en beveiligingsadviezen is in mei 2024 de Tool Cyberweerbaarheid opgeleverd. De Tool Cyberweerbaarheid biedt bibliotheken en andere instellingen informatie waarmee burgers adequaat geholpen kunnen worden met vragen en problemen op het gebied van cyberveiligheid.[28] De publiek toegankelijke tool zal de komende tijd worden verbeterd op basis van feedback uit het werkveld. Daarnaast werkt het CCV aan een doorontwikkeling van de Tool Cyberweerbaarheid, zodat deze ook gebruikt kan worden als een zelfhulptool voor burgers.

Er zijn daarnaast ook stappen gezet omtrent de ontwikkeling van het cyberweerbericht. Het cyberweerbericht zal uiteindelijk worden gebruikt om burgers te waarschuwen over digitale dreigingen. Naar verwachting is het eerste concept in 2025 gereed.

IV.1.3: Betrouwbaarheid digitale overheidsvoorzieningen

Ter verbetering van de herkenbaarheid van de overheid op het internet heeft de staatssecretaris van BZK de Tweede Kamer geïnformeerd over het voornemen om de impact van invoering van een uniforme domeinnaamextensie inzichtelijk te maken.

[28] https://hetccv.nl/tool-cyberweerbaarheid

Eind januari 2024 is gestart met de uitwerking van een plan van aanpak om dit verder te onderzoeken.

Daarnaast is het Register Internetdomeinen Overheid (onderdeel van het Register van Overheidsorganisaties) eind 2023 live gegaan. Zo kunnen burgers op een toegankelijke wijze checken of internetdomeinen wel of niet van de overheid zijn. Op dit moment bevat het register de publieke domeinregistraties van de Rijksoverheid. In de tweede helft 2024 wordt gestart met het aansluiten van de medeoverheden.

Doel 2: Burgers reageren snel en adequaat op cyberincidenten

IV.2.1: Melding of aangifte doen van cybercrime fenomenen

De online aangiftemogelijkheid voor ransomware voor burgers ontwikkeld door de politie is sinds begin 2024 live. Er wordt momenteel gewerkt aan een vernieuwing van het aangiftesysteem, waardoor op termijn ook bedrijven en organisaties de mogelijkheid krijgen om online een aangifte te doen van ransomware.

Doel 3: Leerlingen krijgen onderwijs in digitale vaardigheden gericht op veiligheid

IV.3.1: Curriculum

Onder regie van Stichting Leerplan Ontwikkeling (SLO) worden de kerndoelen voor het funderend onderwijs geactualiseerd. Deze concept kerndoelen zijn overhandigd aan voormalig Minister van OCW, en de verwachting is dat deze 2027 geïmplementeerd zijn. Daarnaast is er in het najaar van 2023 een Expertisepunt Digitale Geletterdheid gelanceerd, als onderdeel van de landelijke ondersteuningsstructuur voor scholen.

Doel 4: De Nederlandse arbeidsmarkt kan voldoen aan de toenemende vraag naar cybersecurity-experts

IV.4.1: Cybersecurity arbeidsmarkt

Het ministerie van EZ heeft op 19 juni 2023 Platform Talent voor Technologie (PTvT) en Dialogic de opdracht gegeven een onderzoek uit te voeren naar de kwalitatieve en kwantitatieve tekorten op de cybersecurityarbeidsmarkt en gevraagd te komen met aanbevelingen hoe deze tekorten aangepakt kunnen worden. Dit heeft geleid tot de Onderzoeksrapportage Onderwijs en Arbeidsmarkt Cybersecurity.[29] Ook is in de Kamerbrief een aantal initiële vervolgacties uiteengezet. Hiermee is deze actie afgerond.

Op basis van de onderzoeksresultaten en aanbevelingen zullen de volgende initiële vervolgstappen worden gezet:

- *Opzetten eigenstandige Cybersecurity Pijler binnen de Human Capital Agenda ICT:* om uitvoering te geven aan de twaalf aanbevelingen uit het onderzoek wordt binnen de Human Capital Agenda ICT HCA ICT een meerjarige eigenstandige cybersecurity programmalijn opgezet.
- *Het vergroten van inzicht in en overzicht van de cybersecurity arbeidsmarkt:* voor het onderzoek hebben Platform Talent voor Technologie (PTvT) en Dialogic veel relevante informatie en data verzameld over de huidige stand van het cybersecurityonderwijs en de arbeidsmarkt. Deze informatie zal online worden ontsloten en worden bijgehouden in de vorm van netwerkkaarten en dashboards, waarbij er zo veel mogelijk zal worden geïntegreerd met bestaande netwerkkaarten en dashboards van HCA ICT.
- *Het versterken van de NWO-call samenwerking kennisinstellingen en bedrijfsleven:* In afstemming met het veld zal via NWO (Regieorgaan Stichting Innovatie Alliantie) een subsidiecall worden opgezet om met praktijkgericht onderzoek de samenwerking te stimuleren tussen kennisinstellingen (mbo, hbo, wo), het bedrijfsleven en overheidsorganisaties. Dit moet leiden tot verbeterde aansluiting tussen de vraag van de arbeidsmarkt en het aanbod van het onderwijs, het opleiden van studenten via onderwijsinstellingen en via het bedrijfsleven en het betrekken van de arbeidsmarkt bij onderwijsvorming. Dit instrument wordt nader vormgegeven in nauwe samenwerking met het cybersecurityveld.

Het ministerie van OCW investeert structureel in hbo-opleidingen in de bètatechniek, waar cybersecurityopleidingen ook onderdeel van zijn. OCW treft in het najaar van 2024 de voorbereidingen voor de eerste tussenevaluatie. De resultaten van deze evaluatie worden eind 2025 verwacht.

Het ministerie van BZK subsidieerde daarnaast een arbeidsmarktinterventie van VNG om landelijk stagebemiddeling voor digitale veiligheid tussen gemeenten en hogescholen in te richten en te ondersteunen.

[29] Onderzoeksrapportage Onderwijs en Arbeidsmarkt Cybersecurity (2024D19328)

Uitgave
Nationaal Coördinator
Terrorismebestrijding
en Veiligheid (NCTV)
Postbus 20301, 2500 EH Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5050

Meer informatie
www.nctv.nl
info@nctv.minjenv.nl
@nctv_nl

Oktober 2024