Voortgangsrapportage 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 Nederlandse Cybersecuritystrategie

Inhoudsopgave

Pijler I

Digitale weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties 7

Herziening van het stelsel 7
Versterken van het Landelijk Dekkend Stelsel (LDS) 7
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) 8
Programma cyclotron 8
Nationaal Detectie Netwerk (NDN) 8
Doelwit- en slachtoffernotificatie (DSN) 8
Digitale weerbaarheid vitale infrastructuur 8
Digitale weerbaarheid MKB en bedrijfsleven 9
Digitale weerbaarheid sectoren (onderwijs, zorginstellingen, infrastructuur en waterstaat, (rijks)overheid) 10
Onderwijs 10
Zorginstellingen 10
Infrastructuur en Waterstaat (IenW) 10
(Rijks)overheid 10
Digitale weerbaarheid sectoren met operationele technologie- en procesautomatiseringssystemen 11
Zicht op digitale weerbaarheid overheid en bedrijfsleven 11
Corporate governance code 11
Verzekeraars 11
Incident- en crisispreparatie en oefenen 12

Pijler II

Veilige en innovatie digitale producten en diensten 15

Europese wetgeving voor digitale producten en diensten en toezicht en handhaving hierop 15
Certificering en standaarden 16
Algemene beveiligingseisen rijksoverheid (ABRO) en overheidsinkoopbeleid 16
Veilige cryptografie en nationale en Europese kennis- en innovatie-onderzoekssamenwerking 16

Pijler III

Tegengaan van digitale dreigingen van staten en criminelen 19

Zicht op statelijke actoren 19
Onderzoeks- en opsporingscapaciteit cybercriminelen 19
Versterken diplomatiek netwerk 20
Attributie en respons 20
Defensieve en offensieve cybercapaciteiten 20
Normatief kader en internet governance 21

Pijler IV

Cybersecurity arbeidsmarkt, onderwijs en digitale weerbaarheid van burgers 23

Voorlichtingscampagnes burgers 23
Beveiligingsadvies burgers 23
Betrouwbaarheid digitale overheidsvoorzieningen 24
Burgers reageren snel en adequaat op cyberincidenten 24
Onderwijs: Curriculum 24
Cybersecurity arbeidsmarkt 24

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 maat-schappelijke organisaties

Herziening van het stelsel

Verschillende trajecten binnen pijler 1 dragen bij aan de herziening van het cybersecuritystelsel. Voorbeelden zijn (i) de integratie van het Nationaal Cyber Security Centrum (NCSC), het Digital Trust Center (DTC) en Cyber Security Incident Response Team for Digital Service Providers (CSIRT-DSP); (ii) uitwerking van het cyclotron rapport; (iii) de implementatie van de EU richtlijn Netwerk- en Informatiebeveiliging (NIS2); (iv) het inrichten van doelwit en slachtoffernotificatie; en (v) de doorontwikkeling van het Landelijk Dekkend Stelsel (LDS). Na afronding van deze trajecten moet er een stelsel staan dat de dreigingen de komende jaren het hoofd kan bieden met één centrale cyber organisatie en, daar waar dit een toevoeging is, enkele sectorale cyber organisaties. De centrale cyber organisatie verspreidt dreigingsinformatie en handelings-perspectief, gebaseerd op input van verschillende private en publieke organisaties verzameld via het platform gecreëerd via project Cyclotron. Alle organisaties in Nederland ontvangen deze informatie via het doorontwikkelde LDS passend bij hun niveau variërend van NIS2 doelgroep organisaties tot het mkb. Tenslotte worden zij ook gewaarschuwd wanneer zij potentieel doelwit of slachtoffer zijn van een cybersecurity aanval.

De herziening van het stelsel is nodig om de doelstellingen binnen pijler 1 te realiseren maar vraagt qua beschikbare capaciteit en middelen veel van de betrokken organisaties, zoals het NCSC, DTC of beleidsafdelingen. Daarnaast zitten er weder-zijdse afhankelijkheden tussen de verschillende trajecten waardoor een vertraging binnen een traject ook voor knelpunten binnen een ander traject kan zorgen. Dit zien we ook terug in de realisatie, er zijn vooralsnog geen substantiële vertragingen ten aanzien van de in de NLCS geschetste tijdlijnen maar sommige trajecten zoals het LDS of de uitwerking van het cyclotronrapport blijven langer in de planfase hangen dan in eerste instantie ingeschat. Het kabinet probeert daarom het aantal nieuwe opdrachten richting de uitvoering tot een minimum te beperken en poogt door middel van coördinatie op de samenhang de verschillende trajecten beter behapbaar te maken voor de betrokken organisaties.

Versterken van het Landelijk Dekkend Stelsel (LDS)

De toekomstige vorm van het Landelijk Dekkend Stelsel is afhankelijk van verschillende acties binnen pijler 1 van het actieplan. Zo zal de implementatie van de NIS2-richtlijn en de komst van de nationale cybersecurity autoriteit het cybersecuri-tystelsel als geheel veranderen. Het is van belang om bij de versterking van het Landelijk Dekkend Stelsel in te spelen op deze complexe realiteit. Daarom werken we samen met schakelorgani-saties aan een toekomstbeeld voor het LDS. Dit toekomstbeeld wordt begin 2024 met uw Kamer gedeeld en zal als kader dienen voor de verdere versterking van het LDS. Deze versterking zal, na publicatie van het toekomstbeeld, omschreven worden in een bouwplan waarin de concrete eisen voor en ondersteuning van stelselpartners zal worden opgenomen.

Dit betekent dat de oplevering van het toekomstbeeld en het bouwplan het startsein vormen voor de uitvoering van andere LDS-acties binnen pijler 1, zoals het ondersteunen van schakelor-ganisaties met financieringsmodellen en een communicatieplan aan de hand waarvan organisaties wegwijs kunnen worden binnen het stelsel.

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)

Voor de zomer is de Tweede Kamer geïnformeerd over de voortgang van de integratie.[1] De eerste belangrijke stappen in de integratie zijn afgelopen jaar gezet. Er is een transitiemanager aangesteld en de organisaties werken al zoveel mogelijk samen. Onder andere door het gezamenlijk organiseren van het waarschuwen van slachtoffers en doelwitten van een cyberaanval en te komen tot één set van meest effectieve maatregelen voor alle organisaties in Nederland waardoor zij zich beter kunnen weren tegen aanvallers. De eerstvolgende mijlpaal van de integratie is het afronden van de eerste fase op 1 oktober 2024. Op die datum dient de vernieuwde organisatie de verschillende taken in samenhang en in voldoende mate uit te voeren. Het NCSC, DTC en CSIRT-DSP voeren na de eerste fase geen eigenstandige koers meer en bestaan alleen nog in formele zin in hun huidige vorm. In de periode tot 1 januari 2026 worden de taken en processen vervolgens volledig geïntegreerd en geoptimaliseerd. Dit draagt bij aan de doelstelling uit de NLCS om te komen tot heldere aanspreekpunten en meer efficiëntie in het cybersecuritystelsel.

Programma cyclotron

Er is een programmamanager aangesteld die de routekaart zal opstellen voor de realisatie van het platform voor wederkerige cybersecurity informatie- en kennisdeling. Parallel aan het opstellen van de routekaart is er alvast gestart met verschillende pilots in klein publiek-privaat verband om informatie en kennis uit te wisselen langs de lijnen van het cyclotronrapport. Op deze manier worden de mogelijkheden en knelpunten inzichtelijk. Het opstellen en daadwerkelijke implementeren van een sluitend programmaplan en publiek-private routekaart is een uitdagend proces gezien de juridische complexiteit rond informatiedelen, de benodigde samenwerking tussen de betrokken organisaties en onzekerheid over de benodigde middelen.

Nationaal Detectie Netwerk (NDN)

Met het Nationaal Detectie Netwerk (NDN) worden meer geavanceerde risico's en aanvallen gedetecteerd. Bijna alle Rijksorganisaties zijn inmiddels aangesloten op het NDN. Het Nationaal Cyber Security Centrum (NCSC) werkt samen met het ministerie van BZK om de laatste relevante Rijksorganisaties aan te sluiten op het NDN per uiterlijk eind 2023. Hierover is uw Kamer ook geïnformeerd via de Kamerbrief over de actualisatie van de routekaarten van de I-strategie op 13 juli jl.[2]

Doelwit- en slachtoffernotificatie (DSN)

De NLCS stelt zich tot doel dat iedereen in Nederland gewaarschuwd moet kunnen worden die (mogelijk) slachtoffer of doelwit is van een cyberaanval. Om dit te realiseren is de afgelopen periode onderzocht hoe doelwit- en slachtoffernotificatie (DSN) uit niet-strafrechtelijke bron verder vormgegeven kan worden. Hiertoe hebben er sinds eind 2022 meerdere gesprekken tussen publieke en verschillende private partijen plaatsgevonden. Naar aanleiding van deze gesprekken is er een projectteam opgericht bestaande uit het NCSC, DTC en het CSIRT-DSP om de actie uit het NLCS Actieplan op te pakken. De afgelopen periode is er door de Rijksoverheid een visie ten aanzien van DSN geformuleerd, waarin de Rijksoverheid een actieve rol neemt ten aanzien van (de uitvoering van) DSN, waarbij nauw wordt samengewerkt met andere (private) partijen. Naar verwachting zal er eind 2023 een dienst worden opgeleverd die het, met bestaande systemen, technisch mogelijk maakt om dreigingsinformatie te delen met organisaties die doelwit of slachtoffer zijn van een cyberdreiging. Parallel wordt er gewerkt aan de verdere realisatie van een voorziening voor de langere termijn, gebruikmakend van één technische oplossing, waarmee organisaties, publiek en privaat, vitaal en niet-vitaal en groot en klein, en mogelijk ook burgers, geïnformeerd kunnen worden, waarmee iedereen in Nederland beter in staat wordt gesteld de digitale weerbaarheid te vergroten. De streefdatum voor de volledige realisatie van de voorziening is voorzien voor het eerste kwartaal van 2025.

Digitale weerbaarheid vitale infrastructuur

Het kabinet werkt, onder coördinatie van het ministerie van JenV, aan een wetsvoorstel ter implementatie van de NIS2-richtlijn. De implementatie van deze Europese richtlijn is een belangrijk instrument om ervoor te zorgen dat organisaties goed zijn beschermd tegen digitale risico's, en raakt daarmee aan veel van de acties onder pijler I van de NLCS.

Als gevolg van de NIS2-richtlijn krijgen veel meer organisaties in Nederland te maken met wettelijke verplichtingen, toezicht en ondersteuning voor hun digitale weerbaarheid. Dit geldt zowel voor overheden, vitale organisaties en andere organisaties die actief zijn in sectoren van maatschappelijk belang.[3] Hiermee zorgen we ervoor dat cybersecurity niet langer vrijblijvend is. Vanwege de samenhang met andere nieuwe wetgeving (zoals de CER-richtlijn voor fysieke beveiliging) en beleid heeft het kabinet de implementatie van de NIS2-richtlijn betrokken bij de versterkte aanpak ter bescherming van de vitale infrastructuur, waar ik u in mei van dit jaar over geïnformeerd heb.

Daarnaast heeft de NIS2-richtlijn ook gevolgen voor de manier waarop de overheid zich georganiseerd heeft. Om ervoor te zorgen dat organisaties die onder de NIS2-richtlijn komen te vallen van de juiste ondersteuning gebruik kunnen maken, heb ik een onafhankelijke verkenning laten uitvoeren naar de (her)inrichting van het CSIRT-stelsel in Nederland. De resultaten van deze verkenning zullen worden betrokken bij de verdere uitwerking van het wetsvoorstel ter implementatie van de NIS2-richtlijn. Naast het uitvoeren van de CSIRT taak krijgt de overheid ook te maken met duizenden nieuwe organisaties die onder toezicht komen te staan van één van de verschillende sectorale toezichthouders. Voor meer dan tien sectoren uit de NIS2-richtlijn moet het toezicht voor het eerst worden ingericht. Dit vraagt veel van de betrokken organisaties.

De complexiteit van het voorstel en de grote gevolgen voor organisaties vragen om een zorgvuldige voorbereiding van het wetsvoorstel. Het kabinet werkt hard aan de doorvertaling van deze richtlijn en verwacht dat dit wetsvoorstel eind dit jaar in consultatie kan worden gebracht. Het kabinet streeft ernaar dat de wet eind 2024 van kracht wordt. Organisaties die zich willen voorbereiden op de komst van NIS2 kunnen voor de actuele stand van zaken van de uitwerking van de richtlijn onder andere terecht op de website van de NCTV en het NCSC.

Digitale weerbaarheid MKB en bedrijfsleven

Het Digital Trust Center (DTC) heeft sinds vijf jaar de verantwoordelijkheid om alle ondernemingen die niet tot het Rijk of de vitale infrastructuur behoren te helpen met het verbeteren van hun digitale weerbaarheid. Een belangrijk gedeelte van deze doelgroep is het midden- en kleinbedrijf (mkb). Om ook hen te ondersteunen geeft het DTC adviezen en tools op hun website waarmee ondernemers zelf aan de slag kunnen om dit te realiseren. De DTC website wordt nog meer uitgebreid met nieuwe content en additionele tools. U bent 23 februari jl. geïnformeerd over de voortgang van het DTC.[4]

Daarnaast wordt ook de DTC community steeds meer de plek voor ondernemers die elkaar willen helpen op het gebied van cybersecurity. Dit is de plek waar tips en tricks kunnen worden uitgewisseld tussen ondernemers onderling maar er zijn ook community leden vanuit de wetenschappelijke instituten en ook werkzaam bij ICT-dienstverleners. De meest recente tool is de CyberVeilig Check gericht op het mkb en zzp'ers.[5]

Tevens worden sinds twee jaar ook alle bedrijven actief genotificeerd door het DTC als er informatie bekend is bij de overheid dat bij hen een kwetsbaarheid aanwezig is. Er wordt dan direct contact gelegd met dat bedrijf door de DTC informatiedienst om ze daarvan op de hoogte te brengen. Tussen juni 2021 en juli 2023 heeft het DTC 35.000 notificaties gestuurd aan bedrijven.

Ook wordt dit jaar wederom een subsidie gegeven voor samenwerkingen van bedrijven die zich inzetten voor het ontwikkelen van tools of activiteiten om ondernemend Nederland digitaal weerbaarder te maken. Deze regeling zal in september bekend worden gemaakt en zal mede gericht zijn op het Nederlandse mkb. Er is voor deze ronde van de subsidieregeling cyberweerbaarheid €800.000 beschikbaar.

De komende jaren wordt het DTC evenals het NCSC en CSIRT-DSP opgenomen in de vernieuwde organisatie. De bovenstaande inzet blijft hierbij geborgd en de verwachting is dat door het bundelen van de verschillende expertises deze inzet alleen maar effectiever zal worden.

Een van de acties die bijdragen aan de weerbaarheid van het bedrijfsleven zijn centrale registers voor cybersecurity gerelateerde informatie. Het NCSC is gestart met de realisatie van een portaal waar organisaties hun organisatie- en netwerkgegevens kunnen bijwerken en waar organisaties informatie over kwetsbaarheden kunnen opzoeken (database van kwetsbaarheden). Het portaal is in eerste instantie alleen toegankelijk voor NIS2 aanbieders.[6]

1 Kamerstukken II / 2022/23 26643 nr. 927

2 Kamerstukken II, 2022-23, 26643, nr. 10161

3 Alle midden en grote bedrijven in de aangewezen sectoren. De aangewezen essentiële sectoren zijn: afvalwater, overheidsdiensten, ruimtevaart, energie, vervoer, bankwezen, infrastructuur voor de financiële markt, zorg, drinkwater en digitale infrastructuur. De aangewezen belangrijke sectoren zijn: sectoren post- en koeriersdiensten; afvalbeheer; fabricage, productie en distributie van chemicaliën; voedselproductie; verwerking en distributie; maakindustrie; en digitale aanbieders

4 Kamerstuk 26 643, nr.980.

5 CyberVeilig Check voor ZZP en MKB https://tools.digitaltrustcenter.nl/cyberveilig-check/

6 NIS2 aanbieders: Alle midden en grote bedrijven in de aangewezen sectoren. De aangewezen essentiële sectoren zijn: afvalwater, overheidsdiensten, ruimtevaart, energie, vervoer, bankwezen, infrastructuur voor de financiële markt, zorg, drinkwater en digitale infrastructuur. De aangewezen belangrijke sectoren zijn: sectoren post- en koeriersdiensten; afvalbeheer; fabricage, productie en distributie van chemicaliën; voedselproductie; verwerking en distributie; maakindustrie; en digitale aanbieders

Naar verwachting is dit portaal in Q1 van 2024 gereed. Na publicatie van het portaal worden de functionaliteiten verder uitgebreid.

Digitale weerbaarheid sectoren (onderwijs, zorginstellingen, infrastructuur en waterstaat, (rijks) overheid)

Onderwijs

De eerste versie van het normenkader informatiebeveiliging en privacy voor organisaties en instellingen het basis- en voortgezet onderwijs is op 19 april 2023 gepubliceerd, waarmee de actie uit het actieplan is afgerond. Periodieke monitors en benchmarks zullen volgen om te toetsen of schoolbesturen voldoen aan de norm. Dit alles is onderdeel van het Programma Digitaal Veilig Onderwijs dat in 2022 is gelanceerd en scholen op weg helpt om de digitale weerbaarheid te verhogen. De inzet op veiligheid en weerbaarheid maakt onderdeel uit van het OCW-beleid over digitalisering in het primair- en voortgezet onderwijs, en is opgenomen in een kamerbrief van 6 juli.[7] Ook in het middelbaar beroepsonderwijs en het hoger onderwijs zijn verdere stappen gezet om de digitale weerbaarheid te vergroten: Er is een toetsingskader gebaseerd op het volwassenheidsmodel Informatiebeveiliging, van de Koninklijke Nederlandse Beroepsorganisatie van Accountants (NBA), dat sinds eind 2022 door alle instellingen in het mbo en sinds 2019 door alle instellingen in het Hoger Onderwijs wordt gebruikt.

Zorginstellingen

Binnen de zorgsector zijn er verschillende ontwikkelingen en zijn meerdere acties uit het actieplan NLCS afgerond. Zo is het programma 'Informatieveilig gedrag in de zorg' is voor 2022-2023 afgerond. Er wordt voor in ieder geval 2024 weer subsidie verstrekt voor het uitvoeren van dit programma. Daarnaast is OpenKAT per 1 juli 2022 beschikbaar gesteld als open-source tool. OpenKAT is de Kwetsbaarheden Analyse Tool, die informatiesystemen kan scannen en analyseren. OpenKAT wordt als open source project samen met de OpenKAT-community gebouwd door het Ministerie van Volksgezondheid, Welzijn en Sport (VWS). Hiermee is de betreffende actie uit het actieplan afgerond. Voor 2023 is het plan om OpenKAT verder door te ontwikkelen en de tool breed onder de aandacht te brengen binnen het zorgveld. Ook is in november 2022 de herziening van de norm voor informatiebeveiliging in de zorg (NEN7510) gestart. Deze norm schrijft onder andere voor dat zorgaanbieders de risico's voor informatiebeveiliging in kaart brengen en hiervoor passende maatregelen nemen. Het beoogde resultaat van de herziening is een geactualiseerde editie van de NEN7510. De eerste werkversie van de herziene norm wordt eind 2023 verwacht en zal na afronding vrij beschikbaar zijn op de webpagina van de NEN. Daarnaast worden meer zorgsectoren stapsgewijs aangesloten bij Z-CERT, het Cyber Emergency Response Team voor de zorg. Zo zullen onder andere organisaties in de eerstelijnssector, revalidatiezorg, en instellingen uit de verpleging-, verzorging-, en thuiszorgsector worden aangesloten. Wanneer zorginstellingen aangesloten zijn, worden ze door Z-CERT voorzien van advies en dreigingsinformatie. In het geval van een incident kan Z-CERT een zorginstelling ondersteunen bij het mitigeren van de gevolgen van een cyberaanval.

Infrastructuur en Waterstaat (IenW)

Binnen de sectoren infrastructuur en waterstaat zijn verschillende ontwikkelingen. 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, nucleair, spoorwegen en plaats- en tijdbepaling. Voorbeelden hiervan zijn de gemaakte nieuwe bestuurlijke afspraken in het *Bestuurlijk Overleg Water* om samen te werken om de cyberweerbaarheid te versterken inclusief een gezamenlijke visie en ambitie. In oktober wordt in een bestuurlijke cybertafel met bestuurders uit de watersector een cyberoefening uitgevoerd. Daarnaast worden er voor verschillende sectoren trainingen, oefeningen en kennisproducten gemaakt en gehouden. Voor de sectoren luchtvaart en maritiem is in 2023 een *cyberweerbaarheidprogramma* van start gegaan waarbinnen onder andere aandacht is voor de ontwikkeling van kennisproducten rondom thema's als operationele technologie en AI in relatie tot cybersecurity. Het ministerie rapporteert over de inzet in de verschillende sectoren via een speciale website.[8]

(Rijks)overheid

Het doel van de Nederlandse Cybersecuritystrategie is het digitaal veiliger maken van Nederland. De digitale weerbaarheid van de Rijksoverheid is daarvoor van belang. De ambitie op de digitale weerbaarheid van de Rijksoverheid wordt uiteengezet in de I-strategie Rijk en de bijbehorende routekaarten. Over de actualisatie van de routekaarten is op 13 juli 2023 een brief verzonden naar de Tweede Kamer.[9] Daarnaast speelt het lokale bestuur een belangrijke rol. De Informatiebeveiligingsdienst (IBD) is de sectorale CERT/CSIRT voor alle Nederlandse gemeenten en onderdeel van de Vereniging Nederlandse Gemeenten (VNG). De IBD is voor gemeenten het schakelpunt met het NCSC en ondersteunt gemeenten op het gebied van informatiebeveiliging en privacybescherming.

Digitale veiligheid op lokaal niveau heeft zowel betrekking op de interne organisatie ('eigen huis op orde') van de gemeente als ook op de digitale openbare orde en veiligheid in de gemeente ten behoeve van inwoners, bedrijven, maatschappelijke organisaties, infrastructuur en vitale processen. Daarom is in december 2022 het Bestuurlijk Convenant Digitale Veiligheid Gemeenten ondertekend door de staatssecretaris Binnenlandse Zaken en Koninkrijkrelaties, de minister van Justitie en Veiligheid en de burgemeester van Den Haag, tevens voorzitter van de Vereniging Nederlandse Gemeenten (VNG).[10] Dit convenant schetst de uitgangspunten om de komende jaren gezamenlijk intensief te werken aan het verbeteren van digitale veiligheid op lokaal niveau. Een ambtelijke kerngroep bestaande uit vertegenwoordigers van BZK, J&V, VNG en G4 werkt nu aan de drie systeemuitdagingen (focuspunten in het convenant). De drie focuspunten zijn de vertaling van het fysieke veiligheidsstelsel naar het digitale veiligheidsstelsel en de vraag hoe de bevoegdheden zich in beide domeinen tot elkaar verhouden, de informatiepositie op digitale veiligheid binnen de eigen gemeente en structurele financiering om de digitale veiligheid van gemeenten te vergroten. Ook werkt de VNG aan een set onderzoeken om de uitdagingen waar gemeenten voor staan, scherp te krijgen. Deze onderzoeken dragen bij aan het beeld van de cyberweerbaarheid waar de Tweede Kamer om heeft gevraagd.[11]

Digitale weerbaarheid sectoren met operationele technologie- en procesautomatiseringssystemen

Het CSBN2023 en de Cyber Security Raad (CSR) vragen terecht aandacht voor de risico's van slechte beveiliging van operationele technologie (OT) systemen. De minister van Infrastructuur en Waterstaat (IenW) zet zich langs de actielijnen uit de NLCS in om deze beveiliging te verbeteren. De Industrial Automation and Control Systems-coalitie (IACS-coalitie) is van start gegaan. Er zijn zes overheidspartijen die de kerngroep vormen: het ministerie van Infrastructuur en Waterstaat (IenW), Rijkswaterstaat (RWS), het Nationaal Cyber Security Center (NCSC) en Digital Trust Center (DTC), de Rijksinspectie Digitale Infrastructuur (RDI) en de Informatiebeveiligingsdienst (IBD). De stakeholders zijn in kaart gebracht en de governance is vastgelegd. Er is een concept actieplan opgesteld waarin deliverables zijn gedefinieerd. Dit actieplan is opgebouwd rond 4 gedefinieerde thema's die als prioriteit worden gezien voor de cybersecurity van IACS, namelijk: (i) Risicomanagement; (ii) Onderzoek, Trainen en Oefenen; (iii) Monitoring, Detectie en Respons en (iv) Crisismanagement. Er wordt op basis van deze thema's bijvoorbeeld gewerkt aan het ontwikkelen van gemeenschappelijke beveiligingsstandaarden en -protocollen en het opzetten van gemeenschappelijke trainingsprogramma's. Er wordt op deze thema's daarnaast actief gezocht naar een publiek-private samenwerking. Tijdens de *One Conference* in oktober 2023 wordt de missie van de IACS-coalitie gepresenteerd.

Zicht op digitale weerbaarheid overheid en bedrijfsleven

Corporate governance code

Eind 2022 is de nieuwe geactualiseerde corporate governance code gelanceerd, waarin cybersecurity als een van de elementen is vermeld waardoor er bij beursgenoteerde bedrijven meer aandacht is voor beheersen van cybersecurityrisico's.[12] Deze actie is afgerond.

Verzekeraars

Het CSBN 2023 constateert dat de verzekerbaarheid van digitale risico's in toenemende mate onder druk komt te staan. Dit komt onder andere door het toenemende aantal cyberaanvallen, waarmee ook de schade toeneemt. Hierdoor stijgen de premies en moeten klanten voldoen aan hogere beveiligingseisen om in aanmerking te komen voor een verzekering. Verzekeringen staan ook onder druk doordat cyberincidenten kunnen uitgroeien tot een systemische crisis en daardoor onverzekerbaar zijn. Daarnaast bestaat er vaak onduidelijkheid over de dekking van risico's binnen bestaande (traditionele) verzekeringen. Dit wordt 'silent cyber' genoemd. Dit kan leiden tot onduidelijkheid over de dekkingsgraad van polissen en de noodzaak van eventuele aanvullende cyberverzekeringen.

7 Kamerstukken II, 2022-23, 36200, nr. 251
8 https://www.versterkencyberweerbaarheid.nl/
9 Kamerstukken II, 2022-23, 26643, nr. 10161
10 Staatscourant 2022, 35231
11 Kamerstukken II, 2022 – 23, 36 200 VII, nr.68
12 Kamerstukken II, 2022-2023, 31 083, nr. 65

In de Nederlandse Cybersecuritystrategie is opgenomen dat samen met verzekeraars wordt verkend welke rol verzekeringen kunnen spelen in de verzekerbaarheid van gevolgschade naar aanleiding van cyberincidenten. De verkenning wordt daarom aangevuld met de conclusies uit het CSBN2023. Deze actie wordt in 2024 opgepakt.

Incident- en crisispreparatie en oefenen

Op 23 december 2022 is het Landelijk Crisisplan Digitaal (LCP-Digitaal) aangeboden aan de Tweede Kamer.[13] Hiermee is deze actie uit het actieplan afgerond. In het LCP-Digitaal is onder andere aandacht voor de complexiteit van cyberincidenten. Het CSBN2023 vraagt hier ook aandacht voor. Departementen en de veiligheidsregio's worden momenteel middels een leerprogramma meegenomen in de inhoud van het plan, in aanloop naar de landelijke cybercrisisoefening ISIDOOR IV. De oefening *ISIDOOR IV* vindt in het najaar van 2023 plaats en zal de onderlinge aansluiting, samenwerking en informatie-uitwisseling beschreven in het LCP-Digitaal beoefenen. De evaluaties die worden opgesteld naar aanleiding van (nationale) oefeningen en crises worden gebruikt als input voor volgende actualiseringen van het LCP-Digitaal.

De Rijksoverheid heeft daarnaast deelgenomen aan de NAVO-oefening CMX 2023 en de EU-oefening PACE 2022, waarin ook cybercrisisaspecten zijn beoefend. Daarmee is deze actie uit het actieplan voltooid. De inzet in het cybergedeelte van de oefeningen richtte zich met name op de verbindingen tussen de nationale crisisstructuur en de crisisstructuren in NAVO/EU verband. In interdepartementaal verband worden voorbereiding getroffen voor een uitgebreidere deelname en inzet in toekomstige edities.

13 Kamerstukken II, 2022-2023, 26 643, nr. 955.

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 betalings-gemak. Een dergelijke verandering is een behoorlijke operatie. Ruim 60.000 poortjes en kaartlezers moeten worden omgebouwd.

Pijler II

Veilige en innovatie digitale producten en diensten

Europese wetgeving voor digitale producten en diensten en toezicht en handhaving hierop

Onder Pijler II zijn verschillende acties ondernomen onder de doelstelling *Digitale producten en diensten zijn veiliger*. Bij de onderhandelingen voor de Europese Cyber Resilience Act (CRA) heeft Nederland zich, met resultaat, actief ingezet voor de opname van een zorgplicht van fabrikanten en leveranciers voor de cybersecurity van hun digitale producten (zowel hard- en software en componenten). Deze producten moeten voldoen aan essentiële cybersecurity-eisen om in de EU op de markt gebracht te mogen worden. Daarnaast blijven fabrikanten conform de Nederlandse inzet gedurende de gehele verwachte productlevensduur verantwoordelijk voor de cybersecurity onder meer door gratis veiligheidsupdates te verstrekken. De nationale markttoezichthouders (in Nederland de Rijksinspectie Digitale Infrastructuur (RDI)) zullen toezicht houden op de naleving. Ook is aandacht besteed aan een goede aansluiting van de CRA op andere Europese regelgeving: zo worden producten die onder gelijke of strengere Europese sectorspecifieke cybersecurityregels vallen uitgezonderd en zullen de cybersecurity-eisen in de Richtlijn Radioapparatuur (RED) voor draadloos verbonden apparaten met de komst van de CRA hierin opgaan. Op 19 juli 2023 is de Raad van de EU een compromistekst overeengekomen, waarmee het Spaans voorzitterschap mandaat heeft om de triloog met het Europees Parlement te beginnen. Het Europees Parlement stemt in september over haar positie.

Zowel de CRA als de al eerder van kracht gaande gedelegeerde handeling onder de RED, zullen essentiële cybersecurity-eisen stellen die worden omgezet in technische normen (geharmoniseerde standaarden). Aan de ontwikkeling van technische normen onder de RED wordt hard gewerkt door experts vanuit private partijen en de overheid via de Europese standaardisatieorganisatie CEN/CENELEC. Het Nederlandse normalisatie-instituut (NEN) voert het secretariaat. Doordat het benodigde standaardisatieproces langer duurt dan voorzien, heeft de Europese Commissie besloten de datum waarop de eisen onder de Radioapparatenrichtlijn van kracht worden te verschuiven van 1 augustus 2024 naar 1 augustus 2025. Hiertoe bestond draagvlak onder EU-lidstaten. Hiermee zal ook het toezicht door RDI hierop later aanvangen. RDI doet in aanloop naar de inwerkingtreding van de cybersecurityeisen onder de RED wel al onderzoek, bijvoorbeeld naar de cybersecurity van omvormers voor zonnepaneelinstallaties, om fabrikanten aan te sporen zich beter voor te bereiden. Het kabinet heeft daarnaast bij de Europese Commissie aangedrongen op een snelle ontwikkeling van technische normen onder de CRA. Hiertoe heeft de Commissie inmiddels een concept-standaardiseringsverzoek doen uitgaan naar de lidstaten en CEN/CENELEC voor feedback.

Consumenten en ondernemers zijn door EZK in samenwerking met brancheorganisaties voorgelicht over de richtlijnen *verkoop goederen en levering digitale inhoud*, op grond waarvan consumenten recht hebben op (veiligheids)updates zolang zij die redelijkerwijs mogen verwachten. Deze informatie is doorlopend te vinden via de website van de KVK.[14] Deze actie is daarmee afgerond.

14 www.ondernemersplein.kvk.nl

Certificering en standaarden

Over de certificeringsschema's op grond van de Cyber Security Act wordt nog intensief in Europa onderhandeld, er zijn momenteel nog geen schema's vastgesteld. De uitvoeringshandeling voor het Common Criteria Schema wordt momenteel afgestemd. Met betrekking tot het EU Cybersecurity Cloud Scheme (EUCS) hebben ENISA en de Europese Commissie in mei 2023 een ontwerp met de lidstaten gedeeld, waar nog over onderhandeld zal worden. Het doel is om eind 2023 een compromistekst over het EUCS te bereiken.

De uitkomsten van het onderzoek van het ministerie van Economische Zaken en Klimaat naar afspraken die bedrijven en organisaties maken over cybersecurity in de contractrechtpraktijk en best practices in business-to-business relaties tussen aanbieders van ICT-producten en -diensten en afnemers worden eind 2023 verwacht.

Algemene beveiligingseisen rijksoverheid (ABRO) en overheidsinkoopbeleid

Op donderdag 6 juli 2023 is een motie van Rajkowski/Bisschop ten aanzien van het programma ABRO aangenomen. In de motie wordt het kabinet verzocht een voortgangsrapportage op te stellen met daarin een bijbehorend tijdspad en versnellingsmogelijkheden. Het voornemen is om de voortgangsrapportage uiterlijk voor de begrotingsbehandeling van digitale zaken op 27 november 2023 met de Tweede Kamer gedeeld.

De doorontwikkeling van de tool voor de Inkoopeisen Cybersecurity Overheid (ICO-tool) loopt volgens planning en zal dit jaar worden afgerond. Met het Centrum voor Informatiebeveiliging en Privacy (CIP, beheerder van de tooling) zijn meerdere activiteiten hierover afgesproken. De belangrijkste activiteit ligt nu op het verbreden van het gebruik van het tool. Op dit moment loopt er een verkenning vanuit het ministerie van Binnenlandse Zaken en Koninkrijksrelaties om te bepalen wat nodig is om de normensets voor veilig (ICT) inkopen te verplichten voor alle overheidsorganisaties (Rijk en medeoverheden).

Veilige cryptografie en nationale en Europese kennis- en innovatie-onderzoekssamenwerking

Er is voortgang geboekt op acties onder de doelstelling Nederland heeft een sterke cybersecuritykennis en -innovatieketen. Dcypher, het samenwerkingsplatform voor cybersecurity innovatie, heeft activiteiten ontplooid om de innovatiesamenwerking in Nederland te versterken. De routekaarten 'cryptocommunicatie' en 'geautomatiseerd kwetsbaarhedenonderzoek (AVR)' zijn verder ontwikkeld. Er wordt samengewerkt met universiteiten door middel van een aantal gefinancierde PhD's en een studenten-challenge om technologie te ontwikkelen. Er worden met het bedrijfsleven use-cases opgezet om technologie in de praktijk toe te gaan passen.

Naast doorlopende onderzoeksprojecten wordt onder deze routekaarten een Small Business Innovation Research (SBIR) traject uitgevoerd, ter grootte van € 1.8 mln., eind 2023 afgerond. In dit traject hebben cybersecurityondernemers innovatieve technische prototypen ontwikkeld die inspelen op de doelstellingen van de routekaarten. Er wordt op dit moment door EZK en dcypher een nieuwe serie SBIR calls, met een totale grote van € 3 mln., voorbereid. Deze nieuwe SBIRs zullen gericht worden op cybersecurity vraagstukken die voor verschillende departementen en topsectoren relevant zijn. Deze calls worden naar verwachting in het najaar van 2023 geopend voor inschrijving door mkb partijen.

Onder leiding van dcypher is in 2023 een operationeel overleg ingericht met representatie uit een groot aantal departementen om de technische elementen van drie prioritaire thema's (automatisering in cybersecurity, de digitale beveiliging van industriële/infrastructurele technologie, en digitale ketenrisico's) verder uit te werken en op termijn samen met bedrijven en kennisinstellingen toe te werken naar één of meerdere innovatieroutekaarten.

Op 30 maart 2023 is het Cybersecurity innovatieprogramma CS4NL (voorheen het Breed Gedragen Programma Cybersecurity BGP) van start gegaan. CS4NL biedt een impuls aan de innovatiekracht van Nederlandse topsectoren op het gebied van cybersecurity. Het programma pakt cyberveiligheidsvraagstukken op die voortkomen uit grote maatschappelijke transities en organiseert publiek-private samenwerking, bijvoorbeeld via onderzoeksfinanciering. In juni 2023 heeft de eerste open call plaatsgevonden vanuit de Topsector Logistiek, Energie, Tuinbouw & Uitgangsmaterialen, Life Sciences & Health, ICT en HTSM, rondom het thema 'Supply Chain Security': digitale veiligheid in en rondom logistieke ketens. Gehonoreerde onderzoeksprojecten zullen eind 2023 van start gaan. CS4NL wordt ondersteund door alle topsectoren, en uitgevoerd door samenwerkingsplatform dcypher. CS4NL zal naar verwachting over de komende vijf jaar 27 tot 36 miljoen euro helpen investeren in cybersecurity innovatie.

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. Als een van de eerste Europese lidstaten zal Nederland eind 2023 een volledig operationeel NCC opgezet hebben die in staat is haar Europese taakstelling te realiseren. Tevens zal NEXIS via RVO eind 2023 een eerste subsidie beschikbaar stellen om Nederlandse cybersecurity innovatieprojecten bij (met name) het mkb te stimuleren, in lijn met de Nederlandse prioritaire innovatiethema's voor cybersecurity. In 2023 heeft Nederland, met ondersteuning van het NCC, een sleutelrol gespeeld bij de totstandkoming van de Strategische Agenda van het ECCC. Hierbij is expliciete aandacht besteed aan de vertaling van Nederlandse innovatie- en onderzoeksbehoefte naar het Europese niveau. Eind 2023 worden de prioriteiten uit de Strategische Agenda doorvertaald naar een actieplan. Wederom wordt hierbij actief gestuurd op de borging van Nederlandse aandachtsgebieden. Beide documenten zullen de basis vormen voor toekomstige subsidieprogramma's als Digital Europe en Horizon 2020.

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

Zicht op statelijke actoren

In de afgelopen periode hebben de AIVD en MIVD ten eerste in het herstel van de verminderde operationele slagkracht geïnvesteerd. Ten tweede investeren beide diensten via gerichte transformatie en innovatie in het uitbouwen naar slagvaardige, data gedreven en technisch toekomstbestendige organisaties. Ten derde investeren zij in de structurele versterkingen van inlichtingenposities, waaronder de verhoging van de cyberweerbaarheid, door de onderzoekscapaciteit te versterken waarmee breder zicht ontstaat op de huidige en voorstelbare statelijke en niet-statelijke digitale dreiging. Daarnaast investeren beide diensten in het in kaart brengen van de verschillende aspecten van economische veiligheid en in de bescherming van vitale sectoren en processen in aansluiting op de behoefte van veiligheidspartners. Dit draagt bij aan de actie ten aanzien van het versterken van de onderzoekscapaciteit ten behoeve van inlichtingenmatig diepteonderzoek.

Op 1 december 2022 hebben de ministers van BZK en Defensie een voorstel voor de Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma ingediend bij de Tweede Kamer. Het voorstel wacht momenteel op behandeling. Met dit voorstel wordt een regeling getroffen om effectief onderzoek te kunnen doen naar landen met een offensief cyberprogramma gewaarborgd.

Onderzoeks- en opsporingscapaciteit cybercriminelen

Onderzoeks- en opsporingscapaciteit voor de bestrijding van cybercriminaliteit is een doorlopende actie voor de politie en het Openbaar Ministerie (OM). Dit sluit aan bij de doelstellingen die zijn opgenomen in de Veiligheidsagenda.[15] Formele rapportage over de afspraken uit de Veiligheidsagenda vindt plaats in het jaarverslag van de politie. Concrete resultaten van deze acties zijn bijvoorbeeld zaken als operatie cookie monster waarin is ingezet op alternatieve interventies zoals preventie en verstoren én op het opsporen en vervolgen van vermoedelijke daders. Een ander voorbeeld zijn de doorlopende bijdragen aan de *Counter Ransomware Initiative* (CRI) waardoor (inter)nationaal kennis wordt uitgewisseld over ransomware. Ook de in 2023 georganiseerde Oefendriehoek door de Vereniging van Nederlandse Gemeenten (VNG), politie en OM is een concrete uitwerking van de acties van politie en OM door meer bewustwording te creëren over de ontwikkelingen binnen de ondermijnende cybercriminaliteit en de uitdagingen die dit voor het lokale bestuur met zich meebrengt. Daarnaast is het opstellen van een eerste veiligheidsbeeld over cybercrime en gedigitaliseerde criminaliteit een belangrijke ontwikkeling.[16]

Het OM investeert in het vergroten van kennis en kunde op het gebied van cybercrimebestrijding. Hiervoor zijn concrete

15 Veiligheidsagenda 2023-2026 | Rapport | Rijksoverheid.nl
16 Kamerstuk II, 2022 – 2023, 26 643, nr. 930

leerprogramma's opgesteld op diverse kennisniveaus. Er wordt bijvoorbeeld in september 2023 gestart met de Cyberacademy voor ambtenaren werkzaam bij het OM.

Versterken diplomatiek netwerk

Om het internationaal cyberbeleid zo efficiënt mogelijk te implementeren heeft het ministerie van Buitenlandse Zaken het aantal cyberdiplomaten aanzienlijk uitgebreid waardoor inmiddels 34 functies op ambassades en Permanente Vertegenwoordigingen een aanzienlijke cybercomponent hebben.[17] Hierdoor neemt de aandacht voor cybervraagstukken op vertegenwoordigingen toe waardoor internationaal cyberbeleid een meer integraal onderdeel wordt van het bredere Nederlandse buitenlandbeleid.

Attributie en respons

Voor het vergroten van onze cyberweerbaarheid is effectieve samenwerking binnen de EU en NAVO en cruciaal. Daarom neemt Nederland binnen beide organisaties een voortrekkersrol om de beleidsvorming inzake het tegengaan van statelijke cyberdreigingen positief te beïnvloeden. Zo is Nederland binnen de EU afgelopen jaar aanjager geweest van de discussie over het aanscherpen van de zogenaamde *Cyber Diplomacy Toolbox*, het geheel aan diplomatieke maatregelen dat de EU tot zijn beschikking heeft om te kunnen reageren op statelijke cyberdreigingen. Nederland heeft er onder andere voor gepleit dat het sanctie instrumentarium gerichter en frequenter moet kunnen worden ingezet. Binnen de NAVO was Nederland het afgelopen jaar, samen met een zestal bondgenoten, trekker van het *Allies Help Allies* initiatief, gericht op preventie van cyberincidenten.

Concrete resultaten van de diplomatieke inzet op het tegengaan van statelijke cyberdreigingen waren de bijdragen die Nederland leverde aan de EU- en NAVO reacties op de cyberaanvallen op Albanië en het opnemen van een nieuw criterium in het 11e sanctiepakket tegen Rusland dat het mogelijk maakt om personen en entiteiten die betrokken zijn bij Russische cyberoperaties te listen.[18] [19] Dankzij dit criterium heeft de EU direct negen Russische cyber-toeleveranciers op een sanctielijst kunnen plaatsen.

Voor pijler III geldt dat veel van de opgenomen doelstellingen en actielijnen verder zijn uitgewerkt in de Internationale Cyberstrategie (ICS) die in juni 2023 verscheen.[20] Over de voortgang ICS omtrent de implementatie van de ICS wordt uw Kamer jaarlijks aan het begin van de zomer geïnformeerd.

Defensieve en offensieve cybercapaciteiten

Zoals in het CSBN2023 geschetst vraagt de huidige geopolitieke situatie onze aandacht. Statelijke actoren grijpen namelijk naar cyberaanvallen om hun belangen te behartigen. Geopolitieke spanningen en verharding dragen hieraan bij. Defensie werkt, met het Defensie Cyber Commando (DCC), de MIVD, het Defensie Cyber Security Centrum (DCSC) en de krijgsmachtdelen, daarom continu aan het verbeteren van de *cyber readiness*. Hierin wordt de komende periode flink geïnvesteerd. Daarbij gaat het niet alleen om het vergroten van de cyberveiligheid van de eigen netwerken en (wapen)systemen, maar speelt Defensie ook een rol om in samenwerking met civiele en internationale partners Nederland digitaal veilig te houden. Bovendien moet de krijgsmacht tijdens een gewapend conflict in staat zijn om in coalitieverband cyberoperaties uit te voeren en te synchroniseren met activiteiten op zee, te land, in de lucht en in de ruimte. De beleidsvisie Informatiegestuurd Optreden, die op 4 juli 2023 naar de Kamer is gestuurd, geeft richting aan deze integratie van cyberoperaties met andere effectbrengers en capaciteiten in de informatieomgeving.

Defensie draagt binnen de eigen organisatie zorg voor het afstemmen van activiteiten in het cyberdomein om de inlichtingenpositie, de digitale weerbaarheid, de offensieve capaciteiten en de rechtshandhaving gelijktijdig te versterken. Centraal in deze ontwikkeling staat het verder uitbouwen en versterken van het interne netwerk van operatiecentra die niet alleen op elkaar, maar ook op de operatiecentra van nationale en internationale partners zijn aangesloten, zoals die van JenV, de EU en de NAVO. In hun samenwerking dragen deze centra zorg voor een goed zicht op en begrip van de ontwikkelingen in het cyberdomein. Een uitbreiding van interne, nationale en internationale oefeningen moet de spankracht van dit netwerk continu testen.

Het CSBN2023 constateert dat cybercriminelen gebruik maken van de reguliere digitale infrastructuur zoals bonafide webhostingbedrijven en cloudservices, dit onderstreept het belang van de verkenning naar de mogelijkheden tot het blokkeren van malafide verkeer door Nederlandse Internet Service Providers. Deze verkenning wordt in 2024 opgepakt.

17 Kamerstuk 35 925 V nr.11
18 Zie EU- & NAVO-verklaringen over cyberincidenten in Albanië
19 11th package of sanctions (europa.eu)
20 Internationale Cyberstrategie 2023 - 2028 | Publicatie | Rijksoverheid.nl

Normatief kader en internet governance

Internationale afspraken over verantwoord statelijk gedrag in het digitale domein zijn een belangrijke voorwaarde om het risico op statelijke cyberdreigingen te beperken. Verdere ontwikkeling van bestaande gedragsregels (vastgelegd in het VN normatief kader) is onder de huidige geopolitieke spanningen zeer complex. Met name Rusland en in iets mindere mate China pogen die onderhandelingen te frustreren. Rusland deelde een voorstel om in VN-verband te komen tot een bindend verdrag over verantwoordelijk statelijk gedrag in het cyberdomein. Voor Nederland is dat nu niet wenselijk. We beschikken immers al over een normatief kader én de vaststelling dat internationaal recht integraal van toepassing is op het cyberdomein. Daar tegenover staat dat Nederland het afgelopen jaar een belangrijke rol gespeeld bij de totstandkoming van een met grote steun aangenomen VN-resolutie voor een *Programme of Action* (PoA). Het PoA moet de opvolger zijn van de huidige door Rusland geïnitieerde *Open Ended Working Group* (OEWG) en moet zich richten op het bijstaan van VN-leden bij de implementatie van het bestaande normatief kader.

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. Dit vraagt om meer Nederlandse inzet in multistakeholder internetorganisaties zoals ICANN en in de multilaterale VN-organisatie International Telecommunications Union (ITU) door de toegenomen presentie van Rusland en China daarin. De inzet van EZK 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.

Daarnaast is afgelopen jaar een proces gestart om op VN-niveau een akkoord te bereiken op een "Global Digital Compact" in september 2024 tijdens de VN Summit of the Future. Dit verdrag moet leiden tot een wereldwijd gedeelde visie op een open, vrij, veilig en mensgerichte digitale toekomst, waaraan de doelstellingen en beginselen van het VN Handvest en de Universele Mensenrechten Verklaring en de Agenda 2030 ten grondslag liggen.[21] Een akkoord hierop bereiken zal door de geopolitieke spanningen zijn uitdagingen kennen. Nederland heeft in april 2023 actief input geleverd in EU-verband, FOC-verband en als individuele lidstaat.[22] [23] [24]

21 our-common-agenda-policy-brief-gobal-digi-compact-en.pdf (un.org)
22 GDC-submission_European-Union.pdf
23 GDC-submission_Freedom-Online-Coalition.pdf (un.org)
24 Global Digital Compact (un.org)

Toenemende digitalisering biedt het onderwijs veel kansen, bijvoorbeeld door het aanbieden van online colleges en voor het ontsluiten van kennis. Tegelijkertijd brengt deze grotere 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

Voorlichtingscampagnes burgers

De ministeries van Binnenlandse Zaken en Koninkrijksrelaties (BZK), Economische Zaken en Klimaat (EZK) en Justitie en Veiligheid (JenV) trekken samen op in een overkoepelende (publieks) campagneaanpak op cybersecurity. Inmiddels zijn de eerste ideeën hiervoor uitgewerkt. Dit najaar zullen in het kader van deze aanpak (wederom) campagnes op verschillende thema's van start gaan, namelijk *social engineering*, *2-factor authenticatie en updates voor slimme apparaten.* Het thema *social engineering* sluit goed aan bij lopende BZK-initiatieven om de bewustwording over digitale vaardigheden en online risico's bij kwetsbare groepen zoals laaggeletterden en senioren te verbeteren en zal naast een landelijke campagne ook lokale aandacht krijgen via het netwerk van sociaal-maatschappelijke en culturele instellingen waarmee BZK vanuit inclusie samenwerkt. Eind 2023 zal een volgende ronde van de publieks-campagne 'Doe je updates' plaats vinden.

In het kader van de City Deal lokale weerbaarheid cybercrime zijn subsidies verleend voor projecten die de cyberweerbaarheid op lokaal niveau versterken. In totaal is er vanaf 2022 tot 2025 jaarlijks twee miljoen euro beschikbaar om gemeenten via de City Deal te ondersteunen. De In 2023 is er een tweede tranche van subsidies gegeven, specifiek voor projecten ter preventie van cybercrime. De tweede tranche is in juni afgesloten met het congres 'City Deal Lokale Weerbaarheid Cybercrime'. Tijdens dit congres hebben 17 innovatieve cyberprojecten hun resultaten gepresenteerd, zoals bijvoorbeeld het Youth Cyber Team (Gemeente Arnhem): dit project richt zich op het versterken van de cyberweerbaarheid van kwetsbare jongeren uit twee Arnhemse wijken. Samen met de eerste tranche zijn er binnen de City Deal nu 32 innovatieve pilots opgeleverd. De City-Deal Lokale Weerbaarheid Cybercrime projecten worden door VNG versterkt via de GemeenteDelers. De derde tranche wordt in het najaar van 2023 uitgevraagd, en begin 2024 uitgegeven. In de derde tranche ligt de focus met name op implementeren en borgen van de effectieve pilots uit de eerste en tweede tranche, maar er is ook ruimte voor nieuwe innovatieve pilots. De komende tijd vinden er evaluaties van de pilots plaats om de effectiviteit te bepalen.

Beveiligingsadvies burgers

Om burgers beter te voorzien van informatie en beveiligings-adviezen op het gebied van digitale veiligheid zijn verschillende acties opgepakt. Zo wordt er momenteel gewerkt aan een tool die de Informatiepunten Digitale Overheid (IDO) ondersteunen om hulpvragen van burgers op het terrein van cyberveiligheid te beantwoorden en waar nodig door te verwijzen naar bestaande steunpunten, informatieloketten en lokale ondersteuningsinitia-tieven van private partners. De tool wordt volgens planning eind 2023 opgeleverd.

Tenslotte is onderzocht hoe de publiek-private website veiliginter-netten.nl het beste kan worden doorontwikkeld. Dit is gedaan door middel van het jaarlijkse onderzoek naar verschillende elementen van de website veiliginternetten.nl, denk aan: vind-baarheid, demografie bezoekers en functionaliteit. Veiliginternetten.nl kreeg voor 2022 een 7,8 als rapportcijfer ten opzichte van de 6,5 van de Nederlandse websites gemiddeld. Hiermee is deze actie uit het actieplan afgerond.

Betrouwbaarheid digitale overheidsvoorzieningen

Ter verbetering van de herkenbaarheid van de overheid op het internet wordt gewerkt aan de ontwikkeling van een "register internetdomeinen overheid", zodat burgers via dit register een snelle check kunnen doen of internetdomeinen van de overheid zijn of niet. Een eerste versie van het register wordt in Q4 2023 opgeleverd.

Burgers reageren snel en adequaat op cyberincidenten

Er is een online aangiftemogelijkheid voor ransomware in ontwikkeling bij de politie. De politie rapporteert formeel in haar jaarverslag over deze afspraak uit de veiligheidsagenda.

Onderwijs: Curriculum

De Stichting Leerplan Ontwikkeling (SLO) werkt momenteel samen met het onderwijsveld aan concrete kerndoelen voor de te ontwikkelen basisvaardigheden, waarvan digitale veiligheid onderdeel uitmaakt. De concept kerndoelen zijn in het najaar van 2023 gereed en worden na overhandiging aan het ministerie gepubliceerd op de website van de SLO. Daarna volgt een periode van beproeving in 2024 en 2025. De implementatie wordt verwacht in 2026. Ter ondersteuning van leerkrachten wordt daarnaast in het najaar van 2023 het expertisepunt Digitale Geletterdheid gelanceerd. Dit is onderdeel van de landelijke ondersteuningsstructuur om de digitale geletterdheid van kinderen te verbeteren.

Cybersecurity arbeidsmarkt

In juni 2023 is in opdracht van het ministerie van EZK een start gemaakt met een onderzoek naar de kwalitatieve en kwantitatieve tekorten op de cybersecurity arbeidsmarkt. Naast een probleemanalyse, opgeleverd in december 2023, wordt begin 2024 ook een beleidsadvies opgeleverd. Doelstelling is om ook tijdens het onderzoek specifiek aandacht te besteden aan het creëren van draagvlak in het veld om zo fragmentatie tegen te gaan in de ICT-brede aanpak van de Rijksoverheid en slagkracht te creëren. Naast dit initiatief hebben EZK, SZW en OCW onder regie van EZK het *actieplan Groene en Digitale banen* ontwikkeld.[25] In dit plan staan maatregelen die het kabinet neemt om de tekorten op de technische en digitale arbeidsmarkt in te perken. Onderstaande initiatieven zijn onderdeel van het actieplan groene en digitale banen.

De *Human Capital Agenda ICT* (HCA ICT) richt zich sinds 2015 op het aanpakken van de groeiende vraag naar ICT-professionals in Nederland, waaronder cybersecurityspecialisten. De HCA ICT werkt aan de ambitie van het kabinet om in 2030 1 miljoen digitaal geschoolden in Nederland beschikbaar te hebben en is betrokken bij het actieplan Groene en Digitale banen.[26] In de afgelopen jaren is onder de HCA ICT een sterk netwerk gebouwd tussen bedrijfsleven, onderwijsinstellingen en overheden. Netwerkkaart ontwikkeld waarin publiek-private samenwerkingen overzichtelijk gepresenteerd worden, regioprofielen zijn opgesteld waarin vraag en aanbod op regionaal niveau zichtbaar wordt en werkende modellen gepresenteerd die werken, zoals omscholingsmodellen.[27] [28] [29] Eén van deze omscholingsprogramma's dat mogelijk wordt gemaakt met de investeringen vanuit EZK is *Make IT Work*, waarbij het bedrijfsleven en onderwijsinstellingen werkenden omscholen tot cyber security specialist en gedurende de scholing kunnen genieten van baangarantie na afronding.

Het ministerie van OCW investeert structureel in hbo-opleidingen in de bètatechniek, waar cybersecurityopleidingen ook onderdeel van zijn. Middelen worden ingezet op (1) hogere instroom binnen de opleiding, (2) lagere studie-uitval en -switch, (3) hogere zijinstroom en, (4) warme overgang van opleiding naar arbeidsmarkt. Het doel van deze maatregel is om de arbeidsmarkttekorten in te perken. OCW zal in 2025 deze investering tussentijds evalueren. Het is nog te vroeg om de effecten van deze investering in kaart te brengen.

OCW werkt aan de doorontwikkeling van Leven-Lang-Ontwikkelen-beleid (LLO). In het najaar van 2023 wordt hierover een brief met de Kamer gedeeld. OCW onderzoekt de komende jaren hoe geleidelijk meer maatwerkmogelijkheden in het onderwijsstelsel kunnen worden ingevoerd met betrekking tot LLO.

Er worden binnen de bestaande sectorplannen Bèta en Techniek verschillende posities voor onderzoek en onderwijs met een focus op cybersecurity gefinancierd. Deze plannen zijn gestart in 2018 en de eindevaluatie vindt plaats 2025. Binnen de nieuwe sectorplannen Bèta en Techniek, die lopen van 2022 tot en met 2029, wordt ook geïnvesteerd in cybersecurity. Het gaat hierbij onder andere om onderzoek naar veiligheid en robuustheid van AI (gebaseerde) digitale systemen. De implementatie en uitvoering van de sectorplannen Bèta en Techniek zullen de komende 6 jaar worden gemonitord door de Sectorplancommissie Bèta en Techniek. Deze commissie zal zowel een midterm evaluatie als eindevaluatie opleveren voor de minister van OCW.

25 Kamerstukken II 2022-2023, 29544, nr. 1173
26 Kamerstukken II 2022-2023, 26643, nr. 941 (bijlage strategie digitale economie)
27 https://netwerk.wijzijnkatapult.nl/map/hcaict/?
28 https://hcaicat.nl/regioprofielen
29 https://www.wijzijnkatapult.nl/hcaict/werkende-modellen/

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 2023