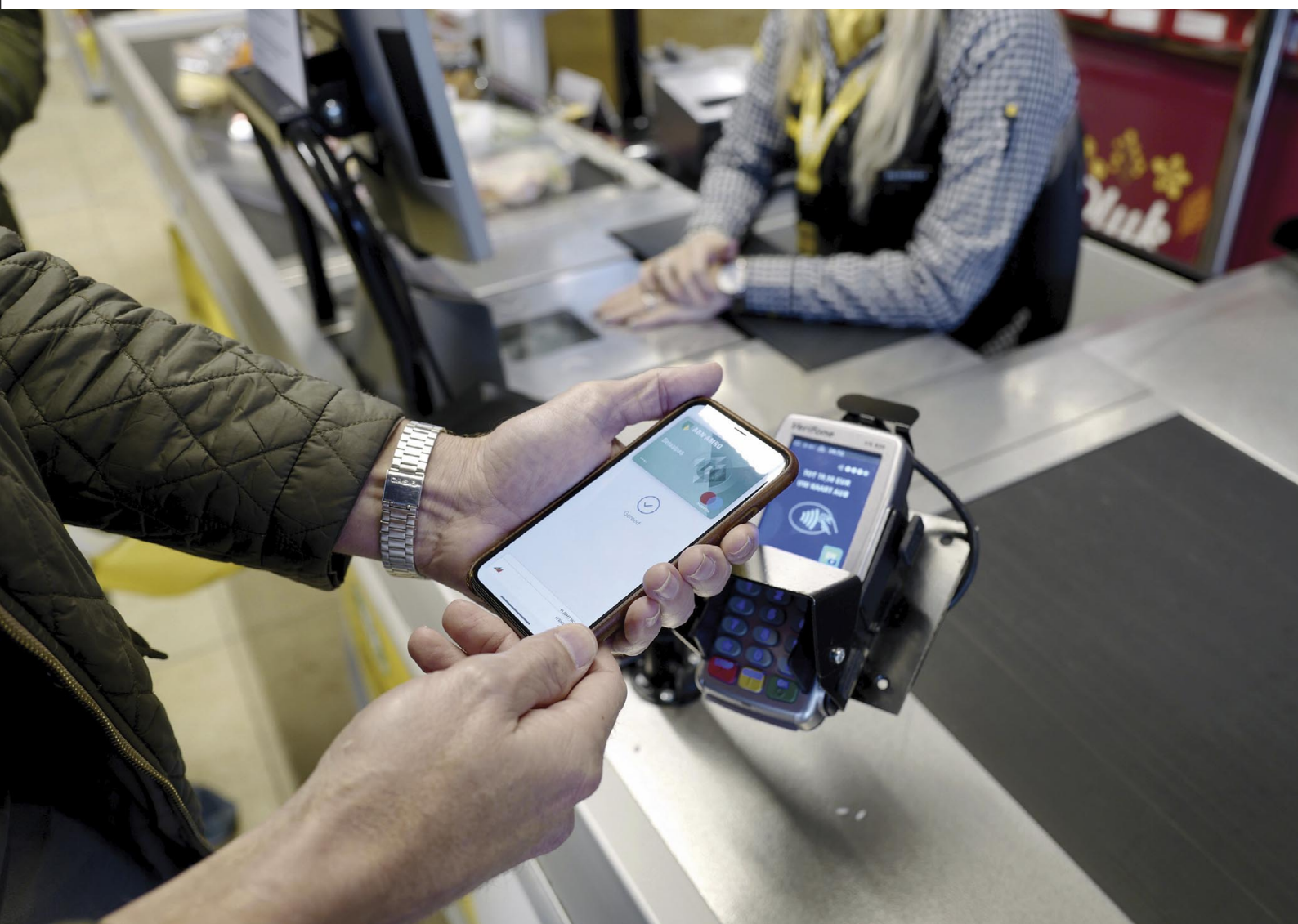




# Actieplan Nederlandse Cybersecuritystrategie 2022-2028

Ambities en acties voor een digitaal veilige samenleving





*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.*

De Nederlandse Cybersecuritystrategie (NLCS) is tot stand gekomen met een brede betrokkenheid van publieke, private en maatschappelijke organisaties, onder coördinatie van de Nationaal Coördinator Terroris-  
mebestrijding en Veiligheid (NCTV). Het Cybersecurity Beeld Nederland 2022 (CSBN) vormt het uitgangspunt voor de pijlers en doelstellingen van de NLCS.


# Actieplan Nederlandse Cybersecuritystrategie 2022-2028


Ambities en acties voor een digitaal veilige samenleving

# Inhoud

	<b>Pijler I</b>	
	<b>Digitale weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties</b>	
<b>Doel 1</b>	<b>Organisaties hebben zicht op cyberincidenten, -dreigingen en -risico's en hoe hiermee om te gaan.</b>	<b>7</b>
	Herziening van het stelsel	7
	Versterken Landelijk Dekkend Stelsel van cybersecurity samenwerkingsverbanden (LDS)	8
	Uitbreiden schakelorganisaties binnen het LDS	9
	Nationaal Detectie Netwerk (NDN)	10
	Slachtoffernotificatie	10
<b>Doel 2</b>	<b>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.</b>	<b>11</b>
	Digitale weerbaarheid vitale infrastructuur	11
	Digitale weerbaarheid MKB en bedrijfsleven	14
	Digitale weerbaarheid onderwijs	15
	Digitale weerbaarheid zorginstellingen	16
	Digitale weerbaarheid sectoren infrastructuur en waterstaat	17
	Digitale weerbaarheid rijksoverheid	18
	Digitale weerbaarheid overheid	19
	Digitale weerbaarheid sectoren met operationele technologie- en procesautomatiserings-systemen	20
	Zicht op digitale weerbaarheid van overheid en bedrijfsleven	21
<b>Doel 3</b>	<b>Organisaties reageren, herstellen en leren snel en adequaat op en van cyber-incidenten en -crises.</b>	<b>22</b>
	Incident- en crisispreparatie	22
	Oefenen	24
	<b>Pijler II</b>	
	<b>Veilige en innovatieve digitale producten en diensten</b>	
<b>Doel 1</b>	<b>Digitale producten en diensten zijn veiliger.</b>	<b>25</b>
	Europese wetgeving voor digitale producten en diensten	25
	Toezicht en handhaving op digitale producten en diensten	26
	Certificering en standaarden	27
	Algemene beveiligingseisen rijksoverheid (ABRO) en overheidsinkoopbeleid	29

<b>Doel 2</b>	<b>Nederland heeft een sterke cybersecuritykennis- en innovatieketen</b>	<b>32</b>
	Veilige cryptografie	32
	Nationale samenwerking kennis- en innovatie-onderzoekssamenwerking	33
	Europese onderzoekssamenwerking en fondsen	34

	<b>Pijler III</b>	
	<b>Tegengaan van digitale dreigingen van staten en criminelen</b>	
<b>Doel 1</b>	<b>Nederland heeft zicht op digitale dreigingen van staten en criminelen</b>	<b>37</b>
	Zicht op statelijke actoren	37
	Onderzoeks- en opsporingscapaciteit cybercriminelen	38
	Versterken diplomatiek netwerk	39
<b>Doel 2</b>	<b>Nederland heeft grip op digitale dreigingen van staten en criminelen</b>	<b>40</b>
	Attributie en respons	40
	Defensieve en offensieve cybercapaciteiten	41
<b>Doel 3</b>	<b>Staten houden zich aan het normatief kader voor verantwoordelijk statelijk gedrag in de digitale ruimte</b>	<b>42</b>
	Normatief kader	42
	Internet governance	43

	<b>Pijler IV</b>	
	<b>Cybersecurity-arbeidsmarkt, onderwijs en digitale weerbaarheid van burgers</b>	
<b>Doel 1</b>	<b>Burgers zijn goed beschermd tegen digitale risico's.</b>	<b>43</b>
	Voorlichtingscampagnes	43
	Beveiligingsadvies burgers	44
	Betrouwbaarheid digitale overheidsvoorzieningen	45
<b>Doel 2</b>	<b>Burgers reageren snel en adequaat op cyberincidenten.</b>	<b>46</b>
<b>Doel 3</b>	<b>Leerlingen krijgen onderwijs in digitale vaardigheden gericht op veiligheid.</b>	<b>47</b>
	Curriculum	47
<b>Doel 4</b>	<b>De Nederlandse arbeidsmarkt kan voldoen aan de toenemende vraag naar cybersecurity-experts.</b>	<b>48</b>
	Cybersecurity arbeidsmarkt	48

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

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

#### Herziening van het stelsel

<p><b>Actie samenvatting</b> Het NCSC, DTC en CSIRT-DSP worden samengevoegd tot één nationale cybersecurity autoriteit (CSIRT).</p>	<p><b>Tijdslijn</b> 2022-2026</p>	<p><b>Eigenaar</b> JenV, EZK</p> <p><b>Betrokken</b> NCSC, DTC, CSIRT-DSP</p>
<p><b>Actie samenvatting</b> Voor de overheidsschakelorganisaties binnen het cybersecurity informatiedelingsstelsel wordt beoordeeld welke van hun taken centraal (bij de nationale cybersecurity autoriteit) of sectoraal moeten worden belegd.</p>	<p><b>Tijdslijn</b> 2022-2023</p>	<p><b>Eigenaar</b> JenV, EZK</p> <p><b>Betrokken</b> VWS, BZK, DEF, OCW, IenW</p>
<p><b>Actie samenvatting</b> Samen met het bedrijfsleven wordt een routekaart opgesteld voor de implementatie van een publiek-privaat platform voor wederkerige cybersecurity informatie- en kennisdeling. De basis voor dit traject is het opgeleverde Cyclotronrapport.</p>	<p><b>Tijdslijn</b> 2022-2023</p>	<p><b>Eigenaar</b> JenV</p> <p><b>Betrokken</b> NCSC, DTC, AIVD, MIVD, politie, OM, private partners, medeoverheden</p>
<p><b>Actie samenvatting</b> Het NCSC verkent met partners de haalbaarheid van een centrale landelijke campus/locatie ter bevordering van samenwerking, informatiedeling, kennisontwikkeling en onderzoek tussen publieke en private partijen.</p>	<p><b>Tijdslijn</b> 2022-2023</p>	<p><b>Eigenaar</b> JenV</p> <p><b>Betrokken</b> NCSC, DTC, AIVD, MIVD, politie</p>

## Versterken Landelijk Dekkend Stelsel van cybersecurity samenwerkingsverbanden (LDS)

<p><b>Actie samenvatting</b> Het wettelijk kader wordt gewijzigd zodat organisaties binnen het LDS in staat worden gesteld om informatie over cybersecurity breed, efficiënt en effectief met elkaar te delen. Voorbeelden hiervan zijn de aankomende wijziging van de Wbni die dit najaar in de Kamer wordt behandeld en het wetsvoorstel bevordering digitale weerbaarheid bedrijven.</p>	<p><b>Tijdslijn</b> 2022-2026</p>	<p><b>Eigenaar</b> JenV, EZK</p> <p><b>Betrokken</b> DTC, NCSC</p>
<p><b>Actie samenvatting</b> In interdepartementaal verband worden eisen voor aansluiting op het LDS geformuleerd. Deze zullen verplichtend zijn voor overheidsschakelorganisaties en als richtinggevende leidraden gelden voor private schakelorganisaties. Private partners worden betrokken bij de uitwerking van deze leidraden.</p>	<p><b>Tijdslijn</b> 2023-2024</p>	<p><b>Eigenaar</b> JenV</p> <p><b>Betrokken</b> EZK, VWS, IenW, DTC, NCSC</p>
<p><b>Actie samenvatting</b> Het kabinet gaat schakelorganisaties ondersteunen met financieringsmodellen waardoor zij in staat worden gesteld om duurzame financiering te borgen.</p>	<p><b>Tijdslijn</b> 2023-2026</p>	<p><b>Eigenaar</b> JenV</p> <p><b>Betrokken</b> NCSC, DTC</p>
<p><b>Actie samenvatting</b> Er wordt een communicatieplan LDS opgeleverd aan de hand waarvan organisaties wegwijs kunnen worden binnen het stelsel. Onderdeel hiervan is te komen tot heldere aanspreekpunten.</p>	<p><b>Tijdslijn</b> 2023-2025</p>	<p><b>Eigenaar</b> JenV</p> <p><b>Betrokken</b> BZK, EZK, NCSC, DTC</p>

## Uitbreiden schakelorganisaties binnen het LDS

<p><b>Actie samenvatting</b> In samenwerking met private partners wordt een LDS-bouwplan opgesteld dat het kabinet in staat stelt om samen met het bedrijfsleven de dekking van het LDS te verhogen. Onderdeel van dit bouwplan is een overzicht van de huidige staat van het LDS om inzicht te creëren in alle initiatieven die reeds zijn ontwikkeld en de huidige leemtes in het LDS.</p>	<p><b>Tijdslijn</b> 2022-2026</p>	<p><b>Eigenaar</b> JenV</p> <p><b>Betrokken</b> EZK, OCW, VWS, IenW, BZK, NCSC, DTC, medeoverheden en private partners</p>
<p><b>Actie samenvatting</b> Met een financiële bijdrage van BZK gaan de provincies, onder regie van het IPO, verder met het inrichten van interprovinciaal informatieknooppunt als schakelorganisatie binnen het LDS.</p>	<p><b>Tijdslijn</b> 2022-2023</p>	<p><b>Eigenaar</b> BZK</p> <p><b>Betrokken</b> IPO</p>
<p><b>Actie samenvatting</b> OCW richt een CERT op voor het primair en voortgezet onderwijs.</p>	<p><b>Tijdslijn</b> 2022-2023</p>	<p><b>Eigenaar</b> OCW</p> <p><b>Betrokken</b> OCW en SURFcert</p>
<p><b>Actie samenvatting</b> IenW versterkt het CERT Watermanagement.</p>	<p><b>Tijdslijn</b> 2022-2023</p>	<p><b>Eigenaar</b> IenW</p> <p><b>Betrokken</b> RWS</p>

## Nationaal Detectie Netwerk (NDN)

<b>Actie samenvatting</b> Alle nog niet aangesloten Rijksoverheidsorganisaties worden aangesloten op het Nationaal Detectie Netwerk.	<b>Tijdslijn</b> 2023	<b>Eigenaar</b> BZK  <b>Betrokken</b> JenV, CIO-Rijk, NCSC
<b>Actie samenvatting</b> De samenwerking en informatiedeling tussen de partners in het Nationaal Detectie Netwerk (AIVD, MIVD, NCSC) en de dienstverlening richting aangesloten organisaties wordt versterkt door geïntensiverde onderlinge kennisuitwisseling.	<b>Tijdslijn</b> 2023-2026	<b>Eigenaar</b> JenV  <b>Betrokken</b> AIVD, MIVD, NCSC, CIO-Rijk

## Slachtoffernotificatie

<b>Actie samenvatting</b> Er komt een 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. De NCTV en NCSC onderzoeken hierbij specifiek hoe slachtoffernotificatie uit niet-strafrechtelijke bron verder kan worden vormgegeven.	<b>Tijdslijn</b> 2022-2023	<b>Eigenaar</b> JenV  <b>Betrokken</b> NCSC, AIVD, MIVD en private partners
<b>Actie samenvatting</b> De politie en het OM verkennen op welke manier het notificeren van slachtoffers die blijken uit strafrechtelijke onderzoeken verder vorm kan krijgen.	<b>Tijdslijn</b> 2022-2025	<b>Eigenaar</b> JenV  <b>Betrokken</b> OM, Politie, NCTV, NCSC

**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.**

## Digitale weerbaarheid vitale infrastructuur

<b>Actie samenvatting</b> De vernieuwde EU NIB-richtlijn (NIB2) zal in 2024 via de Wbni in Nederland worden geïmplementeerd.	<b>Tijdslijn</b> 2022- 2024	<b>Eigenaar</b> JenV  <b>Betrokken</b> OCW, BZK, IenW, VWS, FIN, EZK, LNV, MIVD, AIVD en NCSC
<b>Actie samenvatting</b> Om de lasten voor bedrijven zoveel mogelijk te beperken, zal sectorale wetgeving, zoals de DORA en de Network Code en aanpalende wetgeving zoals de CER-richtlijn in nauwe samenhang met de NIB2 worden geïmplementeerd.	<b>Tijdslijn</b> 2022- 2024	<b>Eigenaar</b> JenV  <b>Betrokken</b> FIN, EZK, OCW, BZK, IenW, VWS en LNV
<b>Actie samenvatting</b> Het kabinet start in 2023 met uitgebreide voorlichtingscampagnes om organisaties die onder de nieuwe wet komen te vallen te informeren over voor hun geldende rechten en plichten, en hen actief te begeleiden bij de implementatie.	<b>Tijdslijn</b> 2023-2024	<b>Eigenaar</b> JenV  <b>Betrokken</b> OCW, BZK, IenW, VWS, FIN, EZK en LNV
<b>Actie samenvatting</b> Om kwaliteit en consistentie van het toezicht op de Wbni na de implementatie van de NIB2 te verzekeren, wordt het <i>Samenhangend Inspectiebeeld Cybersecurity Vitale Processen</i> en de bijhorende governance doorontwikkeld. Op deze manier wordt de samenhang in en transparantie over de aanpak van informatiegestuurd en risicogericht toezicht geborgd.	<b>Tijdslijn</b> 2022- 2024	<b>Eigenaar</b> JenV  <b>Betrokken</b> OCW, BZK, IenW, VWS, FIN, EZK en LNV

<p><b>Actie samenvatting</b> Verkenning naar het opzetten van één centraal meldloket waarmee meldingen voor NIBz laagdrempelig en gelijktijdig kunnen worden gedaan bij het CSIRT en de toezichthouder. Bij deze verkenning worden ook meldingen uit gerelateerde wetgeving betrokken (AVG, DORA, Network Code).</p>	<p><b>Tijdslijn</b> 2022- 2024</p>	<p><b>Eigenaar</b> JenV</p> <p><b>Betrokken</b> OCW, BZK, IenW, VWS, FIN, EZK en LNV</p>
<p><b>Actie samenvatting</b> Evalueren van de huidige methode voor het vaststellen van drempelwaarden meldplicht voor cyberincidenten onder de Wbni. Deze uitkomsten worden in ieder geval betrokken bij het bepalen van drempelwaarden voor nieuw aangewezen aanbieders.</p>	<p><b>Tijdslijn</b> 2022- 2024</p>	<p><b>Eigenaar</b> JenV</p> <p><b>Betrokken</b> OCW, BZK, IenW, VWS, FIN, EZK en LNV</p>
<p><b>Actie samenvatting</b> Het NCSC zal gezien de toename van doelgroeporganisaties, schaalbare technische voorzieningen voor digitale en geautomatiseerde informatiedeling met en tussen doelgroepen en partners realiseren en implementeren.</p>	<p><b>Tijdslijn</b> 2022- 2024</p>	<p><b>Eigenaar</b> JenV</p> <p><b>Betrokken</b> NCSC</p>
<p><b>Actie samenvatting</b> De NIBz-eisen hebben raakvlakken met de Baseline Informatiebeveiliging Overheid (BIO) en worden waar van toepassing daarin opgenomen zodat de verbinding met de basisbeveiliging voor de overheid herkenbaar blijft.</p>	<p><b>Tijdslijn</b> 2022-2024</p>	<p><b>Eigenaar</b> BZK</p> <p><b>Betrokken</b></p>
<p><b>Actie samenvatting</b> Er wordt gestart met een verkenning naar de benodigde stappen voor het verhogen van de digitale weerbaarheid van de vitale infrastructuur in Caribisch Nederland.</p>	<p><b>Tijdslijn</b> 2022-2024</p>	<p><b>Eigenaar</b> JenV</p> <p><b>Betrokken</b> BZK</p>

<p><b>Actie samenvatting</b> Het kabinet start een Versterkte Aanpak Vitaal om de bescherming van de Nederlandse vitale infrastructuur te verbreden. Onderdeel van deze aanpak is een herziening van het vitaalbeleid en bijbehorende wetgeving, mede in het licht van de CER- en NIBz-richtlijnen. Vitale aanbieders zullen begin 2023 over het nieuwe stelsel worden geconsulteerd. De versterkte aanpak voorziet daarnaast in een structurele samenwerking met een deel van de vitale sectoren, een verbeterd beleidsinstrumentarium om sectorale risico's en afhankelijkheden beter in beeld te krijgen en in een doorontwikkeling van informatiedeling over kwetsbaarheden en dreigingen. Cybersecurity maakt hier integraal deel van uit.</p>	<p><b>Tijdslijn</b> 2022-2024</p>	<p><b>Eigenaar</b> JenV</p> <p><b>Betrokken</b> OCW, BZK, IenW, VWS, FIN, EZK, LNV, NCSC, AIVD en MIVD</p>
---	---------------------------------------	--

## Digitale weerbaarheid MKB en bedrijfsleven

<p><b>Actie samenvatting</b> NCSC en DTC ontwikkelen nieuwe producten en diensten met onder andere aandacht voor inbedding van cybersecurity in het risicomanagementproces; crisispreparatie; incidentrespons en thematische advisering. Deze gedifferentieerde en datagedreven informatie- en kennisproducten en -diensten worden gezamenlijk en laagdrempelig beschikbaar gesteld ten behoeve van organisaties op een manier die past bij het volwassenheidsniveau.</p>	<p><b>Tijdljn</b> 2022-2024</p>	<p><b>Eigenaar</b> JenV, EZK</p> <p><b>Betrokken</b> NCSC, DTC</p>
<p><b>Actie samenvatting</b> Realisatie van eerste versie van centrale registers voor cybersecurity gerelateerde informatie (i.e. type ransomware, kwetsbaarheden).</p>	<p><b>Tijdljn</b> 2023</p>	<p><b>Eigenaar</b> JenV</p> <p><b>Betrokken</b> NCSC</p>
<p><b>Actie samenvatting</b> Het gebruik van tools, zoals risicoscans, en producten en beveiligingsadviezen incl. handelingsperspectief, stimuleren onder het MKB onder andere via brancheorganisaties, zoals bij het publiek-private platform Samen Digitaal Veilig.</p>	<p><b>Tijdljn</b> 2022-2024</p>	<p><b>Eigenaar</b> EZK, JenV</p> <p><b>Betrokken</b> DTC, NCSC, VNO-NCW, MKB-Nederland</p>
<p><b>Actie samenvatting</b> Er wordt één set aan basismaatregelen vanuit de overheid geformuleerd en gepromoot voor vrijwillig gebruik door organisaties.</p>	<p><b>Tijdljn</b> 2023 - 2024</p>	<p><b>Eigenaar</b> JenV</p> <p><b>Betrokken</b> EZK, BZK, NCSC, DTC, AIVD, MIVD</p>

## Digitale weerbaarheid onderwijs

<p><b>Actie samenvatting</b> Er wordt een normenkader informatiebeveiliging en privacy geïmplementeerd voor het primair en voortgezet onderwijs, incl. periodieke monitors en benchmarks om te volgen of schoolbesturen voldoen aan de norm.</p>	<p><b>Tijdljn</b> 2022-2024</p>	<p><b>Eigenaar</b> OCW</p>
<p><b>Actie samenvatting</b> Schoolbesturen in het primair en voortgezet onderwijs besteden in hun jaarverslag verplicht expliciet aandacht aan informatiebeveiliging en privacy.</p>	<p><b>Tijdljn</b> 2022-2024</p>	<p><b>Eigenaar</b> OCW</p>
<p><b>Actie samenvatting</b> In het primair onderwijs, voortgezet onderwijs, MBO en hoger onderwijs wordt gewerkt aan bewustzijn van digitale risico's en maatregelen bij studenten, medewerkers en bestuurders door middel van campagnes, crisisoefening en speciale werkgroepen.</p>	<p><b>Tijdljn</b> 2022-2024</p>	<p><b>Eigenaar</b> OCW</p>
<p><b>Actie samenvatting</b> De instellingen in het hoger en middelbaar beroepsonderwijs gebruiken voor hun audits het NBA volwassenheidsmodel en afgeleid hiervan het Toetsingskader Informatiebeveiliging Hoger Onderwijs van SURF.</p>	<p><b>Tijdljn</b> 2022-2024</p>	<p><b>Eigenaar</b> OCW</p> <p><b>Betrokken</b> SURF</p>



## Digitale weerbaarheid zorginstellingen

<p><b>Actie samenvatting</b> Er wordt een herziene versie van de NEN 7510<sup>1</sup> gepubliceerd. Hierbij worden implementatietools ontwikkeld die bijdragen aan een verbeterde implementatiegraad van de NEN 7510.</p>	<p><b>Tijdslijn</b> 2025</p>	<p><b>Eigenaar</b> VWS</p> <p><b>Betrokken</b></p>
<p><b>Actie samenvatting</b> De Kwetsbaarheden Analyse Tool (KAT) is open-source beschikbaar gemaakt zodat alle zorgorganisaties dit kunnen gebruiken om actief te scannen op kwetsbaarheden in hun eigen systemen. VWS en Z-CERT stimuleren zorgorganisaties om dit structureel te doen. De tool wordt ook breder beschikbaar gesteld.</p>	<p><b>Tijdslijn</b> 2022-2023</p>	<p><b>Eigenaar</b> VWS</p> <p><b>Betrokken</b> Z-CERT</p>
<p><b>Actie samenvatting</b> De bijstand bij incidenten binnen de zorgsector wordt uitgebreid door gefaseerd nieuwe subsectoren aan te sluiten op dienstverlening van Z-CERT. Voor 2023 sluiten eerstelijnszorgsector, zoals huisartsen en apotheken aan. In de loop van 2023 en 2024 worden de volgende sectoren aangesloten: Gehandicaptenzorg, Verpleging, verzorging en thuiszorg en Revalidatiezorg.</p>	<p><b>Tijdslijn</b> 2023-2024</p>	<p><b>Eigenaar</b> VWS</p> <p><b>Betrokken</b> Z-CERT</p>
<p><b>Actie samenvatting</b> Het programma Informatieveilig gedrag in de zorg voorziet zorginstellingen van manieren om informatieveilig gedrag te bevorderen.</p>	<p><b>Tijdslijn</b> 2022-2023</p>	<p><b>Eigenaar</b> VWS</p> <p><b>Betrokken</b> ECP, Z-CERT</p>

<sup>1</sup> Een norm voor informatiebeveiliging voor de zorgsector in Nederland. Zorgaanbieders zijn op grond van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabv pz) verplicht om te voldoen aan de NEN-7510.

<p><b>Actie samenvatting</b> In het kader van preventie en detectie zal Z-CERT oefen- en testactiviteiten organiseren samen met aangesloten zorginstellingen en best practices ontwikkelen in relatie tot de vigerende, zorgsector specifieke, informatiebeveiligingsnorm NEN7510.</p>	<p><b>Tijdslijn</b> 2023</p>	<p><b>Eigenaar</b> VWS</p> <p><b>Betrokken</b> Z-CERT</p>
--	----------------------------------	---

## Digitale weerbaarheid sectoren infrastructuur en waterstaat

<p><b>Actie samenvatting</b> De versterking van de digitale weerbaarheid van sectoren waarvoor IenW een systeemverantwoordelijk heeft, zoals drinkwater, kerens en beheren, luchtvaart, maritiem, nucleair, spoorwegen en plaats- en tijdbepaling Global Navigation Satellite System (GNSS). Onder andere door:</p> <ul style="list-style-type: none"> <li>• Het organiseren van bestuurlijk overleg met sectoren om kennis en ervaring uit te wisselen en te bespreken op welke manier kan worden samengewerkt om digitale risico's te kunnen beheersen.</li> <li>• Ontwikkelen van sectorale kennisproducten zoals periodieke cybersecuritydreigingsbeelden per sector die o.a. bijdragen aan integraal risicomanagement; tegengaan van ransomware en inzicht in ketenrisico's.</li> <li>• Faciliteren van organisaties bij opleiding, testen, trainen en oefenen zodat zij beter in staat zijn snel te reageren op en te herstellen na een cyberincident, passend bij de behoefte van de sector.</li> </ul>	<p><b>Tijdslijn</b> 2022-2026</p>	<p><b>Eigenaar</b> IenW</p> <p><b>Betrokken</b> NCSC, AIVD, MIVD, CERT Watermanagement</p>
--	---------------------------------------	--

## Digitale weerbaarheid rijksoverheid

<p><b>Actie samenvatting</b></p> <p>De ambitie van BZK op dit onderwerp wordt uiteengezet in de I-strategie Rijk en de routekaarten, zoals die op 15 juli 2022 met de Kamer is gedeeld.<sup>2</sup> Voorbeelden van concrete acties zijn:</p> <ul style="list-style-type: none"> <li>• In 2022 wordt gestart met de projectaanpak 'redteaming' gericht op drie sporen: risicogericht testen, kennisdeling (binnen Rijksoverheid), opvolging van bevindingen.</li> <li>• Er komt een verplichte basistraining digitale weerbaarheid voor rijksoverheidsmedewerkers vanaf 2024.</li> <li>• Daarnaast wordt, met facilitering vanuit CIO-Rijk, parallel gewerkt aan beleid voor een aantal activiteiten: handreikingen bij het in augustus 2022 herziene rijksbrede cloudbeleid, aanpak risico's quantum computing, rijksbrede voorzieningen voor hoog gerubriceerde informatie, en versterken van het SOC-stelsel Rijk.</li> <li>• Het rijksbrede programma I-Partnerschap richt zich aanvullend aan dcypher op de samenwerking tussen de Rijksoverheid en hoger onderwijs op I-gebied, waaronder cybersecurity. Een van de onderdelen hiervan is het I-doctoraatsprogramma. Dit levert kenniswerkers en draagt met onderzoek en innovatie bij aan de versterking van de kennispositie en de digitale uitdagingen van het Rijk.</li> </ul>	<p><b>Tijdslijn</b></p> <p>2022-2025</p>	<p><b>Eigenaar</b></p> <p>BZK</p> <p><b>Betrokken</b></p> <p>NCSC, Rijks-CIO's, AIVD, MIVD</p>
--	--	--

## Digitale weerbaarheid overheid

<p><b>Actie samenvatting</b></p> <p>Er wordt een bestuurlijk convenant opgesteld met de VNG ten aanzien van digitale veiligheid waarin de gezamenlijke inzet op het gebied van cybersecurity voor gemeenten nader zal worden uitgewerkt.</p>	<p><b>Tijdslijn</b></p> <p>2022</p>	<p><b>Eigenaar</b></p> <p>BZK</p> <p><b>Betrokken</b></p> <p>VNG</p>
<p><b>Actie samenvatting</b></p> <p>In 2023 vindt de doorontwikkeling van en monitoring op de Baseline Informatiebeveiliging Overheid (BIO) plaats incl. de wettelijke verankering hiervan in de Wet Digitale Overheid.</p>	<p><b>Tijdslijn</b></p> <p>2023</p>	<p><b>Eigenaar</b></p> <p>BZK</p> <p><b>Betrokken</b></p>
<p><b>Actie samenvatting</b></p> <p>Het Centrum voor Informatiebeveiliging en Privacybescherming (CIP) verlengt en actualiseert de uitvoering van het ondersteuningsprogramma BIO voor de gehele overheid. Hiermee worden organisaties bijgestaan bij de implementatie en toepassing van de BIO.</p>	<p><b>Tijdslijn</b></p> <p>2022-2027</p>	<p><b>Eigenaar</b></p> <p>BZK</p> <p><b>Betrokken</b></p> <p>CIP</p>
<p><b>Actie samenvatting</b></p> <p>Het CIP verlengt en actualiseert de uitbreiding en doorontwikkeling van de service Informatiebeveiliging en Privacy. Overheden krijgen maatwerkadvies van professionals bij de overheid over digitale veiligheid en privacy. Organisaties met onvoldoende kennis op gebied van informatieveiligheid worden op deze manier laagdrempelig geholpen door organisaties met specifieke expertise.</p>	<p><b>Tijdslijn</b></p> <p>2022-2027</p>	<p><b>Eigenaar</b></p> <p>BZK</p> <p><b>Betrokken</b></p> <p>CIP</p>

<sup>2</sup> Kamerbrief routekaarten I-strategie Rijk 2022-2025 | Kamerstuk | Rijksoverheid.nl

<p><b>Actie samenvatting</b> Doorontwikkeling van verantwoordings-systematiek ENSIA (Eenduidige Normatief Single Information Audit). Door horizontaal en verticaal toezicht te organiseren met de BIO als basis werken gemeenten aan betere informatieveiligheid en wordt de democratische verantwoording over IB gefaciliteerd.</p>	<p><b>Tijdlijn</b> 2022-2025</p>	<p><b>Eigenaar</b> BZK</p> <p><b>Betrokken</b> VNG</p>
--	--------------------------------------	--

### Digitale weerbaarheid sectoren met operationele technologie- en procesautomatiseringssystemen

<p><b>Actie samenvatting</b> De aanpak om de beveiliging van Industrial Automation and Control Systems (IACS) te verhogen wordt versterkt door middel van een coalitie. Voorbeelden van acties binnen de coalitie zijn:</p> <ul style="list-style-type: none"> <li>• De ontwikkeling en implementatie van een (significante en realistische) IACS component in landelijke oefeningen, trainingen en opleidingen.</li> <li>• De versterking van kennisopbouw en de realisatie van instrumenten, bijvoorbeeld handreikingen en best practices om publieke en private organisaties te helpen om voor IACS de juiste maatregelen te implementeren en de juiste risico's te definiëren en aan te pakken.</li> <li>• Het delen van deze kennisproducten en instrumenten via een collectieve kennis hub IACS.</li> </ul>	<p><b>Tijdlijn</b> 2022-2024</p>	<p><b>Eigenaar</b> IenW</p> <p><b>Betrokken</b> NCSC, EZK, (private) partners</p>
---	--------------------------------------	---

### Zicht op digitale weerbaarheid van overheid en bedrijfsleven

<p><b>Actie samenvatting</b> Er worden pilots uitgevoerd waarbinnen de toegevoegde waarde van een IT-verslag en een IT-auditverklaring binnen de overheid wordt onderzocht. Vergelijkbaar met het gangbare financiële jaarverslag. De verkenning sluit aan op pilots uit het bedrijfsleven.</p>	<p><b>Tijdlijn</b> 2023</p>	<p><b>Eigenaar</b> BZK</p> <p><b>Betrokken</b> ADR</p>
<p><b>Actie samenvatting</b> Er wordt samen met het brede cybersecurityveld een monitoringssystematiek voor de digitale weerbaarheid van Nederland opgezet. Een eerste rapportage wordt 2024 verwacht.</p>	<p><b>Tijdlijn</b> 2024-2026</p>	<p><b>Eigenaar</b> JenV</p> <p><b>Betrokken</b> BZK, EZK, NCSC, DTC</p>
<p><b>Actie samenvatting</b> Het Centrum voor Informatiebeveiliging en Privacy (CIP) beheert en ontwikkelt de website basisbeveiliging.nl waarop op basis van verschillende indicatoren, scores op veiligheidsgebied van overheidsorganisaties worden gemeten en getoond.</p>	<p><b>Tijdlijn</b> 2023</p>	<p><b>Eigenaar</b> BZK</p> <p><b>Betrokken</b> CIP</p>
<p><b>Actie samenvatting</b> In het kader van de corporate governance code wordt met het bedrijfsleven overlegd op welke manier zij kunnen samenwerken voor het beheersen van cybersecurityrisico's bij beursgenoteerde bedrijven.</p>	<p><b>Tijdlijn</b> 2022</p>	<p><b>Eigenaar</b> EZK</p>
<p><b>Actie samenvatting</b> Met verzekeraars wordt verkend welke rol zij zouden kunnen spelen in het kader van gevolgschade van cyberincidenten.</p>	<p><b>Tijdlijn</b> 2022-2023</p>	<p><b>Eigenaar</b> JenV</p> <p><b>Betrokken</b> EZK, FIN</p>

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

#### Incident- en crisispreparatie

<p><b>Actie samenvatting</b> Het geactualiseerde Landelijk Crisisplan Digitaal (LCP-Digitaal) wordt gelanceerd en in gebruik genomen. Dit plan biedt de basis voor de digitale crisisaanpak.</p>	<p><b>Tijdslijn</b> 2022</p>	<p><b>Eigenaar</b> JenV</p> <p><b>Betrokken</b> NCP-partners</p>
<p><b>Actie samenvatting</b> Departementen zorgen voor aansluiting van departementale crisisplannen op het Landelijk Crisisplan Digitaal en kunnen aantonen dat incident-, continuïteit- en herstelplannen zijn getest, door middel van bijvoorbeeld een oefening of audit. Ook geven departementen opvolging aan (oefen)evaluaties en bevindingen.</p>	<p><b>Tijdslijn</b> 2022-2024</p>	<p><b>Eigenaar</b> JenV</p> <p><b>Betrokken</b> Departementen</p>
<p><b>Actie samenvatting</b> Als aanvulling op het LCP digitaal wordt onderzocht of het huidige wettelijke crisis instrumentarium (incl. noodwetgeving) voor ingrijpen bij nationale crises voldoende is voor nationale crises met digitale elementen. Hierbij zal ook aandacht zijn voor een verdringingsreeks.</p>	<p><b>Tijdslijn</b> 2022-2024</p>	<p><b>Eigenaar</b> JenV</p>
<p><b>Actie samenvatting</b> Relevante regionale crisisplannen worden aangesloten op het Landelijk Crisisplan Digitaal.</p>	<p><b>Tijdslijn</b> 2022-2023</p>	<p><b>Eigenaar</b> JenV</p> <p><b>Betrokken</b> Veiligheidsregio's</p>

<p><b>Actie samenvatting</b> Nederland neemt een actieve rol in de doorontwikkeling van internationale crisisnetwerken.</p>	<p><b>Tijdslijn</b> 2022-2026</p>	<p><b>Eigenaar</b> JenV</p> <p><b>Betrokken</b> DEF, BZ</p>
<p><b>Actie samenvatting</b> Doorontwikkeling van het Nationaal Response Netwerk (NRN) tot nationaal incident responsnetwerk. Onder andere door beschikbaar maken en houden van defensiecybercapaciteiten voor militaire bijstand en steunverlening. Verhogen inzet door het strategisch detacheren van cyberexperts tussen (Rijks)overheidsorganisaties. Uitbreiden publiek-private samenwerking. In kaart brengen beschikbare responscapaciteit.</p>	<p><b>Tijdslijn</b> 2022-2025</p>	<p><b>Eigenaar</b> JenV, DEF</p> <p><b>Betrokken</b> NRN partners</p>
<p><b>Actie samenvatting</b> Ontwikkeling van kennisproducten/ diensten om organisaties te adviseren over hun incidentresponsprocessen (factsheets, whitepapers, runbooks etc.).</p>	<p><b>Tijdslijn</b> 2022-2024</p>	<p><b>Eigenaar</b> JenV</p> <p><b>Betrokken</b> NCSC, DTC</p>
<p><b>Actie samenvatting</b> Inlichtingengebaseerde incidentcoördinatie vanuit de AIVD en MIVD wordt verder uitgebouwd, onder andere via samenwerking in de CIIC.</p>	<p><b>Tijdslijn</b> 2022-2026</p>	<p><b>Eigenaar</b> BZK, DEF,</p> <p><b>Betrokken</b> NCSC, CIIC</p>
<p><b>Actie samenvatting</b> Defensie investeert in personele en technische capaciteit in de gehele keten bij Defensie om het delen van informatie sneller en veiliger te laten plaatsvinden en de reactiesnelheid bij kwetsbaarheden en incidenten te verhogen. Voor verdere uitwerking, zie bijlage 2 van de Defensienota 2022.</p>	<p><b>Tijdslijn</b> 2023-2026</p>	<p><b>Eigenaar</b> DEF</p>

## Oefenen

<p><b>Actie samenvatting</b> Na de publicatie van de Rijksbrede Risicoanalyse en de Rijksbrede Veiligheidsstrategie zal een interdepartementale oefenagenda worden opgesteld, waarin ook de planning van cyber- en hybride-oefeningen wordt meegenomen.</p>	<p><b>Tijdslijn</b> 2023-2024</p>	<p><b>Eigenaar</b> JenV</p> <p><b>Betrokken</b> Alle departementen</p>
<p>De nationale oefening ISIDOOR wordt georganiseerd. De deelnemers worden in aanloop hiernaartoe gestimuleerd dat organisaties eigen plannen en procedures hebben vastgelegd en hun medewerkers hiervoor zijn opgeleid en getraind.</p>	<p><b>Tijdslijn</b> 2023</p>	<p><b>Eigenaar</b> JenV</p> <p><b>Betrokken</b> NCSC, politie, AIVD, MIVD en private partners.</p>
<p><b>Actie samenvatting</b> Als aanvulling op ISIDOOR worden diverse sectorale en lokale oefeningen georganiseerd. Voorbeelden hiervan zijn het symposium met crisissimulatie dat VWS organiseert voor ongeveer 200 deelnemers uit alle lagen van de zorgsector; het jaarlijks georganiseerde overheidsbrede cyberprogramma waarvan oefeningen deel uitmaken en lokale oefeningen, zoals 'Hack the Hague'.</p>	<p><b>Tijdslijn</b> 2022-2026</p>	<p><b>Eigenaar</b> JenV</p> <p><b>Betrokken</b> Departementen, overheden, operationele partners en private partners.</p>
<p><b>Actie samenvatting</b> Jaarlijks oefenen overheden (Rijksoverheid, provincies, gemeenten en waterschappen) aan de hand van een gesimuleerde hackaanval. Tevens zijn er gedurende het gehele jaar Webinars waarbij organisaties binnen en buiten de overheid kennis delen.</p>	<p><b>Tijdslijn</b> 2022-2026</p>	<p><b>Eigenaar</b> BZK</p> <p><b>Betrokken</b> Medeoverheden</p>

<p><b>Actie samenvatting</b> Defensie gaat frequenter cyberoefeningen organiseren, waarbij ook de verbinding wordt gezocht met nationale en internationale partners.</p>	<p><b>Tijdslijn</b> 2022-2026</p>	<p><b>Eigenaar</b> DEF</p>
<p><b>Actie samenvatting</b> Nederland doet mee aan internationale NAVO- en EU-oefeningen, waaronder edities van PACE, CMX en BlueOLEx, en streeft naar een intensievere jaarlijkse deelname.</p>	<p><b>Tijdslijn</b> 2022-2026</p>	<p><b>Eigenaar</b> JenV, DEF</p> <p><b>Betrokken</b> AIVD, MIVD, NCSC</p>

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. Ruim 60.000 poortjes en kaartlezers moeten worden omgebouwd.



## Pijler II

Veilige en innovatieve digitale producten en diensten

### Doel 1: Digitale producten en diensten zijn veiliger.

#### Europese wetgeving voor digitale producten en diensten

##### Actie samenvatting

Het kabinet maakt zich in de onderhandelingen voor de Europese Cyber Resilience Act (CRA) hard voor opname van een zorgplicht voor fabrikanten en leveranciers van alle ICT-producten, diensten en processen, inclusief bijbehorende standaarden en toezicht. Deze zorgplicht moet gedurende de hele levenscyclus blijven gelden.

Tijdslijn  
2022-2024

Eigenaar  
EZK

##### Betrokken

JenV, BZK, private partners

##### Actie samenvatting

Het kabinet zet zich in om de samenhang tussen regelgeving voor producten en diensten te bevorderen onder meer door in te zetten op goede aansluiting van de CRA op sector specifieke cybersecurity-eisen in Europese regelgeving (zoals voor medische hulpmiddelen en auto's) en generieke wetgeving zoals de Richtlijn voor Algemene Productveiligheid en de Richtlijn voor aansprakelijkheid voor producten met gebreken.

Tijdslijn  
2022-2024

Eigenaar  
EZK

##### Betrokken

JenV, VWS, IenW, private partners

##### Actie samenvatting

Het kabinet draagt samen met private partijen via het Nederlandse normalisatie-instituut NEN bij aan de totstandkoming van Europese geharmoniseerde normen voor cybersecurity-eisen onder de Richtlijn Radioapparatuur.

Tijdslijn  
2022-2024

Eigenaar  
EZK

##### Betrokken

NEN, private partners

## Toezicht en handhaving op digitale producten en diensten

<p><b>Actie samenvatting</b> Consumenten en ondernemers worden 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.</p>	<p><b>Tijdljn</b> 2022-2026</p>	<p><b>Eigenaar</b> EZK</p> <p><b>Betrokken</b> ACM</p>
<p><b>Actie samenvatting</b> Agentschap Telecom versterkt haar toezicht op de cybersecurity markttoegangseisen voor draadloos verbonden apparaten onder de Radio Equipment Directive onder meer door onderzoeken via het Internet of Things Testlab en versterking van capaciteit.</p>	<p><b>Tijdljn</b> 2022-2024</p>	<p><b>Eigenaar</b> EZK</p> <p><b>Betrokken</b> AT</p>
<p><b>Actie samenvatting</b> Agentschap Telecom houdt in Nederland als Nationale Cybersecurity Certificeringsautoriteit (NCCA) toezicht op de certificeringschema's in Nederland en autoriseert de uitgifte van certificaten met het certificeringsniveau 'hoog'. Daarbij werkt zij samen met het Nationaal Bureau Verbindingsbeveiliging van de AIVD.</p>	<p><b>Tijdljn</b> 2022-2026</p>	<p><b>Eigenaar</b> EZK</p> <p><b>Betrokken</b> AT, AIVD</p>
<p><b>Actie samenvatting</b> Autoriteit Consument en Markt houdt toezicht op de verkopers van producten die verplicht zijn informatie te geven aan consumenten over hoe lang (veiligheids)updates beschikbaar zijn.</p>	<p><b>Tijdljn</b> 2022-2024</p>	<p><b>Eigenaar</b> EZK</p> <p><b>Betrokken</b> ACM</p>

<p><b>Actie samenvatting</b> Agentschap Telecom en de Autoriteit Consument en Markt gaan intensiever samenwerken om handhaving en toezicht op het gebied van veilige producten en diensten te verbeteren onder meer door het opstellen van een gezamenlijke oefenagenda.</p>	<p><b>Tijdljn</b> 2022-2024</p>	<p><b>Eigenaar</b> EZK</p> <p><b>Betrokken</b> AT, ACM</p>
--	-------------------------------------	--

## Certificering en standaarden

<p><b>Actie samenvatting</b> Het kabinet draagt in samenwerking met private partijen bij aan de ontwikkeling en adoptie van Europese cybersecurity certificeringschema's voor ICT-producten, diensten en processen, zoals voor clouddiensten, 5G technologie en <i>Common Criteria</i>.</p>	<p><b>Tijdljn</b> 2023</p>	<p><b>Eigenaar</b> EZK</p> <p><b>Betrokken</b> BZK, JenV, private partijen</p>
<p><b>Actie samenvatting</b> Het kabinet zet in op de ontwikkeling van Europese certificeringschema's voor veilige software en cybersecurity diensten.</p>	<p><b>Tijdljn</b> 2022-2026</p>	<p><b>Eigenaar</b> EZK</p> <p><b>Betrokken</b> JenV, BZK, private partijen</p>
<p><b>Actie samenvatting</b> EZK stimuleert de bewustwording en implementatie van certificeringsschema's onder de Cyber Security Act.</p>	<p><b>Tijdljn</b> 2022-2026</p>	<p><b>Eigenaar</b> EZK</p> <p><b>Betrokken</b> AT</p>

<p><b>Actie samenvatting</b> De Baseline Security Product Assessment wordt doorontwikkeld, zodat het overeenkomt met vergelijkbare Europese evaluatiestandaarden om uitwisselbaarheid van (veilige) Europese producten te bevorderen. Daarnaast werkt de AIVD samen met Agentschap Telecom aan een transitie van het op common criteria gebaseerde nationale schema NSCIB naar het Europese schema zodra de Cyber Security Act in werking treedt.</p>	<p><b>Tijdslijn</b> 2022-2023</p>	<p><b>Eigenaar</b> BZK</p> <p><b>Betrokken</b> AIVD, EZK</p>
<p><b>Actie samenvatting</b> Het kabinet stimuleert contacten met gelijkgezinde derde landen over aansluiting van internationale standaarden op Europese standaarden en omgekeerd de ontwikkeling van vergelijkbare wet- en regelgeving en standaarden in die landen.</p>	<p><b>Tijdslijn</b> 2022-2026</p>	<p><b>Eigenaar</b> EZK</p> <p><b>Betrokken</b> JenV, BZ, private partijen</p>
<p><b>Actie samenvatting</b> Er wordt verkend hoe organisaties beter in staat kunnen worden gesteld om duidelijke afspraken te maken over cybersecurity met hun afnemers middels onderzoek naar de contractrechtpraktijk en best practices in business-to-business relaties tussen aanbieders van ICT-producten en -diensten en afnemers.</p>	<p><b>Tijdslijn</b> 2023</p>	<p><b>Eigenaar</b> EZK</p> <p><b>Betrokken</b> DTC, private partijen</p>

## Algemene beveiligingseisen rijksoverheid (ABRO) en overheidsinkoopbeleid

<p><b>Actie samenvatting</b> Er worden Algemene Beveiligingseisen opgesteld voor de Rijksoverheid (ABRO), op basis van doorontwikkeling van het bestaande regime Algemene beveiligingseisen Defensieopdrachten (ABDO), waaraan bedrijven die gevoelige en/of gerubriceerde overheidsopdrachten vervullen moeten voldoen.</p>	<p><b>Tijdslijn</b> 2022-2023</p>	<p><b>Eigenaar</b> BZK</p> <p><b>Betrokken</b> DEF, JenV AIVD, MIVD</p>
<p><b>Actie samenvatting</b> De tool inkoopseisen cybersecurity overheid (ICO) wordt doorontwikkeld, verbreed en geïmplementeerd. Inclusief verdere ontwikkeling van overheidsbrede eisensets. Dit zal indirect de markt positief beïnvloeden om veilige producten en diensten te leveren</p>	<p><b>Tijdslijn</b> 2022-2023</p>	<p><b>Eigenaar</b> BZK</p> <p><b>Betrokken</b> CIP, EZK, medeoverheden</p>
<p><b>Actie samenvatting</b> BZK voert samen met de VNG een verkenning uit naar wat er nodig is om het leveranciersmanagement voor medeoverheden naar een hoger niveau te brengen met aandacht voor integreren van dienstverlening in de inkoopondersteuning en het organiseren van effectief toezicht op leveranciers.</p>	<p><b>Tijdslijn</b> 2022-2023</p>	<p><b>Eigenaar</b> BZK</p> <p><b>Betrokken</b> CIP, EZK, medeoverheden</p>
<p><b>Actie samenvatting</b> Het Centrum voor Informatiebeveiliging en Privacy (CIP) ontwikkelt een pakket aan cybersecurity-eisen en een tool die overheidsorganisaties ondersteunt bij de inkoop van ICT-producten en -diensten. Deze tool wordt verder ontwikkeld en de toepassing wordt bij de overheid gestimuleerd. Tevens zal middels wetgeving worden geborgd dat de normensets voor veilig inkopen ook verplicht worden toegepast door overheden.</p>	<p><b>Tijdslijn</b> 2022-2026</p>	<p><b>Eigenaar</b> EZK, BZK</p> <p><b>Betrokken</b> medeoverheden</p>



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

### Veilige cryptografie

<p><b>Actie samenvatting</b> De productontwikkeling voor high assurance producten wordt gestimuleerd middels versterkt en eensgezind opdrachtgeverschap vanuit de Rijksoverheid, zodat Nederland de beschikking houdt over betrouwbare cryptografische oplossingen. Dat gebeurt in nauwe samenwerking met de Nederlandse cryptografische-industrie.</p>	<p><b>Tijdslijn</b> 2022-2026</p>	<p><b>Eigenaar</b> BZK</p> <p><b>Betrokken</b> AIVD, JenV, DEF, EZK, OCW, lenW, privaat, kennisinstellingen.</p>
<p><b>Actie samenvatting</b> In samenwerking met bedrijven en wetenschappelijke instellingen wordt onderzoek uitgevoerd naar de ontwikkeling van moderne en hoogwaardige beveiligingsproducten.</p>	<p><b>Tijdslijn</b> 2022-2026</p>	<p><b>Eigenaar</b> BZK</p> <p><b>Betrokken</b> AIVD, JenV, DEF, EZK, OCW, lenW, private partijen, kennisinstellingen.</p>
<p><b>Actie samenvatting</b> Het kabinet zet meerjarige thematische routekaarten op aan de hand waarvan onderzoek wordt uitgevoerd of uitgezet middels het platform dcypher. Dit is inclusief een routekaart op cryptocommunicatie en voor geautomatiseerd kwetsbaarhedenonderzoek.</p>	<p><b>Tijdslijn</b> 2022-2026</p>	<p><b>Eigenaar</b> EZK</p> <p><b>Betrokken</b> JenV, BZK, DEF, OCW, lenW, private partijen, kennisinstellingen.</p>

### Nationale samenwerking kennis- en innovatie-onderzoekssamenwerking

<p><b>Actie samenvatting</b> De interdepartementale cybersecurity kennis- en innovatiebehoefte wordt jaarlijks geïnventariseerd en inzichtelijk gemaakt. Indien nodig wordt hierbinnen geprioriteerd.</p>	<p><b>Tijdslijn</b> 2022-2026</p>	<p><b>Eigenaar</b> EZK</p> <p><b>Betrokken</b> BZK, JenV, OCW, DEF, lenW</p>
<p><b>Actie samenvatting</b> Defensie versterkt de <i>Cyber Innovation Hub</i> (CIH) om het innovatieportfolio uit te breiden en de landelijke positie in cybersecurity kennis- en innovatienetwerken te versterken.</p>	<p><b>Tijdslijn</b> 2022-2024</p>	<p><b>Eigenaar</b> DEF</p> <p><b>Betrokken</b></p>
<p><b>Actie samenvatting</b> NCSC voert onderzoeksactiviteiten uit onder een meerjarige agenda in samenwerking met diverse (kennis)instellingen op diverse domeinen gerelateerd aan de rol van het NCSC en haar doelgroep(en).</p>	<p><b>Tijdslijn</b> 2022-2026</p>	<p><b>Eigenaar</b> JenV</p> <p><b>Betrokken</b> NCSC</p>
<p><b>Actie samenvatting</b> De cybersecurity kennis-en innovatiebehoefte van het bedrijfsleven en kennisinstellingen wordt onderdeel van het Nederlandse Topsectoren Programma.</p>	<p><b>Tijdslijn</b> 2022-2026</p>	<p><b>Eigenaar</b> EZK</p> <p><b>Betrokken</b> Private partijen</p>

## Europese onderzoekssamenwerking en fondsen

<p><b>Actie samenvatting</b> Bij de RVO wordt een Nationaal Coördinatie Centrum (NCC-NL) opgericht als onderdeel van het Europese Netwerk van Cyber Competence Centers (ECCCN).</p>	<p><b>Tijdslijn</b> 2022-2026</p>	<p><b>Eigenaar</b> EZK</p> <p><b>Betrokken</b> BZK, DEF, JenV, OCW, IenW</p>
<p><b>Actie samenvatting</b> Organisaties uit het dcypher-netwerk worden ondersteund via het Nationaal Coördinatie Centrum (NCC-NL) in de voorbereiding en uitvoering van projecten uit Europese initiatieven en fondsen zoals Digital Europe en Horizon 2020.</p>	<p><b>Tijdslijn</b> 2022-2026</p>	<p><b>Eigenaar</b> EZK</p>
<p><b>Actie samenvatting</b> Er wordt actief gestuurd op het opnemen van de onderzoeksbehoeften van Nederlandse organisaties in nieuwe werkprogramma's van onder andere Digital Europe en Horizon 2020, hierbij gebruik makend van Nederlandse cybersecurity expertise en innovatiekracht.</p>	<p><b>Tijdslijn</b> 2022-2026</p>	<p><b>Eigenaar</b> EZK</p> <p><b>Betrokken</b> OCW, JenV, BZK, DEF, IenW</p>



## Pijler III

### Tegengaan van digitale dreigingen van staten en criminelen

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.



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

### Zicht op statelijke actoren

<p><b>Actie samenvatting</b> De onderzoekscapaciteit wordt versterkt ten behoeve van inlichtingenmatig-diepteonderzoek waarmee breder zicht ontstaat op de huidige en voorstelbare digitale dreiging.</p>	<p><b>Tijdljn</b> 2022-2026</p>	<p><b>Eigenaar</b> BZK, DEF</p> <p><b>Betrokken</b> AIVD, MIVD</p>
<p><b>Actie samenvatting</b> De unieke inlichtingen worden vertaald naar specifiek handelingsperspectief waarmee afnemers zich beter kunnen weren.</p>	<p><b>Tijdljn</b> 2022-2026</p>	<p><b>Eigenaar</b> BZK, DEF</p> <p><b>Betrokken</b> AIVD, MIVD</p>
<p><b>Actie samenvatting</b> De mogelijkheden tot effectieve inzet van de bijzondere bevoegdheden voor onderzoeken naar landen met een offensief cyberprogramma worden vergroot. Hiertoe wordt een wetsvoorstel ingediend bij Tweede Kamer.</p>	<p><b>Tijdljn</b> 2022-2026</p>	<p><b>Eigenaar</b> BZK, DEF</p> <p><b>Betrokken</b> AIVD, MIVD</p>

## Onderzoeks- en opsporingscapaciteit cybercriminelen

Actie samenvatting Politie en OM zetten, naast strafrechtelijke interventies, met lokaal bestuur en private partners in op het ontwikkelen van niet-strafrechtelijke interventies ter bestrijding van cybercrime, waaronder ransomware.	Tijdelijk 2023-2026	Eigenaar JenV  Betrokken Politie, OM, BZK, medeoverheden, BZ
Actie samenvatting Er wordt ingezet op het vergroten van kennis en kunde van cybersecurityfenomenen binnen het OM.	Tijdelijk 2022-2026	Eigenaar JenV  Betrokken OM
Actie samenvatting De KMar en de politie verkennen de mogelijkheden tot verdere samenwerking op het bestrijden van (grensoverschrijdende) cybercriminaliteit.	Tijdelijk 2022-2024	Eigenaar JenV, DEF  Betrokken KMar, politie
Actie samenvatting Het OM voert een verkenning uit naar de mogelijkheid om middels een 'fasttrack' cyberzaken versneld af te doen.	Tijdelijk 2022-2026	Eigenaar JenV  Betrokken OM
Actie samenvatting De politie stelt jaarlijks een veiligheidsbeeld over cybercrime en gedigitaliseerde criminaliteit op, waarin de belangrijkste criminele fenomenen, werkwijzen en het risico hiervan voor de samenleving geschetst worden. De beelden geven richting aan de keuze van de politie en het OM voor de fenomenen waarop wordt ingezet en de onderzoeken die worden geprioriteerd.	Tijdelijk 2022-2026	Eigenaar JenV  Betrokken Politie, OM

## Versterken diplomatiek netwerk

Actie samenvatting Het aantal cyberdiplomaten en hun taken worden uitgebreid ten behoeve van een versterkte informatiepositie over digitale dreigingen en ontwikkelingen middels gerichte en proactieve rapportages op basis van diplomatieke contacten in derde landen.	Tijdelijk 2022-2026	Eigenaar BZ  Betrokken DEF, BZK, JenV
Actie samenvatting Versterken van cybercompetentie en -kennis binnen het postennetwerk om cybersecurity beter te integreren in regulier diplomatiek contact en in aanpalende beleidsthema's.	Tijdelijk 2022-2026	Eigenaar BZ  Betrokken DEF, BZK, JenV
Actie samenvatting BZ stimuleert in EU- en NAVO-verband betere internationale informatiedeling en gezamenlijke analyse en initieert waar nodig kleinere coalities om het situationeel beeld van digitale dreigingen te versterken.	Tijdelijk 2022-2026	Eigenaar BZ  Betrokken DEF, BZK, JenV, NCSC
Actie samenvatting Het NCSC start met de uitvoering van het capaciteitsopbouwprogramma internationaal o.a. door het ontwerp van trainingsactiviteiten.	Tijdelijk 2022-2024	Eigenaar JenV  Betrokken BZ, NCSC
Actie samenvatting Deelnemen van Defensie aan initiatieven 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. Internationaal oefenen wordt de norm.	Tijdelijk 2022-2026	Eigenaar DEF  Betrokken BZ

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

### Attributie en respons

<p><b>Actie samenvatting</b> Samen met internationale partners worden nieuwe en effectievere opties voor diplomatieke respons op cyberdreigingen ontwikkeld. Bestaande kaders en instrumenten, zoals het interdepartementale diplomatiek responskader bij cyberincidenten, de <i>EU Cyber Diplomacy Toolbox</i> en de <i>NATO Guide</i> worden doorontwikkeld. Dit vindt plaats in samenhang met het Rijksbreed Responskader voor Statelijke Dreigingen.</p>	<p>Tijdelijk 2022-2026</p>	<p>Eigenaar BZ</p> <p>Betrokken DEF, BZK, JenV, AIVD, MIVD, NCSC</p>
<p><b>Actie samenvatting</b> Nederland neemt het initiatief voor kleinere landcoalities om specifieke incidenten of dreigingen te adresseren en beleidsvorming binnen de EU en NAVO op het gebied van (diplomatieke) respons en attributie te stimuleren.</p>	<p>Tijdelijk 2022-2026</p>	<p>Eigenaar BZ</p> <p>Betrokken DEF, BZK, JenV, NCSC</p>

### Defensieve en offensieve cybercapaciteiten

<p><b>Actie samenvatting</b> Defensie investeert in zijn gehele keten van cybercapaciteiten, onder meer via het structureel borgen en vergroten van <i>Cyber Rapid Response Teams</i> (CRRT's) en <i>Cyber Mission Teams</i> (CMT's) en het vergroten van de personele gereedheid via opleiding, training en oefening.</p>	<p>Tijdelijk 2022-2026</p>	<p>Eigenaar DEF</p> <p>Betrokken BZ</p>
<p><b>Actie samenvatting</b> Defensie breidt bijstandsconstructies uit om andere organisaties te kunnen helpen bij grootschalige incidenten. Onder andere via het Nationaal Response Netwerk (NRN).</p>	<p>Tijdelijk 2022-2026</p>	<p>Eigenaar DEF</p> <p>Betrokken JenV</p>
<p><b>Actie samenvatting</b> Verkenning naar de mogelijkheden, en implementatie van actieve cyberverdedigingsmaatregelen in het kader van implementatie van NIBz en het (tijdelijk) laten blokkeren van malafide verkeer door Nederlandse Internet Service Providers met de benodigde juridische waarborgen in het kader van nationale risicomitigatie, tegengaan van meer slachtoffers en dreiging te verminderen.</p>	<p>Tijdelijk 2023-2024</p>	<p>Eigenaar JenV</p> <p>Betrokken EZK, BZK, DEF, NCSC, AIVD, MIVD, BZ</p>

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

#### Normatief kader

<p><b>Actie samenvatting</b> Het VN normatief kader in cyberspace wordt verstevigd en bestendigd binnen onderhandelingen in multilaterale fora middels effectieve inzet op Nederlandse prioriteiten, waaronder bescherming van de kernfunctionaliteit van het internet en het multi-stakeholdermodel voor het beheer van het internet.</p>	<p>Tijdelijk 2022-2026</p>	<p>Eigenaar BZ</p> <p>Betrokken DEF, EZK, JenV, BZK</p>
<p><b>Actie samenvatting</b> De naleving en uitvoering van het VN normatief kader wordt bevorderd door bij te dragen aan de totstandkoming van het Program of Action als implementatiemechanisme. Het kabinet is transparant over de implementatie van het normatief kader in Nederland.</p>	<p>Tijdelijk 2022-2026</p>	<p>Eigenaar BZ</p> <p>Betrokken DEF, JenV, EZK, BZK</p>

#### Internet governance

<p><b>Actie samenvatting</b> Deelname van de Nederlandse multi-stakeholdergemeenschap aan het internationale debat wordt bevorderd (incl. een vergelijkbare inzet van de EU voor de Europese multi-stakeholdergemeenschap) om met een sterker geluid een open, vrij en veilig internet te bepleiten.</p>	<p>Tijdelijk 2022-2026</p>	<p>Eigenaar EZK</p> <p>Betrokken BZ</p>
<p><b>Actie samenvatting</b> Er vindt actieve deelname plaats aan de internationale discussies over technische internetstandaarden en andere technische standaarden die van invloed zijn op de openheid, vrijheid en veiligheid van het internet door standpunten te coördineren op EU-niveau en met gelijkgezinde landen.</p>	<p>Tijdelijk 2022-2026</p>	<p>Eigenaar EZK</p> <p>Betrokken BZ</p>
<p><b>Actie samenvatting</b> Multistakeholder organisaties dienen effectiever te worden in het erkennen en adresseren van maatschappelijke en technische uitdagingen met betrekking tot internet governance. Zodat sneller tot een consensus of beslissing gekomen wordt ten aanzien van oplossingen van deze uitdagingen. Het kabinet wil dit bevorderen door zelf actief deel te nemen aan de discussie, gelijkgestemde landen stimuleren hun presentie te vergroten en door de uitkomsten van de discussies binnen ICANN in het Internet Governance Forum en de EU te agenderen.</p>	<p>Tijdelijk 2022-2026</p>	<p>Eigenaar EZK</p> <p>Betrokken BZ</p>

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

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

#### Voorlichtingscampagnes

<p><b>Actie samenvatting</b> JenV, EZK, BZK organiseren doelgroep-specifieke voorlichtingscampagne-programma's cyberveiligheid gericht op de cybersecurity basismaatregelen. Er vindt een effectmeting plaats na elke campagne. De campagnes worden georganiseerd in samenwerking met gemeenten voor optimale inzet van de beschikbare gemeentelijke communicatiekanalen.</p>	<p><b>Tijdslijn</b> 2022-2026</p>	<p><b>Eigenaar</b> JenV, EZK, BZK</p> <p><b>Betrokken</b> Medeoverheden</p>
<p><b>Actie samenvatting</b> In het kader van de City Deal Cybercrime<sup>3</sup> worden pilotprojecten uitgevoerd met als doel de weerbaarheid van burgers en bedrijven tegen cybercrime te vergroten. De pilots zijn gericht op meer integraliteit om lokale best practices beter en breder te benutten zodat kan worden toegewerkt naar een landelijk dekkend ondersteuningsaanbod.</p>	<p><b>Tijdslijn</b> 2022- 2023</p>	<p><b>Eigenaar</b> BZK, JenV</p> <p><b>Betrokken</b> Medeoverheden</p>
<p><b>Actie samenvatting</b> De jaarlijkse cybersecurity bewustwordingsmaand Alert Online met het partnernetwerk wordt structureel georganiseerd in oktober.</p>	<p><b>Tijdslijn</b> 2022</p>	<p><b>Eigenaar</b> EZK, JenV</p> <p><b>Betrokken</b> BZK</p>

<sup>3</sup> Samenwerking tussen J&V en gemeenten op het gebied van cybercrime.

## Beveiligingsadvies burgers

<p>Actie samenvatting</p> <p>De Informatiepunten Digitale Overheid worden gefaciliteerd om hulpvragen van burgers op het terrein van cyberveiligheid te beantwoorden en waar nodig door te verwijzen naar bestaande steunpunten, informatieloketten en lokale ondersteuningsinitiatieven van private partners.</p>	Tijdelijk 2022	Eigenaar BZK  Betrokken
<p>Actie samenvatting</p> <p>Het publiek-private veiliginternetten.nl wordt doorontwikkeld en verbreed als de centrale vindplaats voor cybersecurity-informatie en handelingsperspectief voor burgers.</p>	Tijdelijk 2022-2023	Eigenaar EZK  Betrokken BZK
<p>Actie samenvatting</p> <p>Het cyberweerbericht wordt periodiek opgesteld en gepubliceerd. Na twee jaar vindt een effectiviteitsevaluatie plaats.</p>	Tijdelijk 2022-2024	Eigenaar JenV  Betrokken EZK

## Betrouwbaarheid digitale overheidsvoorzieningen

<p>Actie samenvatting</p> <p>De overheid zet in op een uniforme domeinnaamextensie, zodat burgers gemakkelijk kunnen herkennen of zij online echt te maken hebben met een overheid of niet. Dit helpt online fraude als phishing tegen te gaan.</p>	Tijdelijk 2022-2026	Eigenaar BZK
<p>Actie samenvatting</p> <p>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. Bij onduidelijkheden over de echtheid van websites kunnen burgers terecht bij een contactpunt.</p>	Tijdelijk 2022-2023	Eigenaar BZK

## Doel 2: Burgers reageren snel en adequaat op cyberincidenten.

<p>Actie samenvatting</p> <p>De politie maakt vanaf 2023 voor meer cybercrime fenomenen het mogelijk om online melding of aangifte te doen.</p>	Tijdelijk 2023	Eigenaar JenV  Betrokken Politie
---	-------------------	--



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

#### Curriculum

<p><b>Actie samenvatting</b> Stichting Leerplan Ontwikkeling (SLO) heeft de opdracht gekregen om samen met het onderwijsveld concrete kerndoelen voor de basisvaardigheden te ontwikkelen waarvan digitale veiligheid deel uitmaakt. Deze opdracht voeren ze uit voor zowel het PO als het VO. De aangescherpte kerndoelen voor het PO en het VO in 2025 in een wetsvoorstel aan de Tweede Kamer voorgelegd.</p>	<p>Tijdlijn 2022-2025</p>	<p>Eigenaar OCW</p>
<p><b>Actie samenvatting</b> Het 'masterplan basisvaardigheden' wordt opgezet dat ervoor moet zorgen dat de leraar goed toegerust is om het beste onderwijs te geven in taal, rekenen/wiskunde, burgerschap en digitale geletterdheid. Met de ingang van het schooljaar 2022-2023 zullen de eerste scholen hiermee beginnen.</p>	<p>Tijdlijn 2022-2026</p>	<p>Eigenaar OCW</p>

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

#### Cybersecurity arbeidsmarkt

<p><b>Actie samenvatting</b> Onderwijsinstellingen werken aan bij- en omscholingsprogramma's om de cybersecurity-expertise van werknemers te vergroten. Daartoe werken zij samen met het bedrijfsleven en andere relevante partijen. Hierbij worden o.a. knelpunten en beperkingen in die samenwerking voortvloeiend uit regelgeving geïnventariseerd en gezien welke oplossingen daarvoor nodig zijn.</p>	<p>Tijdlijn 2022-2026</p>	<p>Eigenaar OCW</p> <p>Betrokken OCW, onderwijsinstellingen en werkgevers</p>
<p><b>Actie samenvatting</b> Er wordt geïnvesteerd in hbo-opleidingen in de bètatechniek, waar cybersecurityopleidingen ook onderdeel van zijn. Middelen worden ingezet op (1) hogere instroom binnen de opleiding, (2) lagere uitval en switch, (3) hogere zijinstroom, (4) inductie/warme overgang van opleiding naar arbeidsmarkt. Het doel van deze maatregel is om de arbeidsmarkttekorten in te perken.</p>	<p>Tijdlijn 2023-2029</p>	<p>Eigenaar OCW</p> <p>Betrokken Hogescholen</p>

<p><b>Actie samenvatting</b> Afhankelijk van definitief advies van een onafhankelijke commissie waarover eind september/begin oktober 2022 uitsluitel zal komen, wordt voor een aantal specifieke onderwerpen in het WO vanuit de sectorplannen geïnvesteerd in cybersecurity. Het doel van deze middelen is om samenwerking te stimuleren. Universiteiten maken per sector/domein een analyse waarin zij de kansen en knelpunten op gebied van onderzoek en onderwijs in kaart brengen, en voorstellen doen voor maatregelen om hierop in te spelen. In het ingediende sectorplan Techniek wordt ook aandacht besteed aan cybersecurity. Via deze weg zullen ook de universitaire cybersecurity opleidingen profiteren.</p>	<p>Tijdlijn 2023-2026</p>	<p>Eigenaar OCW</p> <p>Betrokken Universiteiten</p>
<p><b>Actie samenvatting</b> De kwalitatieve en kwantitatieve tekorten op de cybersecurity arbeidsmarkt worden onderzocht, inclusief aanbevelingen hoe deze tekorten aan te pakken.</p>	<p>Tijdlijn 2023</p>	<p>Eigenaar EZK</p> <p>Betrokken OCW, JenV, werkgevers, CBS, Universitaire Commissie voor Wetenschapsbeoefening.</p>
<p><b>Actie samenvatting</b> Verkend wordt of de initiatieven voor inzicht in ICT- brede tekorten en de ontwikkeling van een onderwijs en arbeidsmarktdashboard ICT ook voldoende inzicht bieden in regionale tekorten van cybersecurity specialisten.</p>	<p>Tijdlijn 2023-2024</p>	<p>Eigenaar EZK</p> <p>Betrokken OCW, SZW, BZK</p>

<p><b>Actie samenvatting</b> Het kabinet zet zich via de <i>Human Capital Agenda ICT</i> in om de instroom van cybersecurityspecialisten/ICT-specialisten te vergroten en de kwaliteit van de instroom te beïnvloeden. Dit wordt in nauwe samenwerking met het bedrijfsleven, regionale en lokale overheidsinstellingen en onderwijsinstellingen opgepakt.</p>	<p>Tijdlijn 2022-2026</p>	<p>Eigenaar EZK</p> <p>Betrokken</p>
<p><b>Actie samenvatting</b> Via thematische routekaarten en communities worden gesprekken gefaciliteerd tussen kennisinstellingen en het bedrijfsleven met betrekking tot de high-end kennisontwikkeling die nodig is om innovatieve productontwikkeling tot stand te brengen.</p>	<p>Tijdlijn 2022-2026</p>	<p>Eigenaar EZK</p> <p>Betrokken Dcypher</p>

Oktober 2022

Deze publicatie is een uitgave van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) namens de Rijksoverheid.  
[info@nctv.minjenv.nl](mailto:info@nctv.minjenv.nl)