Bijlage 1 Overzicht van preventieactiviteiten cybercrime

Onderstaand overzicht biedt inzicht in de verschillende preventieactiviteiten door de ministeries van Justitie en Veiligheid (JenV), Binnenlandse Zaken en Koninkrijksrelaties (BZK), en Economische Zaken (EZ) die zich concentreren op drie typen maatregelen: (potentiële) slachtoffers weerbaarder maken door hun basisveiligheid te vergroten (slachtofferpreventie), de daderpopulatie verkleinen door middel van gerichte interventies om daderschap te ontmoedigen en recidive te beperken (daderpreventie), en systemen en producten waar burgers en bedrijven gebruik van maken veiliger maken (situationele preventie).

Slachtofferpreventie

Vergroten van de basisweerbaarheid van burgers

Het vergroten van de digitale weerbaarheid van burgers door middel van het vergroten van hun basisweerbaarheid is noodzakelijk om de kans op slachtofferschap van cybercriminaliteit te verlagen. Het gaat hierbij specifiek om het informeren van burgers over vormen van cybercriminaliteit en het bieden van concrete handelingsperspectieven zoals toelichting over het treffen van basismaatregelen.

Nationale cursus digitale weerbaarheid

Het ministerie van BZK heeft financiële middelen beschikbaar gesteld voor de totstandkoming van de Nationale Cursus Digitale Weerbaarheid. De gratis online cursus is gericht op het vergroten van de digitale weerbaarheid van Nederlanders vanaf 12 jaar, zodat zij zich beter kunnen beschermen tegen digitale dreigingen, zoals phishing, online oplichting, desinformatie, hacken en sexting. Inmiddels zijn al meer dan 29.000 mensen gestart met de Nationale Cursus Digitale Weerbaarheid.

Campagne 'Laat je niet interneppen'

In 2023 is de campagne 'Laat je niet interneppen' in samenwerking tussen de ministeries van JenV en BZK gestart om mensen te waarschuwen voor het gebruik van social engineering door criminelen. Naast bewustmaking worden mensen en bedrijven ook voorzien van handelingsperspectieven om slachtofferschap te voorkomen of te beperken door een einde aan de situatie te maken. Op veiliginternetten.nl kunnen burgers terecht voor informatie en tips. In het najaar van 2025 wordt de campagne doorgezet met een nieuwe campagneflight. Daarbij worden de inzichten van het campagne-effectonderzoek dat jaarlijks wordt uitgevoerd, meegenomen.

Tool Cyberweerbaarheid

Het ministerie van BZK heeft in samenwerking met het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) de Tool Cyberweerbaarheid ontwikkeld voor baliemedewerkers van maatschappelijke en sociale instellingen, waaronder bibliotheken. Dit is een help-de-helper tool waarmee vragen en problemen van burgers op het gebied van cyberveiligheid beantwoord en opgelost kunnen worden. Inmiddels zijn de eerste ervaringen met de tool opgedaan.

Campagne 'Dubbel beveiligd is dubbel zo veilig'

In februari 2024 is de campagne 'Dubbel beveiligd, is dubbel zo veilig' gelanceerd door het ministerie van JenV. Deze campagne richt zich op het aanzetten van burgers tot het

instellen van tweestapsverificatie (2FA).[1] Er zal in 2025 worden ingezet op het verder versterken van samenwerkingen, onder andere met cyberburgemeesters, het CCV, en de Vereniging van Nederlandse Gemeenten (VNG). De campagne zal daarnaast, op basis van inzichten uit 2024, worden voortgezet met vergelijkbare doelstellingen en een aanscherping van de boodschap omtrent de noodzaak voor het instellen van 2FA. Tot slot wordt de landingspagina, veiliginternetten.nl, structureel geactualiseerd en voorzien van nieuwe content om jongeren én andere doelgroepen aan te sporen tot de gewenste gedragsverandering.

Campagne 'Doe je updates'[2]

Sinds 2019 richt het ministerie van EZ zich met campagnes op consumenten die slimme apparaten (verbonden met het internet) kopen of in bezit hebben. De campagne 'Doe je updates' is een initiatief om de bewustwording van burgers met betrekking tot het uitvoeren van updates van slimme apparaten te vergroten. 89% van de Nederlanders heeft één of meerdere slimme apparaten in huis[3] en het merendeel van deze mensen is zich ervan bewust dat deze apparaten gehackt kunnen worden en dat ze voorzien moeten worden van updates om hacken te voorkomen. Toch stelt meer dan de helft van de mensen updates uit. Daarmee zijn Nederlanders kwetsbaar voor internetcriminelen. Deze campagne wordt ondersteund door de convenantpartners van 'Doe je updates', waar een toolkit met artikelen en afbeeldingen is ontwikkeld om de campagne via de eigen kanalen te ondersteunen[4]. In de zomer 2025 start naar verwachting (met een soft launch) de zevende flight van de campagne, waarbij de online uitingen zich primair richten op Nederlanders tussen de 18 en 45 jaar. Op basis van de resultaten uit het campagne effectonderzoek worden met name aanpassingen doorgevoerd in de kanalenkeuze en de manier waarop wordt opgeroepen tot actie.

Vergroten basisweerbaarheid overheid en ondernemers

Actieprogramma Veilig Ondernemen (AVO)

De preventie van cybercrime voor het midden- en kleinbedrijf is een geprioriteerd thema binnen het Actieprogramma Veilig Ondernemen 2023-2026 van het Nationaal Platform Criminaliteitsbeheersing. Doel van het Nationaal Platform Criminaliteitsbeheersing is om publiek-private samenwerking te stimuleren op nationaal, regionaal en lokaal niveau. Het Digital Trust Center (DTC) is een belangrijke partner in deze aanpak. Gedurende de fusie tussen het DTC en het Nationaal Cyber Security Centrum kunnen ondernemers blijven rekenen op de diensten en producten van die zij nodig hebben om meer cyberweerbaar te worden. Het Digital Trust Center en de Platforms Veilig Ondernemen (PVO) werken daarbij nauw samen om de ontwikkelde producten op maat gesneden aan te bieden bij ondernemers om de cyberweerbaarheid te verhogen.

City Deal Lokale Weerbaarheid Cybercrime

De City Deal Lokale Weerbaarheid Cybercrime zet zich in om gemeenten in Nederland te ondersteunen bij het versterken van de cyberweerbaarheid van bedrijven en kwetsbare inwoners. In 2024 zijn opnieuw nieuwe innovatieve pilots van start gegaan met als doel het verhogen van de cyberweerbaarheid van de doelgroepen jeugd, senioren, laaggeletterden, het midden- en kleinbedrijf. Ook zijn pilots gestart om gemeenten te

[1] Dubbel beveiligd is dubbel zo veilig (veiliginternetten.nl)
[2] Informatie is geactualiseerd op basis van publiek beschikbare informatie.
[3] Bijna kwart Nederlanders gebruikt kunstmatige intelligentie zoals ChatGPT | CBS
[4] Convenantpartners Doe je updates

faciliteren in hun aanpak van online aangejaagde ordeverstoringen. Projecten die succesvol zijn gebleken, worden actief verspreid door regionale samenwerkingsverbanden die gemeenten en ondernemers bijstaan met expertise en capaciteit op het thema cybercrime. Enkele projecten worden voorzien van effectevaluaties door CyberweerbaarNL. De City Deal loopt eind 2025 af. Om te zorgen dat ook na 2025 gebruik kan worden gemaakt van de succesvolle projecten, ontwikkelde werkwijzen en ontstane netwerken, wordt in samenwerking met de betrokken publieke en private partijen ingezet op het borgen hiervan. Daarnaast is er doorlopend aandacht voor actuele en relevante problemen van de doelgroep.

Alert Online

In de cybersecurity-maand oktober wordt via het publiek-private partnernetwerk van Alert Online, een initiatief van het ministerie van EZ, aandacht gevraagd voor cybersecurity en cybercrimepreventie. De partners van Alert Online organiseren in die maand onder de vlag van Alert Online evenementen, trainingen of oefeningen voor hun medewerkers, relaties en/of klanten om zo cybersecurity onder de aandacht te brengen. Dit draagt bij aan het bewustzijn dat leidt tot grotere digitale weerbaarheid.

Verkleinen van de daderpopulatie

Naast de preventie van slachtofferschap, richt preventie zich ook op het verkleinen van de daderpopulatie door middel van gerichte interventies om daderschap te ontmoedigen en recidive te beperken[5]. In april 2024 zijn drie pilots van start gegaan, in samenwerking met de politie, gericht op daderpreventie onder jongeren. De huidige activiteiten voor het verkleinen van de daderpopulatie onder jongeren bestaan uit:

- Uitbreiding van onlineadvertenties en voorlichtingsprogramma's op scholen om jongeren bewust te maken van de juridische en sociale gevolgen van cybercriminaliteit.
- Interventieprogramma's in samenwerking met Halt en gemeenten, waarbij jongeren die een cyberdelict hebben gepleegd, begeleid worden naar legitieme ICT-gerelateerde opleidingen of banen (RE_B00TCAMP).
- Meer aandacht voor signalen van 'eerste stappen' in cybercriminaliteit, zoals het gebruik van DDoS-aanvallen en online fraude, zodat interventies eerder kunnen plaatsvinden (Cease & Desist en Hack_Right).

Hack_Right is een keteninterventie voor jongeren die voor een cyberdelict worden vervolgd. In deze interventie werken private en publieke organisaties samen om recidive te voorkomen en het cybertalent van jongeren verder te ontwikkelen binnen de kaders van de wet. Gedurende Hack_Right krijgt de jongere twee begeleiders: één begeleider vanuit Halt, de Raad voor de Kinderbescherming of Reclassering Nederland en één begeleider vanuit de private sector, veelal een cybersecuritybedrijf. De jongere doorloopt modules die gaan over online grenzen, slachtoffers, impactbesef en herstel.

Begin 2025 is Hack_Right met een communicatiecampagne opnieuw onder de aandacht gebracht van de politie, het OM en de uitvoerders Halt, Raad voor de Kinderbescherming en Reclassering Nederland. Hack_Right wordt tot en met eind 2026 gesubsidieerd door het Ministerie van Justitie en Veiligheid. Aan het eind van de subsidieperiode wordt bekeken of Hack_Right voldoende instroom heeft om definitief te worden ingebed in het interventiepalet van de uitvoerders. Hack_Right is een door Nederland ontwikkelde

[5] Kamerbrief over integrale aanpak cybercrime en digitale opsporing (28-06-2024).

interventie die internationaal in de belangstelling staat. Eind 2024 is door het InterCOP netwerk (International Cyber Offender Prevention Network), dat door het COPS-team van de Nederlandse politie wordt geleid, een workshop georganiseerd voor meer dan 10 landen die interesse hebben in de methodiek van Hack_Right.

Situationele preventie

Pilot Anti Phishing Shield (APS)

Een Anti Phishing Shield (APS) is een systeem dat internetgebruikers herleidt naar een waarschuwingspagina in het geval zij een malafide website dreigen te bezoeken. Het Centrum voor Cybersecurity België (CCB) heeft een aantal jaar geleden een APS opgetuigd, waarbij in 2022 maar liefst 14 miljoen keer werd voorkomen dat een malafide website werd bezocht[6]. Om de inzet van een effectief Anti Phishing Shield (APS) in Nederland te onderzoeken, wordt door het NCSC in samenwerking met KPN in de zomer van 2025 van een pilot gestart.

[6] 14 miljoen kliks naar verdachte websites vermeden dankzij uniek Anti-Phishing Shield | Centrum voor Cybersecurity België