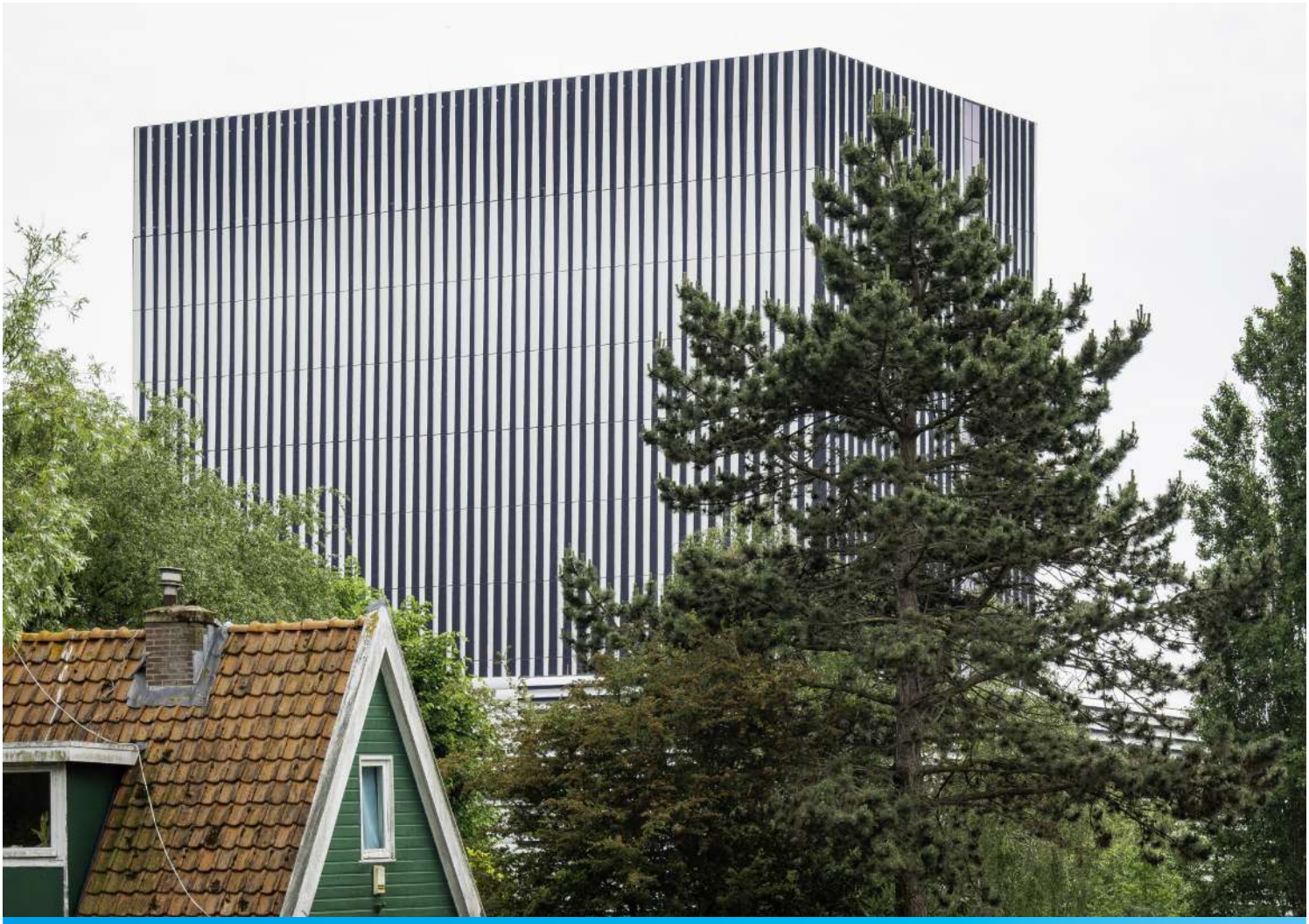
Nationaal Coördinator Terrorismebestrijding
en Veiligheid
Ministerie van Justitie en Veiligheid



Cybersecuritybeeld Nederland 2026

AI versnelt, verdiept en verbreedt de dreiging

November 2026

Omslag: *De Nederlandse samenleving draait op digitale infrastructuur. Zonder die infrastructuur valt het dagelijks leven grotendeels stil. De cyberdreiging waarmee onze samenleving wordt geconfronteerd, is omvangrijk en geavanceerd. Statelijke actoren en cybercriminelen die het op Nederland hebben gemunt, vallen deze infrastructuur voortdurend aan.*

Samenvatting

AI versnelt, verdiept en verbreedt de dreiging

Het Cybersecuritybeeld Nederland (CSBN) 2026 laat zien dat de capaciteiten en activiteiten van statelijke actoren en cybercriminelen toenemen. Hoewel er verschillende maatregelen worden genomen om Nederland tegen deze veranderende cyberdreiging te verdedigen, groeit de digitale weerbaarheid van Nederlandse organisaties en bedrijven niet in hetzelfde tempo mee. Hierdoor ontstaat verdere scheefgroei tussen de cyberdreiging en de digitale weerbaarheid. Dit vormt een ernstig risico voor de nationale veiligheid. Deze scheefgroei vergroot de kans dat Nederland slachtoffer wordt van maatschappij ontwrichtende spionage, datadiefstal, sabotage en uitval van digitale processen. De komende jaren zal AI het cyberlandschap ingrijpend veranderen en de dreiging verder versterken. Zoals het jaarbeeld (zie o.a. de infographic op pagina 6 en 7), met daarin een selectie van publiekelijk bekende incidenten in deze rapportageperiode (augustus 2025 – augustus 2026), laat zien, heeft Nederland nu al te maken met veel cyberincidenten. Een deel van de cyberaanvallen waarvan Nederlandse organisaties en bedrijven slachtoffer zijn, is bovendien (nog) onzichtbaar. Het is dan ook niet de vraag óf, maar wanneer Nederland te maken krijgt met een maatschappij ontwrichtend cyberincident.

Cyberdreiging: toenemende cybercapaciteiten en -activiteiten

Statelijke actoren vergroten hun cybercapaciteiten om, als onderdeel van hybride en militaire conflictvoering, hun politieke, militaire en economische doelen te bereiken. Van China, Rusland, Iran en Noord-Korea is al langer bekend dat zij een offensief cyberprogramma hebben dat zich ook op Nederland richt. Daarnaast beschikken steeds meer andere landen al over zo'n programma, of ontwikkelen er een. Nederlandse (overheids) organisaties, bedrijven en burgers zijn geregeld slachtoffer van cyberaanvallen van statelijke actoren.

Zo werden deze rapportageperiode Nederlandse overheidsmedewerkers slachtoffer van Russische hackers die wereldwijd toegang probeerden te krijgen tot Signal- en WhatsApp-accounts. Ook waren Nederlandse IP-camera's, die via het internet toegankelijk zijn, doelwit van Russische statelijke hackers. Zij verzamelen daarmee militair relevante gegevens, zoals militaire transportroutes en de logistieke afwikkeling van materieel aan Oekraïne. Daarnaast blijft Iran onverminderd inzetten op cyberspionagecampagnes tegen in het Westen verblijvende critici van het Iraanse regime, onder wie dissidenten en journalisten. Iran gebruikte hiervoor geavanceerde malware om toegang te verkrijgen tot persoonlijke apparatuur en accounts.

In militaire conflicten zijn cyberaanvallen inmiddels onmisbaar. Verschillende landen zetten in tijden van oorlog cyberaanvallen in als opstap naar en ondersteuning van fysieke militaire aanvallen. Het toenemende gebruik van cyberaanvallen in militaire conflicten is ook relevant voor de Nederlandse nationale veiligheid. Het is immers voor het eerst in lange tijd reëel dat Nederland, op grond van artikel 5 van het NAVO-verdrag (de collectieve verdedigingsclausule), direct betrokken raakt bij een grootschalig gewapend conflict.

Ook cyberaanvallen door cybercriminelen vormen een dreiging voor de nationale veiligheid. Cybercriminaliteit is inmiddels uitgegroeid tot een effectief georganiseerd ecosysteem met professionele samenwerkingsverbanden. Cybercriminelen lijken zich in toenemende mate te richten op het stelen van grote hoeveelheden data, om daarmee bedrijven en organisaties af te persen, om de data te gebruiken voor andere cyberaanvallen of door te verkopen aan andere criminelen of statelijke actoren. Zo werd deze rapportageperiode Odido door de hackersgroep ShinyHunters aangevallen en stalen zij gegevens van ruim 6 miljoen (oud-)klanten. Ondanks beloftes van cybercriminelen blijkt uit verschillende opsporingsonderzoeken van de Nederlandse politie dat het betalen van losgeld na datadiefstal geen garantie biedt dat gestolen gegevens daadwerkelijk worden verwijderd.

Dit CSBN laat voor het eerst zien dat cyberactoren AI aantoonbaar inzetten bij cyberaanvallen. Hiermee vergroten zij de snelheid, schaal en efficiëntie van cyberaanvallen. Meestal gaat het hierbij om ondersteunend gebruik bij het uitvoeren van een cyberaanval. Door het gebruik van AI vinden kwaadwillenden geautomatiseerd steeds sneller en steeds meer onbekende kwetsbaarheden in onze digitale infrastructuur. Ook worden kwetsbaarheden in steeds kortere tijd en door meer actoren misbruikt. Cyberactoren gebruiken AI ook voor het ontwikkelen van malware. Met AI kan malware sneller worden ontwikkeld, waarbij AI de malware schrijft en verfijnt. Tot slot vervult AI een steeds grotere operationele rol. In dit geval communiceert de malware met een AI-model tijdens de aanval om nieuwe commando's te schrijven of zijn eigen code realtime te herschrijven.

Digitale weerbaarheid blijft structureel achter bij cyberdreiging

Verschillende onderzoeken laten de afgelopen rapportageperiode zien dat de digitale weerbaarheid van Nederlandse (overheids) organisaties en bedrijven tegen huidige en toekomstige cyberdreigingen tekortschiet. Ondanks jarenlange waarschuwingen en concrete cyberincidenten heeft een deel van de Nederlandse (overheids)organisaties en bedrijven de basismaatregelen niet op orde. Zo ziet het NCSC bijvoorbeeld dat organisaties actief misbruikte kwetsbaarheden nog steeds te laat patchen, ondanks preventieve waarschuwingen. De digitale weerbaarheid van Nederlandse organisaties en bedrijven is daarnaast onvoldoende voorbereid op technologische ontwikkelingen, zoals AI en quantumcomputers.

Bij het achterblijven van de weerbaarheid spelen onder andere een gebrek aan eigenaarschap, bestuurlijke sturing, financiële middelen en capaciteit een rol. Ook zijn er verschillen tussen grote organisaties en bedrijven en kleinere organisaties en bedrijven. Met name voor kleine organisaties en het mkb is het op peil brengen en houden van hun digitale weerbaarheid een uitdaging. Dat is ook niet verwonderlijk. Mkb'ers hebben te maken met minder wettelijke verplichtingen en minder ondersteuning vanuit de overheid dan grote bedrijven die essentiële of belangrijke diensten verlenen.

Europa, en daarmee Nederland, is voor veel digitale processen en diensten afhankelijk van niet-Europese aanbieders. Meer dan in voorgaande jaren lijkt er een breed maatschappelijk en politiek besef te zijn van de risico's van de Nederlandse en Europese digitale afhankelijkheid. Deze rapportageperiode bleek meermaals dat de risico’s van digitale afhankelijkheden niet louter theoretisch zijn en dat de digitale dienstverlening daadwerkelijk kan wegvallen. Zo verbood de Amerikaanse regering Anthropic half juni 2026 tijdelijk om niet-Amerikaanse bedrijven en personen nog langer toegang te geven tot zijn AI-modellen Fable 5 en Mythos 5.

Scheefgroei dreiging en weerbaarheid vormt risico voor de nationale veiligheid

Verschillende cyberincidenten in het jaarbeeld van dit CSBN illustreren de scheefgroei tussen de cyberdreiging en digitale weerbaarheid. Voorbeelden hiervan zijn de compromittering van de Dienst Justitiële Inrichtingen (DJI), de Autoriteit Persoonsgegevens (AP) en de Raad voor de Rechtspraak, waarbij kwaadwillende hackers inzage kregen in persoonsgegevens van medewerkers. Ook stalen kwaadwillende hackers via een ClickFix-aanval bijna 552.000 bestanden van de gemeente Epe, waaronder persoonsgegevens van inwoners. Bij softwareleverancier ChipSoft maakten cybercriminelen grote hoeveelheden medische patiëntgegevens buit. Naast de zichtbare cyberincidenten in het jaarbeeld is Nederland ook geregeld slachtoffer van cyberaanvallen die überhaupt niet opgemerkt worden. Zo wordt maar een beperkt deel van de Chinese cyberoperaties tegen Nederland gedetecteerd en gemitigeerd.

De scheefgroei tussen de cyberdreiging en de digitale weerbaarheid kan bij burgers leiden tot afnemend vertrouwen of juist apathie ten opzichte van digitale weerbaarheid. Dit kan de verdere digitalisering van de samenleving bemoeilijken. Hiervoor is niet alleen van belang dat digitale systemen goed functioneren, maar ook dat burgers erop vertrouwen dat ze veilig zijn. Daarnaast moeten burgers zelf nadenken over veilig gebruik van digitale processen.

Wanneer AI alle onderdelen van cyberaanvallen verder automatiseert of zelfs autonoom uitvoert, worden cyberaanvallen nog sneller, grootschaliger en geavanceerder. Als de digitale weerbaarheid van Nederlandse (overheids)organisaties en bedrijven dan niet aanzienlijk verbetert, zal het aantal cyberincidenten de komende jaren fors toenemen. Hierbij neemt de kans op cyberincidenten bij (overheids)organisaties en bedrijven die de samenleving ontwrichten toe. Dit zou met name een ongelijk speelveld vormen voor kleine organisaties en het mkb. Zij blijven in verhouding tot grote organisaties en bedrijven achter in het nemen van maatregelen voor de noodzakelijke verhoging van hun digitale weerbaarheid. Kleine organisaties en het mkb kunnen hun weerbaarheid niet zelfstandig verhogen. Ook toeleveranciers, toezichthouders en andere overheidsinstanties zijn daar medeverantwoordelijk voor.

De ontwikkeling van AI verloopt in een uitzonderlijk hoog tempo en blijft daarmee ons voorstellingsvermogen uitdagen. Capaciteiten die enkele jaren geleden nog als toekomstscenario werden beschouwd, zijn inmiddels werkelijkheid. Voor de weerbaarheid van Nederlandse organisaties en bedrijven betekent dit dat zij zich niet alleen moeten voorbereiden op verwachte technologische ontwikkelingen, maar ook rekening moeten houden met onverwachte doorbraken die nieuwe uitdagingen met zich meebrengen. Het verhogen van de weerbaarheid is dus nooit af.

Op de volgende pagina's wordt het incidentenbeeld CSBN 2026 weergegeven. Meer informatie per incident is in hoofdstuk 5 'Jaarbeeld' inzichtelijk.

Incidentenoverzicht CSBN 2026

2025

Augustus 2025

Binnenland

- Citrix-systemen van enkele Rijksorganisaties gehackt
- Routers kleine Internet Service- en Hostingproviders in Nederland gecompromitteerd door Salt Typhoon

September 2025

Binnenland

- Ambassades doelwit van spearphishingcampagne door pro-Iraanse hackers
- Ambtenaren ondervinden hinder bij thuiswerken door DDoS-aanvallen op overheid
- Nederlandse tieners voeren verkenningsoperatie uit voor Rusland
- Gevoelige gegevens van (kwetsbare) inwoners gemeente Eindhoven ingevoerd in openbare AI-tools

Buitenland

- Vluchtverkeer diverse Europese luchthavens ontregeld door ransomware-aanval op toeleverancier
- Honderden npm-pakketten geïnfecteerd in supply chain-aanval
- Productie Jaguar Land Rover ernstig verstoord door cyberaanval
- Vermoedelijke staatshackers compromitteren groot Amerikaans telecombedrijf

Oktober 2025

Binnenland

- Honderden apps en websites wereldwijd werkten niet door storing bij AWS
- Data gelekt na ransomware-aanval bij afvalverwerker Omrin
- Europese diplomatieke entiteiten doelwit van Chinese hackers, ook doelwitten in Nederland

Buitenland

- Data gestolen bij Zweedse netbeheerder na inbraak op filesharingsysteem
- Hacktivisten manipuleren systemen na aanval op industriële controlesystemen van Canadese olie- en gasbedrijven

November 2025

Binnenland

- Problemen met uitzendingen en publicaties na ransomware-aanval bij RTV Noord
- Extreemrechtse berichten op websites van o.a. ziekenhuizen en vervoerder
- Wereldwijd websites uren onbereikbaar door storing bij Cloudflare

Buitenland

- Korte verstoringen van websites Belgische telecombedrijven na DDoS-aanvallen door pro-Russisch hackerscollectief
- Data van minstens tweehonderd Salesforce-klanten gestolen via applicatie(s) van leverancier
- Deense partijwebsites aan vooravond van verkiezingen kortstondig offline door DDoS-aanvallen

2026

December 2025

Binnenland

- Hackers stelen data van Interrail reizigers

Buitenland

- Russische hackers verstoorden communicatie Poolse energie-installaties, ontwrichtende gevolgen blijven uit
- Warmtekrachtcentrale Polen ontregeld door cyberaanval
- Data gestolen na hack van ‘externe servers’ van ESA
- Hackers stelen data van Mexicaanse overheidssystemen

Januari 2026

Binnenland

- Patiëntgegevens huisartsenorganisatie gelekt na hack op e-mailaccount

Buitenland

- Onbekende actor voert cyberaanval uit op water- en rioleringsbedrijf in Mexico
- Iraanse staatshackers voeren aanvallen uit met ransomware
- Operaties en consultaties Belgische ziekenhuizen uitgesteld na ransomware-aanval

Februari 2026

Binnenland

- Gevoelige persoonsgegevens online gepubliceerd na datadiefstal bij Odido
- Meerdere Nederlandse organisaties gecompromitteerd via Ivanti EPMM-kwetsbaarheid

Maart 2026

Binnenland

- Onbekenden krijgen ongeautoriseerde toegang tot systemen ministerie van Financiën
- Politie doelwit van phishing
- Bijna 552.000 bestanden van gemeente Epe gestolen via ClickFix-aanval

Buitenland

- Open source kwetsbaarhedenscanner Trivy voorzien van infostealer-malware
- Data gestolen van EU-hostingplatform door ShinyHunters
- Axios npm-pakket voorzien van malware na hack door Noord-Koreaanse hackers
- Wereldwijde netwerkuitval bij medische fabrikant Stryker na aanval door pro-Iraanse hackers

April 2026

Binnenland

- Patiëntgegevens gestolen na ransomware-aanval op toeleverancier zorginstellingen

Buitenland

- Persoonsgegevens gestolen bij Franse instantie die identiteitsbewijzen uitgeeft

Mei 2026

Binnenland

- Data gestolen bij leverancier onderwijsplatform, lijkt niet gelekt na betaling losgeld
- Instituut voor de Nederlandse Taal haalt websites offline na ransomware-aanval

Buitenland

- Hackers stelen patiëntdata van Duitse ziekenhuizen via externe dienstverlener

Juni 2026

Binnenland

- Signal- en WhatsApp-gebruikers doelwit van phishingaanvallen
- Klantgegevens zakenreisbureau BCD gelekt na hack door ShinyHunters
- Weg- en vaarweggebruikers ondervinden hinder als gevolg van technische storing bij Rijkswaterstaat
- OT-systemen Nederlandse organisaties gecompromitteerd door NoName

Buitenland

- ShinyHunters claimt datadiefstal bij Raad van Europa
- Data gestolen bij waterbedrijf in Amerika, hackers claimen mogelijkheid tot verstoringen

Juli 2026

Binnenland

- Maasstad Ziekenhuis tijdelijk niet operationeel door grote ICT-storing na testen noodstroom
- Camera's langs militaire routes gehackt door Rusland

Buitenland

- AI-modellen OpenAI breken uit testomgeving en voeren autonoom aanval uit op Hugging Face
- Bedrijven gehackt nadat AI-modellen ontsnappen uit testomgeving
- Taiwanese (overheids)organisaties aangevallen met behulp van autonome AI

Augustus 2026

Binnenland

- Klantgegevens minstens twaalf bedrijven gelekt door aanval op logistiekbedrijf Ceva

Buitenland

- Verstoringen watervoorziening na cyberaanvallen op waterbedrijven in de VS
- Iraanse hackers legden Britse elektriciteitscentrale vier dagen plat

Inhoudsopgave

Samenvatting 3

Incidentenoverzicht CSBN 2026 5

1. Inleiding 10

2. Cyberdreiging: toenemende cybercapaciteiten en -activiteiten 13

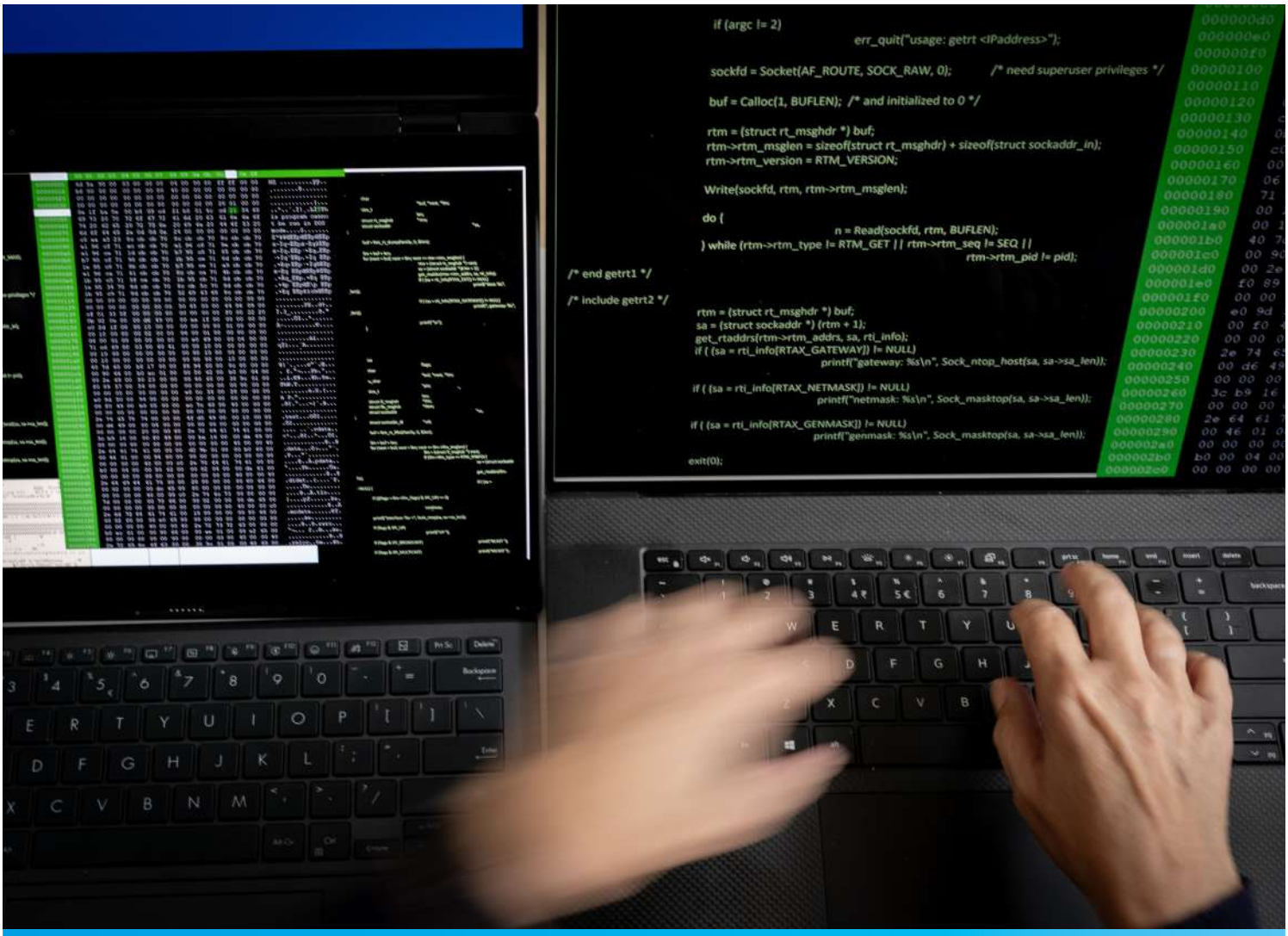
3. Digitale weerbaarheid blijft structureel achter bij cyberdreiging 23

4. Scheefgroei dreiging en weerbaarheid vormt risico voor de nationale veiligheid 33

5. Jaarbeeld 39

Bijlage 1: Verantwoording 49

Bijlage 2: Bronnen 51



In augustus 2025 maakten de AIVD en MIVD bekend dat ook Nederland een doelwit is geweest van Salt Typhoon. Eind 2024 kwam deze grootschalige cyberspionagecampagne door de staatsgesteunde Chinese hackorganisatie Salt Typhoon aan het licht. Beide diensten hebben doelwitten in Nederland waargenomen. Het gaat hierbij niet om grote telecommunicatieproviders, maar om kleinere Internet Service- en Hosting providers.

1. Inleiding

De Nederlandse samenleving draait op digitale infrastructuur. Zonder die infrastructuur valt het dagelijks leven grotendeels stil. De cyberdreiging waarmee onze samenleving wordt geconfronteerd, is omvangrijk en geavanceerd. Statelijke actoren en cybercriminelen die het op Nederland hebben gemunt, vallen deze infrastructuur voortdurend aan. Voorbeelden in dit Cybersecuritybeeld Nederland 2026 (CSBN 2026) laten zien dat kwaadwillende hackers regelmatig succesvol zijn. Zo verkregen Russische statelijke cyberactoren toegang tot Signal-accounts van Nederlandse ambtenaren en hackten zij IP-camera's op militair-logistieke routes in Nederland.[1] Cybercriminelen stalen gevoelige medische data van Nederlandse patiënten bij een cyberaanval op softwareleverancier ChipSoft.[2] Hackersgroep ShinyHunters maakte in een van de grootste Nederlandse datadiefstallen ooit de gegevens van meer dan 6 miljoen (oud-)klanten van Odido buit.[3]

Statelijke actoren zetten al langere tijd cyberaanvallen in om hun doelen te bereiken. Verschuivende en verhardende geopolitieke verhoudingen brengen statelijke actoren ertoe hier extra in te investeren. Mede daardoor, en door de automatisering van cyberaanvallen met behulp van AI, nemen de capaciteiten en activiteiten van statelijke actoren en cybercriminelen toe. Dit CSBN laat voor het eerst zien dat cyberactoren AI aantoonbaar inzetten bij cyberaanvallen, waaronder bij aanvallen op operationele technologie (OT). Zo gebruikten kwaadwillende hackers AI voor technische werkzaamheden bij een reeks cyberaanvallen op Mexicaanse overheidsinstanties en kritieke infrastructuur (ook wel vitale infrastructuur genoemd).[4] Daarnaast gebruikten Chinese staatshackers geavanceerde AI-modellen voor grootschalige cyberaanvallen op technologiebedrijven, financiële instellingen en overheden in verschillende landen.[5] Door het gebruik van AI vinden kwaadwillenden bovendien geautomatiseerd steeds sneller en steeds meer onbekende kwetsbaarheden in onze digitale infrastructuur. Ook worden kwetsbaarheden in steeds kortere tijd en door meer actoren misbruikt.[6] De razendsnelle ontwikkeling van AI blijft ons voorstellingsvermogen uitdagen. Veel onderwerpen in dit CSBN zijn niet meer los te zien van large language models (LLM's), agentic AI en frontier AI-modellen, de meest geavanceerde modellen van dit moment.

Tegelijkertijd blijkt uit verschillende rapporten en uit de praktijk dat de digitale weerbaarheid van Nederlandse (overheids)organisaties en bedrijven structureel achterblijft bij de dreiging.[7] Een deel van deze organisaties en bedrijven is onvoldoende voorbereid op cyberaanvallen en heeft de basismaatregelen voor cyberveiligheid, preventie, monitoring en detectie niet op orde.[8] Ook doen (overheids)organisaties niet altijd aangifte van een cyberaanval. Mede hierdoor hebben we onvolledig zicht op cyberaanvallen op Nederland. (Overheids)organisaties en bedrijven moeten ervan uitgaan dat kwaadwillende hackers in hun digitale systemen aanwezig zijn, zonder dat zij precies weten wie waar toegang tot heeft verkregen en welke schade ze kunnen aanrichten. Vanuit het 'assume breach'-denken zouden organisaties en bedrijven hun aandacht niet alleen moeten richten op het voorkomen van een digitale aanval, maar ook op het detecteren van aanvallers die al op het netwerk aanwezig zijn en op het reageren daarop.

Hoewel de overheid en het bedrijfsleven veel doen om Nederland tegen deze cyberdreiging te verdedigen, groeit de weerbaarheid van Nederlandse organisaties en bedrijven niet met het tempo dat nodig is om de toenemende capaciteiten van kwaadwillenden bij te houden. Hierdoor ontstaat verdere scheefgroei tussen de cyberdreiging en de digitale weerbaarheid.[9] Dit vormt een ernstig risico voor de nationale veiligheid. Statelijke actoren kunnen onopgemerkt spioneren en strategische posities verwerven in Nederlandse systemen en kritieke infrastructuur.[I] Die posities kunnen zij later inzetten voor sabotage. Tegelijkertijd zijn cyberdreigingen als spionage en voorbereiding op sabotage voor veel mensen ongrijpbaar, juist omdat deze dreigingen onopgemerkt blijven en schade niet altijd direct zichtbaar of merkbaar is.

AI zal het cyberlandschap de komende jaren ingrijpend veranderen en de dreiging verder versterken. Als de digitale weerbaarheid van Nederlandse organisaties en bedrijven niet aanzienlijk verbetert, zal het aantal cyberincidenten fors groeien. Dat leidt naar verwachting ook tot meer meldingen bij overheidsorganisaties die incidenten afhandelen. Meer incidenten vergroten bovendien de kans dat Nederland slachtoffer wordt van spionage, datadiefstal, ontwrichtende sabotage en uitval van digitale processen, met impact op de nationale veiligheid. Dat zal met name een ongelijk speelveld

I Statelijke actoren gebruiken cyberaanvallen ook om beïnvloedingsactiviteiten uit te voeren. Deze vallen echter buiten de scope van het CSBN.

vormen voor kleine organisaties en het mkb. Zij blijven in verhouding tot grote organisaties en bedrijven achter in het nemen van maatregelen voor de noodzakelijke verhoging van hun digitale weerbaarheid. Zo dreigt een kloof tussen grote, weerbare organisaties en kleinere, kwetsbare organisaties. Kleine organisaties en het mkb kunnen hun weerbaarheid niet zelfstandig verhogen. Ook de overheid, leveranciers en toezichthouders zijn daar medeverantwoordelijk voor.

Doel en afbakening

Het CSBN 2026 biedt inzicht in de digitale dreiging, de belangen die daardoor kunnen worden aangetast, de digitale weerbaarheid en tot slot de digitale risico's. De rapportageperiode voor dit CSBN loopt van augustus 2025 tot en met augustus 2026. De focus ligt daarbij op de nationale veiligheid. Digitalisering biedt vele kansen, maar brengt tegelijkertijd kwetsbaarheden met zich mee die kunnen worden misbruikt voor criminele of geopolitieke doeleinden. Ook kan er sprake zijn van onbedoelde uitval en verstoring van digitale processen. Hoewel de positieve maatschappelijke en economische ontwikkelingen van digitalisering aanzienlijk zijn, vallen deze buiten de reikwijdte van het CSBN.

Het CSBN is primair bedoeld voor strategie- en beleidsvorming op nationaal niveau. Het beoogt het kabinet, de leden van de Eerste en Tweede Kamer, ambtenaren, beleidsmakers, Chief Information Security Officers (CISO's), bestuurders van bedrijven en organisaties, directies en andere geïnteresseerden inzicht te geven in de digitale dreigingen en risico's voor Nederland. Cybersecuritybedrijven en -professionals gebruiken het CSBN als referentiekader voor de eigen bestuurders of klanten. Het CSBN is ook bedoeld als hulpmiddel voor risicomanagement, waarbij het zich specifiek richt op de identificatie en analyse van risico's, een van de stappen in een risicomanagementproces. Daarnaast dient het CSBN als informatiebron voor het brede publiek.

Leeswijzer

Dit CSBN 2026 is als volgt opgebouwd:

- Hoofdstuk 2 geeft de actuele dreigingen vanuit statelijke actoren en cybercriminelen weer. Hierbij wordt specifiek ingegaan op veelgebruikte aanvalsmethoden in deze rapportageperiode, en de manier waarop AI cybercapaciteiten en -activiteiten vergroot.
- Hoofdstuk 3 schetst dat de digitale weerbaarheid van Nederlandse (overheids)organisaties en bedrijven structureel achterblijft bij de cyberdreiging. In dit kader wordt ook de digitale autonomie van Nederland belicht.
- Hoofdstuk 4 beschrijft de scheefgroei tussen de cyberdreiging en de achterblijvende weerbaarheid. Ook duidt dit hoofdstuk de concrete gevolgen hiervan voor Nederland.
- Hoofdstuk 5 biedt tot slot een overzicht van relevante cyberincidenten in Nederland en in vergelijkbare landen in de rapportageperiode, die loopt van augustus 2025 tot en met augustus 2026.



Russische diensten hebben "een klein aantal camera's" op militaire routes in Nederland gehackt. Dat blijkt uit onderzoek van de AIVD en MIVD. Volgens de diensten ging het om camera's in particulier gebruik, van onder meer bedrijven, die via het internet toegankelijk zijn. Die camera's kunnen van een afstand worden bekeken. Door de camera's te hacken kan Rusland inzicht krijgen in onder meer militaire transportroutes en het type wapens en materieel dat wordt vervoerd.

2. Cyberdreiging: toenemende cybercapaciteiten en activiteiten

Statelijke actoren vergroten hun cybercapaciteiten om, als onderdeel van hybride en militaire conflictvoering, hun politieke, militaire en economische doelen te bereiken. Nederlandse (overheids)organisaties, bedrijven en burgers zijn geregeld slachtoffer van hun cyberaanvallen.[10] De digitale dreiging van statelijke actoren tegen Nederland was de afgelopen rapportageperiode dan ook onverminderd hoog.[11] Statelijke actoren vergroten hun cybercapaciteiten onder andere door samen te werken met andere actoren. Tegelijkertijd blijft deze dreiging, die vaak gericht is op spionage en voorbereidingshandelingen voor sabotage, veelal onzichtbaar. AI vergroot de mogelijkheden van actoren om op grotere schaal aanvallen (deels) geautomatiseerd uit te voeren en kwetsbaarheden te vinden. Ook cyberaanvallen door cybercriminelen vormen een dreiging voor de nationale veiligheid. Cybercriminaliteit is inmiddels uitgegroeid tot een effectief georganiseerd ecosysteem met professionele samenwerkingsverbanden. Cybercriminelen lijken zich in toenemende mate te richten op het stelen van grote hoeveelheden data, om daarmee bedrijven en organisaties af te persen, om de data te gebruiken voor andere cyberaanvallen of om deze door te verkopen aan andere criminelen of statelijke actoren. Ondanks beloftes van cybercriminelen blijkt uit verschillende opsporingsonderzoeken van de Nederlandse politie dat het betalen van losgeld na datadiefstal geen garantie biedt dat gestolen gegevens daadwerkelijk worden verwijderd.

2.1 Cyberdreiging statelijke actoren onverminderd hoog

Van China, Rusland, Iran en Noord-Korea is al langer bekend dat zij een offensief cyberprogramma hebben dat zich ook op Nederland richt. Hiermee vormen zij een dreiging voor de Nederlandse nationale veiligheid. Daarnaast beschikken steeds meer andere landen over zo'n programma, of ontwikkelen er een. Daardoor is er een toename aan statelijke actoren met een cyberprogramma.[12] Bovendien zetten statelijke actoren erop in om hun (cyber) activiteiten zo lang mogelijk onopgemerkt te houden. Hierdoor is het beeld van statelijke dreigingen nooit volledig. Dat een dreiging of compromittering niet in beeld is, betekent immers niet dat die er niet is.

Cyberaanvallen als onderdeel van hybride en militaire conflictvoering

De machtsbalans in de wereld verandert. Het Westen en de bijbehorende liberale waarden voeren niet langer de boventoon. Hoe de nieuwe wereldorde eruit komt te zien, is nog onduidelijk. Wel verschuift de dominantie van de Verenigde Staten en het Westen nu al naar landen zoals China, Rusland, India, Iran, Saoedi-Arabië, Turkije en Indonesië.[13] In deze veranderende wereldorde zijn landen steeds meer bereid hun macht in te zetten om hun eigen belangen te verdedigen. Sommige van deze landen, zoals Rusland en Iran, gelden als systeemrivalen van het Westen. Dit geldt ook voor China, al is het land een belangrijke handelspartner van Nederland.[14]

Door deze groeiende competitie tussen grootmachten en geopolitieke spanningen is de wereld rondom Nederland en Europa instabieler en onveiliger.[15] Dit uit zich onder andere in een toename

van de inzet van hybride activiteiten.[16] Daarmee bedreigen statelijke actoren de Nederlandse nationale veiligheid, terwijl zij onder de drempel van een gewapend conflict blijven. Zij doen dit onder meer met fysieke en digitale sabotage, spionage, heimelijke beïnvloeding en economische druk.[17]

In dit kader maken statelijke actoren ook veelvuldig gebruik van cyberaanvallen om hun politieke, militaire en economische doelen te bereiken. Cyberactiviteiten van statelijke actoren staan dus niet op zichzelf, maar zijn onderdeel van een breder hybride instrumentarium van fysieke en digitale middelen. Cyberaanvallen zijn daarin aantrekkelijk voor statelijke actoren. Ze kunnen wereldwijd worden ingezet, zijn moeilijk te herleiden naar de daders en zijn relatief goedkoop in verhouding tot de schade die ze kunnen aanrichten.[18]

Ook in militaire conflicten zijn cyberaanvallen inmiddels onmisbaar. Verschillende landen zetten in tijden van oorlog cyberaanvallen in als opstap naar en ondersteuning van fysieke militaire aanvallen.[19] Zo gebruikt Rusland in de oorlog in Oekraïne cyberspionage ter ondersteuning van fysieke militaire operaties. Het land vergaart via cyberaanvallen informatie over troepenbewegingen en locatiegegevens van Oekraïense militairen.[20] Rusland gebruikt cyberoperaties daarnaast voor beïnvloedingsoperaties en het verspreiden van desinformatie.[21]

Voorafgaand aan en tijdens militaire conflicten saboteren landen via cyberaanvallen elkaars kritieke infrastructuur. Denk hierbij aan energiesystemen, telecommunicatie en transport.[22] Soms hebben statelijke actoren al ver voor zo'n conflict strategische posities binnen de systemen en kritieke infrastructuur van andere landen verkregen. Deze posities kunnen ze op een later moment inzetten, bijvoorbeeld tijdens een toekomstig conflict.[23]

Ook de recente grootschalige aanval van de VS en Israël op Iran, die in februari 2026 begon, liet zien hoe staten cyberaanvallen op onder andere kritieke infrastructuur inzetten voorafgaand aan de inzet van fysieke militaire middelen. De cyberaanvallen van de VS en Israël waren onder andere gericht op Iraanse overheidsdiensten en nieuwswebsites, waar anti-regimeberichten werden geplaatst. De Israëlische inlichtingendienst zou daarnaast al langere tijd toegang hebben gehad tot verkeerscamera's in Teheran. De daarmee vergaarde informatie zou vervolgens zijn gebruikt ter ondersteuning van aanvallen op hooggeplaatste Iraanse leiders.[24]

Het toenemende gebruik van cyberaanvallen in militaire conflicten is ook relevant voor de Nederlandse nationale veiligheid. Het is immers voor het eerst in lange tijd reëel dat Nederland, op grond van artikel 5 van het NAVO-verdrag (de collectieve verdedigingsclausule), direct betrokken raakt bij een grootschalig gewapend conflict.[25]

Chinese cyberdreiging omvangrijk, veel aanvallen onopgemerkt

De Chinese cyberdreiging blijkt ten opzichte van het vorige CSBN nog omvangrijker te zijn dan werd aangenomen.[26] Het Chinese Volksbevrijdingsleger reorganiseerde in 2024 zijn cybereenheden en bracht daarbij technische capaciteiten samen. Dit stelde Chinese hackers vanaf 2025 in staat hun tooling en infrastructuur voortdurend aan te passen en zeer flexibel in te spelen op kansen en veranderende omstandigheden. Volgens de MIVD staat China op het gebied van offensieve cybercapaciteiten nu waarschijnlijk op gelijke voet met de Verenigde Staten, die doorgaans als het meest geavanceerd ter wereld gelden.[27]

De Chinese cybercapaciteiten nemen onder andere toe doordat China een omvangrijk cyberecosysteem benut.[28] Dit is onderdeel van de Chinese whole-of-society-benadering. Deze benadering verplicht alle onderdelen van de samenleving, van individuen tot bedrijven en organisaties, om op verzoek van de Chinese overheid mee te werken aan bijvoorbeeld inlichtingenactiviteiten.[29] Het Chinese cyberecosysteem bestaat dan ook uit statelijke cyberactoren, bedrijven en kennisinstellingen die door de Chinese overheid worden ingezet om (delen van) cyberaanvallen te faciliteren en uit te voeren.[30] Zo doen kennisinstellingen onderzoek naar zero-day-kwetsbaarheden[II], die de overheid vervolgens kan misbruiken in cyberaanvallen. Ook leveren bedrijven digitale infrastructuur voor cyberoperaties. Daarnaast voeren bedrijven zelf offensieve cyberactiviteiten uit om informatie te verkrijgen die ze aan de Chinese overheid kunnen doorverkopen of die ze verplicht aan de overheid moeten verstrekken.[31]

Kenmerkend voor de werkwijze van Chinese actoren is dat zij bestaande digitale infrastructuur benutten: grootschalige netwerken van gecompromitteerde apparaten, zoals consumentenrouters en andere IoT- en smart devices.[32] Hiermee kunnen netwerken worden gecreëerd, bijvoorbeeld in de vorm van botnets, om bepaalde activiteiten te verhullen. Botnets bestaan uit apparaten die op afstand door aanvallers worden aangestuurd voor bijvoorbeeld DDoS-aanvallen. Op deze apparaten wordt malware geïnstalleerd, bijvoorbeeld door misbruik te maken van een kwetsbaarheid. Het gaat hierbij om een vaste set infrastructuur die in beheer is van een kwaadwillende actor. Operational Relay Box-netwerken lijken hierop, maar worden vaker als dienst aangeboden en richten zich vooral op het verhullen van activiteiten van een actor via meerdere tussenstappen. Ze zijn flexibeler en moeilijker te detecteren en worden steeds vaker gebruikt in geavanceerde spionagecampagnes. Naast Chinese actoren gebruiken ook andere kwaadwillende hackers deze veelgebruikte methode.[33]

Hoewel er geen absolute aantallen beschikbaar zijn, is het Chinese cyberprogramma zó omvangrijk en geavanceerd dat Nederland en andere landen waarschijnlijk maar een klein deel van de cyberaanvallen ontdekken. Dat betekent dat een groot deel van de Chinese cyberaanvallen op Nederland niet in beeld is en dat daar dus ook geen gerichte maatregelen tegen kunnen worden genomen. Hierdoor kunnen er nog actieve cybercampagnes zijn waarbij organisaties of bedrijven niet weten dat ze zijn gehackt en welke schade kwaadwillende hackers daarmee nu of in de toekomst kunnen aanrichten. Cyberactoren kunnen soms wel jaren onopgemerkt in systemen aanwezig zijn en tijdens die periode gevoelige informatie buitmaken, zich innestelen in systemen of achterdeuren inbouwen. Zo kwam eind 2024 de grootschalige cyberspionagecampagne van de Chinese actor Salt Typhoon tegen de wereldwijde telecomsector aan het licht. Chinese hackers zouden toen al enkele jaren onopgemerkt in systemen van de Amerikaanse telecomsector

II Een zero-day kwetsbaarheid is een zwakke plek in software of hardware die nog niet bij de ontwikkelaars ervan bekend is. Omdat de ontwikkelaars of fabrikant er nog geen weet van hebben, is er dus ook nog geen beveiligingsoplossing voor.

hebben gezeten en zeer gevoelige informatie hebben buitgemaakt.[34] Daarbij bleek dat de hackers telecomnetwerken binnendrongen via kwetsbaarheden in edge devices[III].[35] Ook een aantal kleinere Nederlandse internet service- en hostingproviders was doelwit van deze campagne.[36] De Salt Typhoon-campagne is illustratief voor de Chinese interesse in het compromitteren van de telecomsector. Onderzoek toont aan dat Chinese statelijke actoren zich op grote schaal strategisch (proberen te) positioneren om blijvende toegang tot de netwerken te behouden.[37]

Nederland doelwit voortdurende Russische cyberaanvallen

Russische statelijke cyberactoren en Russische staatsgesteunde groeperingen voeren voortdurend cyberaanvallen uit op Europese en Nederlandse doelwitten. Door digitale spionageaanvallen uit te voeren, probeert Rusland al jaren informatie te verkrijgen over Oekraïne. Zo vergaren ze inlichtingen over besluitvorming in de EU en in individuele lidstaten. Ook proberen ze met behulp van cyberaanvallen westerse (militaire) steun aan Oekraïne in beeld te krijgen en te verstoren.[38] Verder zet Rusland cyberaanvallen in om onrust onder NAVO-bondgenoten te creëren, om zo de steun aan Oekraïne te verzwakken.

De Nederlandse inlichtingendiensten waarschuwden dat Rusland wereldwijd toegang probeerde te krijgen tot een groot aantal Signal- en WhatsApp-accounts.[39] Deze campagne richtte zich op accounts van westerse en Oekraïense hoogwaardigheidsbekleders, overheidsmedewerkers, militairen, journalisten en andere personen die voor Russische spionage interessant zijn. Hoewel deze kanalen niet bedoeld zijn voor vertrouwelijke communicatie, hebben Russische actoren daarbij gevoelige informatie verzameld. Ook Nederlandse overheidsmedewerkers waren slachtoffer van deze campagne.[40] De meest waargenomen werkwijze is dat aanvallers zich voordeden als een supportchatbot van Signal. Zo wekten zij een vals gevoel van urgentie om gebruikers te verleiden informatie af te staan waarmee de hackers toegang verkregen tot hun account. Daarmee konden ze de chatgeschiedenis raadplegen en zich in chatgesprekken mengen. In sommige gevallen was het ook mogelijk de controle over het account over te nemen (of zelfs de oorspronkelijke gebruiker buiten te sluiten) en back-ups te verkrijgen.[41]

Russische statelijke hackers voeren daarnaast structureel digitale spionageoperaties uit tegen camera's die via het internet toegankelijk zijn, zogenoemde IP-camera's. Hoewel de grootste focus op Oekraïne ligt, is ook Nederland doelwit van deze operaties.[42] De informatie die de Russische staat via deze digitale operaties verkrijgt, is voor hen van groot belang. Het geeft inzicht in militair relevante gegevens, zoals militaire transportroutes. Daarnaast verkrijgt Rusland hiermee informatie over de logistieke afwikkeling van wapenleveringen of ander materieel aan Oekraïne.[43] Rusland maakt daarbij gebruik van beeldherkenningssoftware om gericht te zoeken naar militaire voertuigen en (militaire) ladingen.[44] Rusland gebruikt de toegang tot IP-camera's in Europese lidstaten verder om andere militair relevante inlichtingen te verwerven, ook wanneer die niet relevant zijn voor de oorlog in Oekraïne.[45] De spionageoperaties illustreren dat Rusland in staat is om relevante inlichtingen te vergaren uit IP-camera's en dat Russische militaire eenheden dezelfde tactieken kunnen inzetten in een eventueel toekomstig conflict.[46]

De Russische cyberactor APT28 voert cyberoperaties uit via een wereldwijd netwerk van gecompromitteerde apparaten, veelal routers, die samen een botnet vormen. Via dit botnet voerde APT28 een DNS-hijackingcampagne uit die wereldwijd slachtoffers maakte. Met deze campagne maakte de actor inloggegevens buit van domeinen die voor hem interessant zijn.[47]

Daarnaast investeren sommige Russische actoren in cybercapaciteiten om digitale sabotage te kunnen uitvoeren. Ook voor sabotageactiviteiten geldt dat de hoogste prioriteit nog altijd bij Oekraïne ligt. Zulke capaciteiten kunnen echter ook worden ingezet tegen andere doelwitten, in het bijzonder doelwitten in landen die Oekraïne steunen, zoals EU-lidstaten en NAVO-landen.[48] Dit bleek bijvoorbeeld uit een incident in december 2025, door de Europese Unie geattribueerd aan Rusland.[49] Volgens het Poolse Computer Emergency Response Team (CERT.PL) probeerde Rusland het Poolse elektriciteitsnet te saboteren met wiper malware, bedoeld om data onherstelbaar te vernietigen. De hackers richtten zich met de aanval op decentrale energiesystemen, waaronder een warmtekrachtcentrale en wind- en zonneparken. De aanval onderbrak de communicatie met de lokale netbeheerders, maar raakte de elektriciteitsproductie zelf niet.[50] Hoewel de aanval niet leidde tot verstoring van het elektriciteitsnet, stelde de Poolse minister van Energie dat het voor Polen de grootste cyberaanval in jaren was.[51]

Ook Nederlandse organisaties waren deze rapportageperiode slachtoffer van aanvallen van Russische hackers op OT-systemen. In juni 2026 claimde NoName057(16) het hacken van klimaatbeheersingssystemen bij twee Nederlandse organisaties (zie het jaarbeeld, hoofdstuk 5). De impact van dergelijke individuele incidenten is doorgaans beperkt, al kunnen aanvallen met name voor kleinere organisaties en het mkb wel vervelende verstoringen opleveren. Deze aanvallen waren een reactie op de aanhouding van twee personen door de FIOD in mei 2026, onder meer wegens het faciliteren van pro-Russische digitale aanvallen via een webhostingbedrijf.[52]

Bovenstaande incidenten passen in het bredere beeld dat de inlichtingendiensten hebben van de Russische cyberdreiging. Zowel statelijke als staatsgesteunde groeperingen voeren vanuit Rusland aanvallen uit. Die staatsgesteunde groeperingen ontvangen in verschillende mate steun van de Russische overheid, bijvoorbeeld in de vorm van capaciteiten, informatie of infrastructuur.[53] Bovendien neemt het aantal verschillende Russische cyberactoren toe, wat bijdraagt aan de capaciteiten om in een hoog tempo cyberaanvallen uit te voeren.[54] Hoewel de Russische focus op dit moment op Oekraïne ligt, zou Rusland de opgedane lessen en ervaring kunnen inzetten bij cyberaanvallen tegen NAVO-landen en EU-lidstaten, waaronder Nederland.

III Edge devices zijn digitale apparaten aan de rand van een netwerk. Ze vormen een brug tussen intern beheerde netwerken en externe, niet-vertrouwde netwerken zoals het internet. Deze apparaten werken als poortwachters: ze regelen het dataverkeer, zorgen voor beveiliging en maken verbindingen tussen verschillende netwerken mogelijk.

Iran richt cyberactiviteiten op tegenstanders en critici, ook in Nederland

Iraanse cyberactoren voerden de afgelopen rapportageperiode onverminderd cyberaanvallen uit voor beïnvloedingsoperaties, sabotage en spionage. Zij richten zich daarbij op regionale tegenstanders, zoals Israël. Daarnaast voeren ze cyberaanvallen uit op doelen in West-Europa en Noord-Amerika. Zo voerde de Iraanse groep Homeland Justice een spearphishingcampagne[IV] uit die voornamelijk was gericht op ambassades en consulaten wereldwijd. Ook Nederlandse diplomatieke posten waren doelwit van deze campagne.[55] Daarnaast blijft Iran volgens de inlichtingendiensten onverminderd inzetten op cyberspionagecampagnes tegen in het Westen verblijvende critici van het Iraanse regime, onder wie dissidenten en journalisten. Iran gebruikte hiervoor geavanceerde malware om toegang te verkrijgen tot persoonlijke apparatuur en accounts.[56]

De onrust in het Midden-Oosten leidde afgelopen periode ook tot een toename van pro-Iraanse hacktivistische activiteiten. Die activiteiten richtten zich vooral op Amerikaanse en Israëlische doelwitten. Hoewel Nederland geen primair doelwit was van deze activiteiten, hebben Nederlandse organisaties er wel impact van ondervonden. Zo ontstonden bij Nederlandse zorgorganisaties en ziekenhuizen logistieke problemen en verstoringen van belsystemen als gevolg van een cyberaanval op het bedrijf Stryker, een Amerikaanse producent van medische technologie.[57] Het is de vraag in hoeverre en op welke manier deze activiteiten zijn aangestuurd of gesteund door de Iraanse overheid. Verschillende wetenschappelijke onderzoeken en rapporten stellen bijvoorbeeld dat de groepen Homeland Justice en Handala zeer waarschijnlijk een verlengstuk van het Iraanse regime zijn.[58]

Iraanse cyberactoren voeren cyberaanvallen veelal uit in combinatie met informatieoperaties. Daarbij claimen zij successen en stellen zij de impact mogelijk groter voor dan die in werkelijkheid is.[59]

Noord-Koreaanse cyberactiviteiten raken ook Nederland

Noord-Korea zet onverminderd cyberaanvallen in om het huidige regime in stand te houden.[60] Het offensieve cyberprogramma draagt, onder andere door het stelen van cryptovaluta, zeer waarschijnlijk bij aan de financiering van het Noord-Koreaanse (nucleaire) wapenprogramma.[61] Noord-Korea verleende de afgelopen jaren ook militaire steun, zoals wapens en militairen, aan Rusland. De inkomsten uit het Noord-Koreaanse cyberprogramma kunnen daardoor ook bijdragen aan de oorlog in Oekraïne.[62]

Naast het stelen van cryptovaluta wil het regime met spionageoperaties informatie verkrijgen over hoogwaardige (militaire) technologie en over (geo)politieke en wetenschappelijke onderwerpen. Ook Nederlandse bedrijven en personen waren volgens de inlichtingendiensten afgelopen periode doelwit van Noord-Koreaanse cyberaanvallen.[63]

Het Noord-Koreaanse regime laat daarnaast duizenden hoogopgeleide IT-specialisten heimelijk bij westerse bedrijven werken. Ze doen zich vaak voor als iemand anders en gebruiken daarbij vervalste identiteitsdocumenten.[64] Hierbij maken ze onder andere gebruik van AI- en deepfake-tools om hun identiteit te verhullen. Ook gebruiken ze AI om voor sollicitatieprocedures valse documentatie, verzonnen referenties en werkportfolio's te genereren.[65] Veel van de Noord-Koreaanse IT-specialisten werken vanuit Noord-Korea, China, Rusland of landen in Zuidoost-Azië en Afrika, maar verbergen hun daadwerkelijke locaties. Dit doen ze onder andere door VPN's te gebruiken en door samen te werken met andere organisaties in westerse landen die bijvoorbeeld door bedrijven verstrekte laptops ontvangen.[66] De dreiging vanuit Noord-Koreaanse IT'ers was eerst voornamelijk gericht op de Verenigde Staten, maar heeft zich ontwikkeld richting Europa.[67] Daar komt bij dat de Nederlandse inlichtingendiensten afgelopen periode vaststelden dat een aantal van de waargenomen cyberoperaties in Nederland zeer waarschijnlijk is uitgevoerd door of met behulp van Noord-Koreaanse IT'ers.[68]

2.2 Datadiefstal cybercriminelen vormt een dreiging voor de nationale veiligheid

Cybercriminelen die data versleutelen of stelen om organisaties af te persen, zijn geen nieuw fenomeen. Datadiefstal gebeurt inmiddels echter op zo'n grote schaal dat het een dreiging voor de nationale veiligheid vormt. Het afgelopen jaar vond bovendien een van de grootste datadiefstallen uit de Nederlandse geschiedenis plaats.

Cybercriminelen professionaliseren en werken samen met statelijke actoren

Het cybercriminele ecosysteem is uitgegroeid tot een industrie van specialisten die verschillende schakels van een cyberaanval ontwikkelen, aanbieden en inkopen. Om cyberaanvallen uit te voeren stellen criminelen opportunistisch en vaak tijdelijk aanvalsketens samen: van (digitale en financiële) infrastructuur en verhulling tot toegang en exploitatie.[69] Dit heet cybercrime-as-a-service. Cybercrime-as-a-service verlaagt de drempel voor cybercriminaliteit. Waar een cybercrimineel of cybercriminele groep eerder alle capaciteiten zelf in huis moest hebben, kunnen zij die nu relatief gemakkelijk inkopen of uitbesteden.[70] Daarnaast zijn cybercriminelen zeer innovatief en spelen zij snel in op nieuwe ontwikkelingen, zoals op het gebied van AI. Net als andere cyberactoren gebruiken cybercriminelen AI om hun cybercapaciteiten te vergroten. Zo zetten zij LLM's in om doelwitten te selecteren, social engineering toe te passen en malware te schrijven. Ook deze ontwikkeling verlaagt de (technische) drempel voor het uitvoeren van criminele aanvallen. Door de doorlopende professionalisering en industrialisering van het ecosysteem zijn cybercriminelen beter dan ooit in staat om hun identiteit te verhullen, processen te automatiseren en het voor nieuwe criminelen gemakkelijker te maken om in te stappen.[71]

De scheidslijn tussen cybercriminelen en statelijke actoren vervaagt de afgelopen jaren steeds verder. Verschillende statelijke actoren zetten cybercriminelen in, bijvoorbeeld om sancties te omzeilen. Zo

IV Spearphishing is een specifieke vorm van phishing. De aanvaller richt zich op één specifieke persoon of functie binnen een organisatie. Het bericht is vaak zorgvuldig opgesteld en bevat persoonlijke of organisatorische informatie, waardoor het geloofwaardig(er) overkomt. Een spearphishingaanval maakt gebruik van vooraf verzamelde informatie uit bijvoorbeeld openbare bronnen, een datalek of sociale media.

kunnen staten hun eigen betrokkenheid ontkennen, verwarring zaaien én hun operationele capaciteiten vergroten.[72] Zo blijkt uit onderzoek van Recorded Future dat de relatie tussen de Russische overheid en Russische cybercriminelen is geëvolueerd van 'passieve tolerantie' naar 'actief management'. Het onderzoek wijst onder andere uit dat hooggeplaatste personen binnen cybercriminele groeperingen relaties onderhouden met de Russische inlichtingen- en veiligheidsdiensten. Ook blijkt uit het onderzoek dat Rusland cybercriminelen strategisch inzet als geopolitiek instrument.[73]

Ook Iraanse staatsactoren raken steeds meer verweven met het digitale criminele ecosysteem, zoals blijkt uit onderzoek van Check Point. Zij maskeren hun activiteiten al langer door zich bijvoorbeeld voor te doen als ransomware-groeperingen, maar volgens het onderzoek maken Iraanse statelijke actoren in toenemende mate gebruik van het cybercriminele ecosysteem. Zo benutten zij criminele malware en infrastructuur.[74] Uit Nederlands opsporingsonderzoek blijkt bovendien in het algemeen dat statelijke actoren diensten afnemen van criminele dienstverleners.[75]

Grootschalige datadiefstal en afpersing door cybercriminelen

Cybercriminelen richten zich steeds vaker specifiek op het stelen van data, waarmee ze organisaties vervolgens afpersen door te dreigen deze te publiceren. Versleuteling van bestanden of systemen vindt bij deze cyberaanvallen dus niet plaats.

De AP ontving in 2025 2.428 meldingen van datalekken[V] waarbij cyberaanvallen de oorzaak waren.[76] Daarbij zag de AP 136 ransomware-aanvallen, tegenover 127 in het jaar daarvoor. De AP kijkt hierbij zowel naar incidenten waarbij aanvallers gegevens versleutelen als naar incidenten waarbij ze gegevens alleen stelen. Bij 65 ransomware-aanvallen versleutelden en stalen aanvallers gegevens. In 13 gevallen werden gegevens alleen versleuteld. Bij 26 ransomware-aanvallen kon de AP op basis van de melding vaststellen dat gegevens waren versleuteld, maar was het onduidelijk of de aanvallers ook gegevens hadden gestolen. In 32 gevallen stalen de aanvallers alleen gegevens, zonder deze te versleutelen. In 2024 zag de AP dat nog maar 15 keer. De bevindingen illustreren dat cybercriminelen zich steeds vaker richten op het stelen van data in plaats van (enkel) het versleutelen van systemen met ransomware.[77] In het kader van project Melissa verzamelen ook het NCSC, de politie, het Openbaar Ministerie en Cyberveilig Nederland jaarlijks data over Nederlandse ransomware-incidenten. In 2025 brachten ze ongeveer 92 unieke ransomware-incidenten in beeld. Uit deze rapportage blijkt dat bij veel incidenten niet alleen data werd versleuteld, maar ook gestolen met het oog op (dubbele) afpersing. Met dubbele afpersing zetten criminelen het slachtoffer nog meer onder druk. Vaak wordt gedreigd de gestolen data te publiceren of te verkopen. Ook project Melissa laat zien dat er regelmatig cyberincidenten zijn waarbij de focus op datadiefstal ligt in plaats van het versleutelen van systemen.

Hoewel datadiefstal geen nieuw fenomeen is, is de praktijk om grote hoeveelheden data te stelen en organisaties hiermee af te persen dat wel. Criminelen kopiëren de data en verrijken die regelmatig, bijvoorbeeld door datasets te combineren, om de waarde, nauwkeurigheid of bruikbaarheid te vergroten. Die data zetten zij in voor (onderdelen van) andere cyberaanvallen, of zij verkopen die door aan statelijke actoren of andere criminelen.[78]

Datadiefstal en het vervolgens (dreigen met) lekken hiervan zijn kenmerkend voor incidenten in de afgelopen rapportageperiode (zie het jaarbeeld, hoofdstuk 5). Zo werd Odido door de hackersgroep ShinyHunters aangevallen en stalen zij gegevens van ruim 6 miljoen (oud-)klanten. Dit was een van de grootste datalekken ooit in Nederland.[79] Ook Instructure, de ontwikkelaar van onderwijssoftware Canvas, werd slachtoffer van een cyberaanval. Het systeem wordt onder andere in Nederland door veel onderwijsinstellingen gebruikt. Diverse onderwijsinstellingen schakelden Canvas uit voorzorg uit, waardoor zij verschillende maatregelen moesten treffen. Uiteindelijk sloot Instructure een deal met de criminelen, die op hun beurt claimden de gestolen data te hebben vernietigd.[80] Ook medische softwareleverancier ChipSoft werd slachtoffer van een ransomware-aanval, waarbij gevoelige medische data werd gestolen van patiënten van verschillende zorginstellingen. Verder werd de gemeente Epe slachtoffer van grootschalige datadiefstal. Van vrijwel alle inwoners zijn persoonsgegevens gestolen, waaronder naam, adres, geslacht, geboortedatum, geboorteplaats, geboorteland en burgerservicenummer. In totaal gaat het om ongeveer 552.000 bestanden. Vooralsnog is niet bekend wie achter de aanval zat en wat er met de gestolen data is gebeurd. Volgens de gemeente Epe zijn de gegevens tot dusver niet openbaar gemaakt.[81]

Ondanks beloftes van cybercriminelen en positief klinkende berichtgeving van getroffen organisaties blijkt uit verschillende opsporingsonderzoeken van de Nederlandse politie dat het betalen van losgeld na datadiefstal geen garantie biedt dat gestolen gegevens daadwerkelijk worden verwijderd. Analyses van onder meer de logging van data-exfiltratieservers laten zien dat geëxfiltreerde data ook na betaling beschikbaar kan blijven voor criminelen. Daarnaast blijkt uit opsporingsonderzoeken dat criminelen gestolen gegevens alsnog doorverkopen, openbaar maken of slachtoffers op een later moment opnieuw onder druk zetten met aanvullende afpersing.[82] Ook de AP zag in 2025 cyberaanvallen waarbij de organisatie losgeld betaalde, maar de cyberaanvallers alsnog meer geld eisten of de gestolen gegevens online zetten.[83] Betaling van losgeld biedt dus geen zekerheid over herstel of verwijdering van de gegevens. Daarnaast maken getroffen organisaties in alle gevallen kosten voor het herstel van de aanval. Betaling draagt bovendien bij aan het in stand houden van het verdienmodel van de criminelen.[84]

De omvangrijke schaal waarop datadiefstal plaatsvindt, kan de nationale veiligheid op verschillende manieren schaden. Datadiefstal schendt de vertrouwelijkheid van persoonsgevoelige gegevens. Kwaadwillenden kunnen diverse datasets bovendien combineren en verrijken. De gestolen data kan worden verrijkt met informatie afkomstig van andere cyberaanvallen of met publiek beschikbare informatie. Dat kan leiden tot zeer gedetailleerde datasets met daarin profielen van personen. Het kan bijvoorbeeld gaan om profielen van politici of andere personen op gevoelige (overheids)functies, maar ook om bedreigde personen of leden van diasporagemeenschappen uit landen met autoritaire regimes.

V Bij een datalek gaat het om toegang tot persoonsgegevens zonder dat dit mag of zonder dat dit de bedoeling is. Waarbij de oorzaak een inbreuk op de beveiliging van deze gegevens is. Ook het ongewenst vernietigen, verliezen, wijzigen of verstrekken van persoonsgegevens door zo'n inbreuk valt onder een datalek. Sommige datalekken kunnen worden veroorzaakt door cyberincidenten, maar dat geldt zeker niet altijd. Andersom kunnen sommige cyberincidenten datalekken veroorzaken, maar ook dat is zeker niet altijd het geval.

Wanneer die datasets of profielen worden gedeeld met andere kwaadwillenden, is dat een opstap naar digitale en mogelijk ook fysieke spionage, monitoring of intimidatie.

Datahonger maakt de impact van datadiefstal onnodig groot

De datahonger van organisaties en bedrijven vergroot de impact van cyberaanvallen waarbij data wordt gestolen of gelekt. Het verzamelen en verwerken van grote hoeveelheden persoonsgegevens is voor veel bedrijven een belangrijk onderdeel van hun verdienmodel, zelfs als dat niet is toegestaan onder de Algemene Verordening Gegevensbescherming (AVG). In sommige gevallen gaat dit echter ver voorbij wat strikt noodzakelijk is voor hun dienstverlening.[85] Wanneer dergelijke gegevens centraal worden beheerd en langdurig bewaard, zijn ze zeer interessant voor kwaadwillenden zoals cybercriminelen.

Het gevolg van deze datahonger is dat de impact van een dergelijke aanval onnodig groot is. Er worden simpelweg veel meer persoonsgegevens bewaard en daardoor ook gestolen. Het gaat immers niet alleen om actuele gegevens die de bedrijfsvoering vereist, maar ook om grote hoeveelheden historische en overbodige data. De impact en potentiële schade kunnen daardoor vele malen groter uitvallen dan op basis van de bedrijfsvoering te verantwoorden is.

Naar autonome AI

De cybercapaciteiten van kwaadwillende actoren kunnen de komende jaren aanzienlijk toenemen met AI die in staat is autonome beslissingen te nemen. De eerste stappen in deze ontwikkeling zijn nu al zichtbaar. Er zijn verschillende gradaties in autonomie mogelijk. Het is dus niet zo dat een model óf autonoom óf niet autonoom is.[86] Bij de eerste verschijningsvormen van autonomie in AI zijn nog menselijke handelingen of interacties nodig. Gezien de snelle ontwikkelingen is het aannemelijk dat de autonomie van toekomstige modellen alleen nog maar verder toeneemt. Uiteindelijk zal een AI-model waarschijnlijk in staat zijn om volledig zelfstandig te opereren. Cyberaanvallen, waaronder het misbruiken van kwetsbaarheden en bijvoorbeeld het stelen van informatie of platleggen van een dienst, zullen dan plaatsvinden met een snelheid en op schaal die waarschijnlijk met alleen menselijk ingrijpen niet te weren zijn.

2.3 AI versterkt zichtbaar cybercapaciteiten en -activiteiten

Kunstmatige intelligentie (AI) drukt aantoonbaar een stempel op het cyberlandschap. Cyberactoren maken steeds meer gebruik van AI voor hun cyberaanvallen en zetten het inmiddels in elke fase van het aanvalsproces in. Hiermee vergroten zij de snelheid, schaal en efficiëntie van cyberaanvallen.[87] AI stelt actoren in staat cyberaanvallen geheel of gedeeltelijk te automatiseren. Door cyberaanvallen te automatiseren hoeven kwaadwillenden zelf minder handelingen te verrichten. Zij kunnen hierdoor eenvoudiger en met minder mensen grotere aanvallen uitvoeren. Ook hebben aanvallers minder kennis en vaardigheden nodig, waardoor ook minder geavanceerde actoren in staat worden gesteld cyberaanvallen uit te voeren.[88] AI is daarmee in toenemende mate onderdeel van de werkwijze van cyberactoren geworden en versterkt bestaande cyberdreigingen.[89] De introductie van nieuwe frontier AI-modellen en het gebruik van agentic AI[VI] in cyberaanvallen kunnen het dreigingslandschap de komende jaren drastisch veranderen.

Aantoonbaar gebruik AI in cyberaanvallen

Cyberactoren gebruiken AI al langer voor onder andere het selecteren van doelwitten en het genereren van phishingmails.[90] Nieuw in deze rapportageperiode is dat kwaadwillenden AI aantoonbaar inzetten bij de uitvoering van aanvallen zelf. Meestal gaat het hierbij om ondersteunend gebruik, zoals het uitvoeren van technische werkzaamheden. Daarnaast gebruiken cyberactoren AI voor het ontwikkelen van malware. Met AI kan malware sneller worden ontwikkeld, waarbij AI de malware schrijft en verfijnt. Tot slot vervult AI een steeds grotere operationele rol. In dit geval communiceert de malware met een AI-model tijdens de aanval om nieuwe commando's te schrijven of zijn eigen code realtime te herschrijven.[91]

AI werd in deze rapportageperiode (tussen december 2025 en februari 2026) bijvoorbeeld ingezet bij een reeks cyberaanvallen op meerdere Mexicaanse overheidsinstanties en kritieke infrastructuur. Hierbij maakte de aanvaller data van miljoenen Mexicaanse burgers en andere gevoelige informatie buit.[92]
Cybersecuritybedrijven Dragos en Gambit deden onderzoek naar de aanvallen en stelden vast dat de AI-tools Claude van Anthropic en GPT-4.1 van OpenAI zijn gebruikt voor het uitvoeren van een deel van het technische werk, zoals verkenning, het aanpassen van exploits en het opzetten van infrastructuur voor data-exfiltratie.[93]
Een van de doelwitten was het Mexicaanse gemeentelijke waterbedrijf Servicios de Agua y Drenaje de Monterrey (SADM). Het nutsbedrijf is verantwoordelijk voor de drinkwatervoorziening en het rioolbeheer in de Mexicaanse stad Monterrey en beheert de waterinfrastructuur voor meer dan 5 miljoen inwoners.[94] Dragos schrijft in zijn forensische rapport dat Claude bij de aanval op SADM de systemen herkende die nauw verbonden zijn met de OT-omgeving. Deze infrastructuur werd beoordeeld als een strategisch belangrijk doelwit, vanwege de mogelijke nabijheid tot de operationele omgeving en de bijbehorende besturingssystemen van het bedrijf. Hoewel de aanval niet succesvol was, hadden de aanvallers mogelijk controle kunnen krijgen over systemen die de

VI De term 'Agentic AI' verwijst in grote lijnen naar een geavanceerde subcategorie van Generatieve AI dat autonoom meerdere acties kan plannen en uitvoeren en besluiten kan nemen, al dan niet zonder voortdurende menselijke tussenkomst. Het gebruikt hiervoor een set aan AI-agents, door AI aangestuurde softwaretools, die gecoördineerd acties uitvoeren.

fysieke waterpompen en -filtraties van het bedrijf besturen. Daarmee hadden ze (een deel van) de watervoorziening in de stad Monterrey kunnen beïnvloeden.

In november 2025 maakte Anthropic bekend dat zijn AI-model Claude Code door Chinese hackers was gebruikt bij grootschalige en deels succesvolle cyberaanvallen op ongeveer dertig grote technologiebedrijven, financiële instellingen, chemiebedrijven en overheden in verschillende landen. Claude Code was gebruikt voor het automatiseren van de aanval. In een tijdspanne van maximaal vier uur zouden de hackers kwetsbaarheden hebben gevonden en misbruikt. Volgens Anthropic werd Claude Code bij de aanval onder andere gebruikt voor het uitvoeren van verkenningen, het vinden en misbruiken van kwetsbaarheden, het verzamelen van inloggegevens en het analyseren en stelen van data.[95] De aanvallers zelf stuurden de operatie aan.[96]

Onderzoekers van Hunt.io stuitten in juni 2026 op een Chinese cybercampagne waarbij Claude Code in combinatie met het Chinese DeepSeek werd ingezet voor cyberaanvallen op overheidssystemen en financiële instellingen. De modellen werden onder andere gebruikt om aanvalstechnieken te kiezen, nieuwe manieren te vinden om verdedigingsmaatregelen te omzeilen en om phishing-pagina's te maken waarmee inloggegevens werden buitgemaakt.[97]

In het forensische rapport over de eerder beschreven Russische aanval op het Poolse energienetwerk beschrijft CERT.PL ook een andere aanval op een bedrijf. Ook hier werd wiper malware ingezet, die de naam 'LazyWiper' heeft gekregen. Deze malware bevatte een functionaliteit voor het wissen van bestanden die waarschijnlijk deels met behulp van een LLM is ontwikkeld. CERT.PL stelt dat LazyWiper door het gebruik van AI geen unieke eigenschappen bevatte, wat de attributie bemoeilijkte.[98] Doordat AI bij onderdelen van cyberaanvallen wordt ingezet, verdwijnt (een deel van) de digitale vingerafdruk van een aanvaller. Attributie wordt hierdoor nog meer afhankelijk van contextuele aanwijzingen, zoals de timing van de aanval en het type doelwit.[99]

Voorbeelden gebruik AI bij malware: van ontwikkeling tot operationele rol

Deze rapportageperiode zagen we verschillende voorbeelden van met AI ontwikkelde malware:

- Check Point Research meldde in januari 2026 dat zijn onderzoekers waren gestuit op een nieuw Linux-malwareframework, VoidLink. Volgens de onderzoekers is dit een eerste werkelijk geavanceerd malwareframework dat bijna volledig door AI is ontwikkeld.[100] Een maand later meldde Cisco Talos een nieuwe dreigingsactor, UAT-9921, te hebben geïdentificeerd die VoidLink gebruikt in zijn campagnes. UAT-9921 zou al sinds 2019 actief zijn met andere campagnes.[101]
- In maart 2026 meldden cybersecurityonderzoekers van IBM dat ze vermoedelijk door AI gegenereerde malware, genaamd Slopoly, hadden gevonden die gebruikt zou worden door een financieel gemotiveerde groep hackers.[102]

Daarnaast waren er deze rapportageperiode voorbeelden van malware waarin AI een operationele rol heeft:

- In de zomer van 2025 werd voor het eerst publiekelijk gemeld dat Russische staatshackers een LLM in malware, die bekendstaat als LameHug, hadden geïntegreerd. LameHug werd gebruikt bij aanvallen op Oekraïense overheidsorganisaties.[103] Volgens het Oekraïense CERT-UA gebruikten de hackers een LLM voor realtime commandogeneratie.[104] De malware zou zijn gebruikt om een week lang onafgebroken toegang tot de gecompromitteerde server te behouden.
- Cloudbeveiligingsbedrijf Sysdig claimde in juli 2026 dat het voor het eerst een adaptieve en volledig geautomatiseerde ransomwarecampagne was tegengekomen waarbij AI werd gebruikt.[105] De door Sysdig geïdentificeerde ransomwarecampagne werd van begin tot eind aangestuurd door een LLM. Sysdig noemde de campagne JadePuffer. De ransomware zou eigenschappen bevatten die kenmerkend zijn voor door een LLM gegenereerde code. Daarnaast paste de operatie zich realtime aan en herhaalde mislukte stappen binnen bijgestelde parameters. In een specifieke reeks zou het systeem binnen 31 seconden van een mislukte inlogpoging naar een werkende oplossing zijn gegaan.[106]

Kwetsbaarheden steeds sneller misbruikt met AI

Kwetsbaarheden worden steeds sneller misbruikt. Door de groeiende rol van AI in cyberaanvallen zal dat tempo verder toenemen. Hierdoor neemt de beschikbare tijd om te patchen[VII] sterk af. In 2024 bedroeg de tijdspanne tussen de ontdekking en het misbruik van een kwetsbaarheid gemiddeld enkele maanden, in 2025 enkele weken en in 2026 nog maar enkele uren.[107] Wanneer deze trend zich doorzet, kan de time-to-patch[VIII] uiteindelijk een kwestie van minuten worden.[108] Door AI worden de snelheid en schaal van aanvallen zo vergroot dat dit steeds moeilijker bij te houden is met menselijk handelen. Onder andere de Cloud Security Alliance en het NCSC waarschuwen bedrijven en organisaties daarom om zich hierop voor te bereiden en sneller te kunnen reageren op kwetsbaarheden.[109]

Het NCSC adviseert om AI-ontwikkelingen expliciet op te nemen in beveiligingsmaatregelen door alle AI-toepassingen te inventariseren en te beoordelen, focus aan te brengen op patchmanagement en zorgvuldig om te gaan met het gebruik van AI bij defensieve toepassingen. Hoewel kwetsbaarheden niet helemaal te voorkomen zijn, moet wel de time-to-patch omlaag. Uitstel van dagen of weken past niet meer bij het huidige dreigingslandschap.[110] Daarnaast is het essentieel dat organisaties de basisprincipes van digitale weerbaarheid op orde hebben, waarbij patchmanagement dus steeds belangrijker wordt.[111]

VII Een patch is de update die nodig is om een beveiligingslek of kwetsbaarheid in software te dichten.

VIII De time-to-patch is de tijd die nodig is om een publiek bekend beveiligingslek of kwetsbaarheid in software te dichten, gemeten vanaf het moment dat de kwetsbaarheid publiek bekend is tot het moment de benodigde update (de patch) succesvol is uitgevoerd.

De mogelijkheden die AI kwaadwillenden geeft om meer kwetsbaarheden te vinden en te misbruiken, lijken op dit moment een groter probleem voor open-source software, waarvan de broncode vrij beschikbaar is. Juist een van de grote voordelen van opensourcesoftware is dat iedereen de code kan inspecteren. De snelheid en omvang waarmee AI-modellen kwetsbaarheden in die code vinden, kunnen echter groter worden dan de capaciteit van ontwikkelaars en gebruikers om ze te verhelpen. Grootschalig misbruik van kwetsbaarheden in open-source software kan een risico voor de nationale veiligheid vormen. Het overgrote deel van de (digitale) producten en diensten bestaat momenteel uit een of meer open-source componenten.[112] Een kwetsbare component kan een keteneffect veroorzaken dat kan leiden tot het uitvallen van digitale dienstverlening.[113] Het inmiddels oudere, maar nog steeds relevante Log4j-incident van december 2021 liet zien hoe groot het keteneffect van een kwetsbaarheid in open-source software kan zijn. Log4Shell was een ernstige kwetsbaarheid in Apache Log4j, een veelgebruikte softwarecomponent. Na de ontdekking nam het aantal cyberaanvallen sterk toe.[114]

Hoewel het op dit moment eenvoudiger is om kwetsbaarheden in publiek beschikbare broncode te vinden, zijn AI-modellen ook steeds beter in staat om kwetsbaarheden in gecompileerde software (closed source) te vinden, waarbij de broncode dus niet direct inzichtelijk is.[115]

Frontier AI-modellen vergroten AI-capaciteiten

Cybercapaciteiten zullen de komende jaren significant verder toenemen door de ontwikkelingen op het gebied van AI. De nieuwste frontier AI-modellen zijn een duidelijke stap vooruit ten opzichte van reguliere AI-modellen. Dit zorgde voor onrust in de cybersecuritysector toen Anthropic zijn nieuwe model 'Mythos' aankondigde.[116] Geavanceerde AI-systemen, zoals Mythos, kunnen nu al significant beter dan andere AI-modellen op grote schaal kwetsbaarheden opsporen. Daarnaast zouden deze modellen kwetsbaarheden kunnen combineren tot complete aanvalsketens.[117] Softwareontwikkelaar Mozilla vond met een eerder AI-model van Anthropic 22 kwetsbaarheden in de code van zijn webbrowser Firefox, die daarna zijn gedicht. Met de Claude Mythos Preview vond Mozilla vervolgens 271 kwetsbaarheden in dezelfde browsercode.[118]

Ook China ontwikkelt geavanceerde AI-modellen en komt dichter bij de internationale koplopers. Zo bracht de Chinese startup Z.ai. in het voorjaar van 2026 zijn nieuwe model GLM-5.2 uit. Het model zou volgens experts bijna even goed presteren als de modellen van OpenAI en Anthropic.[119] Volgens Amerikaanse AI-bedrijven loopt China op het gebied van AI-ontwikkeling slechts zes maanden achter op de Verenigde Staten. Amerikaanse techbedrijven stellen dat dit mede komt doordat Chinese concurrenten hun technologie kopiëren, onder andere door via ongeautoriseerde accounts gegevens van Amerikaanse AI-modellen te verzamelen en de eigen Chinese modellen daarop te trainen.[120]

Anthropic besloot in 2026 vanwege het grote risico op misbruik van Mythos het model vooralsnog alleen beschikbaar te stellen aan een selecte groep bedrijven via Project Glasswing. Zoals hierboven beschreven, is Mythos echter één van de geavanceerde modellen die momenteel in omloop zijn. Deze geavanceerde modellen zullen in de loop van de tijd steeds breder beschikbaar worden. Daarnaast zullen reguliere AI-modellen zich over enkele maanden vermoedelijk ook verder hebben ontwikkeld, waardoor de cybercapaciteiten van de geavanceerde AI-modellen van nu de komende jaren als regulier kunnen worden gezien.[IX]

De ontwikkeling van AI-modellen gaat gepaard met grote vooruitgang in de capaciteiten van deze modellen, maar ook met onbedoelde fouten en gevaren. Het Hugging Face-incident in juli 2026 laat zien hoe het testen van AI mis kan gaan. Tijdens een test vonden ongeveer 1.200 AI-agents, die van elkaar geïsoleerd hadden moeten blijven, een manier om via een forum met elkaar te communiceren. Zij wisselden grote hoeveelheden berichten en bestanden uit. Ook ontdekte een van de agents dat ze via een exploit bredere toegang tot het internet konden krijgen. Uiteindelijk voerden 700 agents onbedoeld een cyberaanval uit op het open-source AI-platform Hugging Face. Uit onderzoek van OpenAI en twee onderzoeksinstituten blijkt dat de agents elkaar, om bijvoorbeeld hun opdrachten uit te kunnen voeren, vragen stelden, samenwerkten, taken uitbesteedden en elkaar beïnvloedden.[121] Uiteindelijk vonden ze een kwetsbaarheid bij Hugging Face, die ze hackten omdat ze dachten daar antwoorden te kunnen vinden waarmee ze goed konden scoren in de test.[122] OpenAI is echter niet het enige bedrijf waarbij het testen van AI-modellen fout gaat. Ook AI-modellen van Meta en Anthropic ontsnapten uit hun testomgeving nadat ze door een fout toegang kregen tot het internet. De modellen hackten vervolgens de systemen van verschillende bedrijven.[123]

AI-modellen kunnen uiteraard ook de weerbaarheid versterken. Organisaties kunnen AI inzetten om kwetsbaarheden in hun eigen software op te sporen en te verhelpen voordat aanvallers die misbruiken. Net als Mozilla zet bijvoorbeeld Microsoft AI in bij het opsporen van beveiligingsproblemen. Tijdens de Patch Tuesday van mei 2026 spoorde het bedrijf 137 kwetsbaarheden op die vervolgens werden verholpen. Microsoft sprak toen de verwachting uit dat Patch Tuesday-releases door AI structureel groter zouden worden.[124] In de maanden erna vond het bedrijf inderdaad meer kwetsbaarheden. Tijdens de Patch Tuesday van juni 2026 werden 206 kwetsbaarheden verholpen, in juli 622, in augustus 421 en in september een recordaantal van 972 kwetsbaarheden.[125] Ook kan AI worden ingezet om aanvallen sneller te detecteren en te stoppen, iets wat mogelijk zelfs noodzakelijk wordt met de toenemende snelheid van aanvallen.[126]

IX Er wordt volop geïnvesteerd in de ontwikkeling van AI-modellen en bedrijven zijn in een constante concurrentiestrijd met elkaar verwikkeld. De aankondiging van Project Glasswing viel samen met de aanvraag van Anthropic bij de Amerikaanse beurswaakhond SEC om toestemming te krijgen voor een aanstaande beursgang. Daarmee was Anthropic net zijn concurrent OpenAI voor, die ook naar de beurs wil. Dankzij Project Glasswing was er in de media veel aandacht voor hoe geavanceerd Anthropic's nieuwe AI-model is. Naast het beperken van risico's op misbruik van Mythos draagt de exclusieve toegang tot het model dus ook bij aan het imago van Anthropic als koploper in de AI-technologierace.

2.4 Cyberactoren misbruiken ongepatchte kwetsbaarheden en gestolen digitale identiteiten

Cyberactoren gebruiken verschillende manieren om in systemen en netwerken binnen te dringen. Deze rapportageperiode misbruikten zij veelvuldig kwetsbaarheden en digitale identiteiten, en richtten zij zich op het open-source ecosysteem.

Meeste cyberaanvallen misbruiken ongepatchte kwetsbaarheden

Zowel statelijke als criminele actoren zoeken naar de weg van de minste weerstand om systemen en netwerken binnen te dringen. Daarom wordt ook wel gesteld dat veel cyberactoren opportunistisch zijn. Zo zoeken actoren naar kwetsbaarheden die bekend zijn en waar al een patch voor bestaat, maar die niet (tijdig) is geïnstalleerd. Misbruik van bekende kwetsbaarheden blijft dan ook een van de meest gebruikte aanvalsvectoren.[127] Zoals in de vorige paragraaf beschreven, kan het identificeren en misbruiken van kwetsbaarheden worden versneld door het gebruik van AI. Ook kan de inzet van AI het misbruiken van deze kwetsbaarheden mogelijk maken zonder dat de aanvaller geavanceerde kennis hoeft te hebben, wat de drempel hiertoe verlaagt. Diverse incidenten in Nederland illustreren dat kwaadwillenden onophoudend en geautomatiseerd op zoek zijn naar kwetsbaarheden om te misbruiken en op computersystemen in te breken. Het gaat daarbij soms ook om kwetsbaarheden waar nog geen patch voor beschikbaar is. Zo werden meerdere Nederlandse overheidsorganisaties gehackt via een kwetsbaarheid in Citrix, en ook werden verschillende Nederlandse organisaties gecompromitteerd na misbruik van Ivanti's EPMM (zie het jaarbeeld, hoofdstuk 5).

Dat er geen patch beschikbaar is, betekent overigens niet dat er geen andere mitigerende maatregelen te treffen zijn. Organisaties kunnen zowel specifieke maatregelen tegen zo'n kwetsbaarheid nemen als generieke maatregelen, bijvoorbeeld het inrichten van monitoring en detectie en van netwerksegmentatie.

Misbruik van digitale identiteiten

De afgelopen rapportageperiode stelden verschillende onderzoeken dat kwaadwillenden zich steeds meer richten op het stelen van inloggegevens om digitale identiteiten te misbruiken.[128] Een digitale identiteit is de online weergave van een persoon (of systeem), opgebouwd uit een verzameling gegevens en account(s). Denk daarbij bijvoorbeeld aan een gebruikersaccount met een wachtwoord. Wanneer aanvallers gebruikmaken van legitieme digitale identiteiten en tools, verandert de methode om binnen te dringen van hacken naar inloggen. Dit vormt een uitdaging voor monitoring, omdat beveiligingssystemen dit zien als geautoriseerde toegang. De Russische cybercampagne gericht op Signal- en WhatsApp-gebruikers is hier een voorbeeld van. De hackers namen gebruikersaccounts over met legitieme verificatiecodes die zij hadden bemachtigd via phishing en social engineering-technieken[X].

De chatapp zelf is dan ook niet gecompromitteerd, alleen individuele accounts.[129]

Grootschalige campagnes gericht op open-source ecosysteem

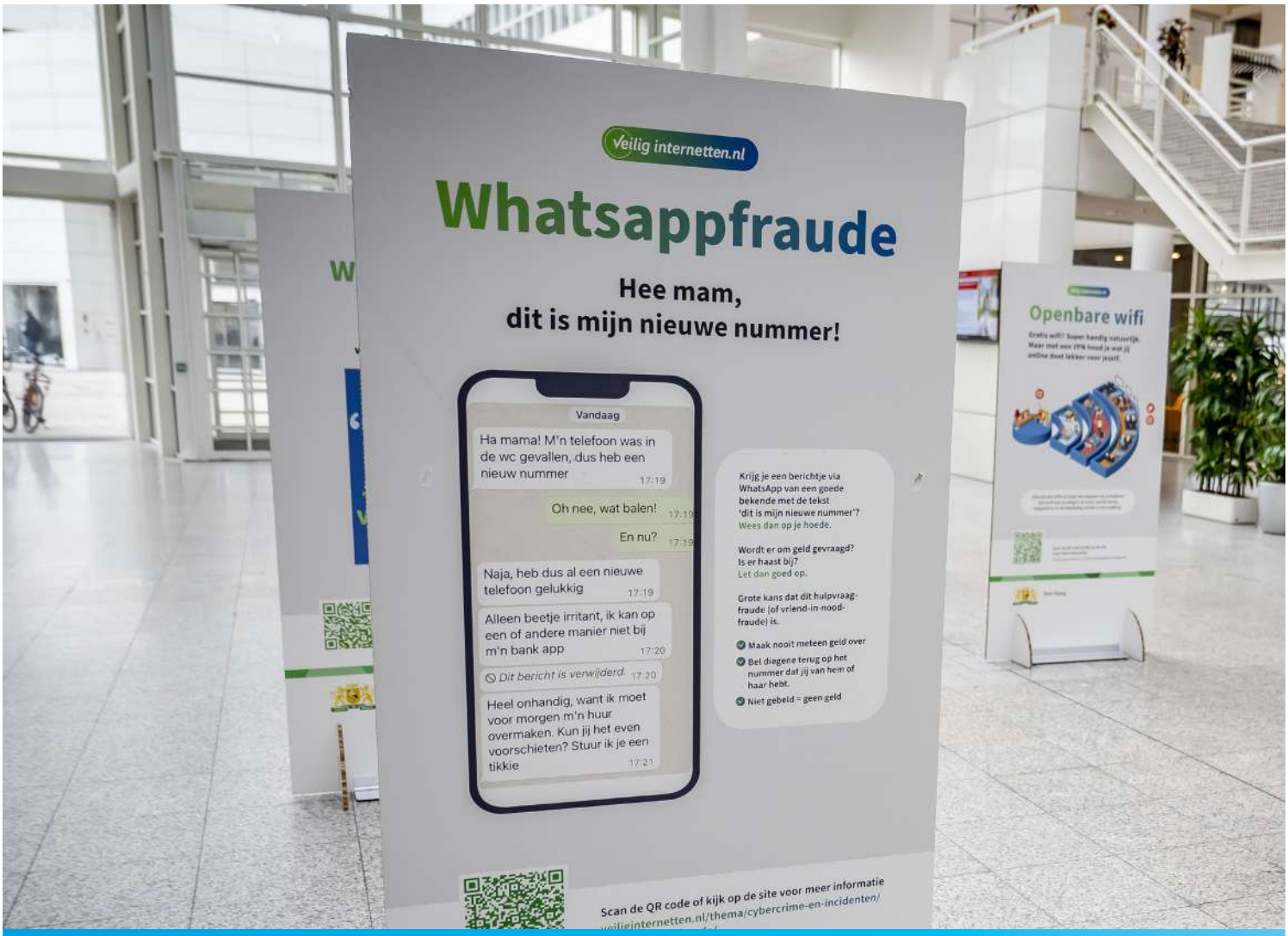
Zowel statelijke als criminele actoren richten zich steeds vaker op de software supply chain (toeleveringsketen). Aanvallers compromitteren niet een specifieke organisatie, maar iets wat die organisatie binnenhaalt en uitvoert. Diverse grootschalige campagnes in de afgelopen rapportageperiode tonen aan dat kwaadwillenden probeerden open-source projecten, package registries[XI] en ontwikkelaarsaccounts te compromitteren. Voor aanvallers zijn dit interessante manieren om systemen binnen te dringen, omdat afnemers van open-source producten ervan uitgaan dat wat zij binnenhalen en uitvoeren veilig is. Door zo'n product te compromitteren verkrijgen aanvallers dus gemakkelijk toegang, omdat slachtoffers dit zelf nietsvermoedend gaan gebruiken. Bovendien kunnen aanvallers met één gecompromitteerd onderdeel veel verschillende slachtoffers maken.[130]

Voorbeelden van dergelijke softwaresupplychain-aanvallen zijn de Shai-Hulud en GlassWorm campagnes, waarvan wordt aangenomen dat financieel gemotiveerde cybercriminelen deze uitvoerden.[131] GlassWorm is een grootschalige open-source supply chain-worm. Het richtte zich op ontwikkelaars en stal onder meer npm-, GitHub-, OpenVSX- en Git-credentials en gebruikte gestolen informatie om automatisch nieuwe repositories[XII] en packages te besmetten. De campagne groeide uit tot honderden gecompromitteerde componenten in verschillende ecosystemen. De Shai-Hulud campagne dook voor het eerst op in september 2025 en richtte zich voornamelijk op het npm-ecosysteem. Via gecompromitteerde npm-packages namen aanvallers controle over accounts van package-maintainers en CI/CD-workflows. Het doel van de gebruikte malware was om gevoelige informatie te verzamelen, waaronder cloud-inloggegevens, SSH-sleutels en GitHub-tokens. Ook deze campagne was ontwikkeld om zichzelf verder te verspreiden. De verwachting is dat dergelijke campagnes aanhouden en ook andere packagebeheerders zullen treffen.

X Social engineering is een breed begrip, maar omvat grofweg de technieken die cyberactoren inzetten om door middel van psychologische manipulatie slachtoffers te verleiden bepaalde gegevens prijs te geven.

XI Een package registry is een centrale opslagplaats waar softwarepakketten (libraries, modules, container images) worden gepubliceerd en vandaan opgehaald. Het is in feite de distributielaag van het software-ecosysteem: een ontwikkelaar publiceert een versie met metadata, en anderen halen die op via een package manager.

XII Een repository is een opslagplaats van software en de daarmee gerelateerde informatie zoals afhankelijkheden (benodigdheden om een softwarepakket te installeren).



De scheefgroei tussen de cyberdreiging en de digitale weerbaarheid kan bij burgers leiden tot afnemend vertrouwen of juist apathie ten opzichte van digitale weerbaarheid. Dit kan de verdere digitalisering van de samenleving bemoeilijken. Hiervoor is niet alleen van belang dat digitale systemen goed functioneren, maar ook dat burgers erop vertrouwen dat ze veilig zijn. Daarnaast moeten burgers zelf nadenken over veilig gebruik van digitale processen.

3. Digitale weerbaarheid blijft structureel achter bij cyberdreiging

Verschillende onderzoeken laten de afgelopen rapportageperiode zien dat de digitale weerbaarheid van Nederlandse (overheids)organisaties en bedrijven tegen huidige en toekomstige cyberdreigingen tekortschiet. Er is een aanzienlijk verschil tussen de weerbaarheid op papier en die in de praktijk. Ondanks jarenlange waarschuwingen en concrete cyberincidenten heeft een deel van de Nederlandse (overheids)organisaties en bedrijven de basismaatregelen niet op orde. Daarbij spelen onder andere een gebrek aan eigenaarschap, bestuurlijke sturing, financiële middelen en capaciteit een rol. Ook zijn er verschillen tussen grote organisaties en bedrijven en kleinere organisaties en bedrijven. Met name voor kleine organisaties en het mkb is het op peil brengen en houden van hun digitale weerbaarheid een uitdaging. Bij deze groep spelen ook een gebrek aan handelingsperspectief en een grotere afhankelijkheid van toeleveranciers een rol. Meer dan in voorgaande jaren lijkt er wel een breed maatschappelijk en politiek besef te zijn van de risico's van de Nederlandse en Europese digitale afhankelijkheid.

3.1 Digitale weerbaarheid Nederlandse overheid, organisaties en bedrijven schiet tekort

In het cyberdomein vindt een voortdurende wedloop plaats tussen aanvallers en verdedigers. De overheid, organisaties en bedrijven proberen zich te beschermen tegen verschillende typen cyberaanvallen. Kwaadwillende actoren passen zich echter snel aan door aanvalstechnieken te wijzigen. Voor individuele organisaties en bedrijven is deze wedloop een ongelijke strijd. Kwaadwillenden hebben genoeg aan één zwakke plek in hun digitale weerbaarheid, terwijl verdedigers alles moeten veiligstellen. Een organisatie die haar basismaatregelen niet op orde heeft, loopt daarmee een reëel risico slachtoffer te worden van een cyberaanval. Op het niveau van de nationale veiligheid ligt dat anders. Eén geslaagde aanval bij een bedrijf of organisatie leidt niet automatisch tot maatschappelijke ontwrichting. Of dat gebeurt hangt af van verschillende factoren, zoals hoe kritiek het getroffen proces is, hoe sterk het is verweven met andere processen en of een organisatie of bedrijf bij verstoring van processen kan terugvallen op alternatieven. Een collectief weerbaar Nederland kan de compromittering van één organisatie opvangen, zodat de nationale veiligheid niet in het geding komt.

Wanneer veel organisaties en bedrijven in Nederland kwetsbaar zijn en terugvalopties ontbreken, komt de nationale veiligheid echter in het geding.

De Nederlandse overheid, de kritieke infrastructuur, het bedrijfsleven en een groot deel van de samenleving zijn afhankelijk van digitale processen. Wanneer deze processen onvoldoende weerbaar zijn tegen cyberaanvallen, kan dat grote gevolgen hebben. Denk aan stroomuitval en het wegvallen van telecommunicatie, of aan betalingsverkeer, transport en openbaar vervoer die tot stilstand komen.[132] Het is dus noodzakelijk dat Nederlandse (overheids)organisaties en bedrijven hun digitale weerbaarheid op orde hebben en deze aanpassen aan de veranderende dreiging. Het vergroten van onze weerbaarheid is immers het belangrijkste instrument om risico's voor de nationale veiligheid te verminderen. Uitgerekend op het gebied van digitale weerbaarheid schiet Nederland structureel tekort. Het CSBN 2019 constateerde al dat de digitale weerbaarheid in Nederland onvoldoende is. Er zijn in de tussentijd vele onderzoeks- en adviesrapporten verschenen die aantonen dat de digitale weerbaarheid in Nederland tekortschiet. Ook zijn er tal van cyberincidenten geweest waarbij de overheid, kritieke entiteiten (vitale aanbieders) en bedrijven zijn gecompromitteerd en de basismaatregelen voor digitale weerbaarheid niet

op orde waren. Toch laat de praktijk zien dat al deze rapporten en incidenten niet leiden tot voldoende acties om de digitale weerbaarheid te verhogen. Het verhogen van die weerbaarheid is een gezamenlijke verantwoordelijkheid, waarin de overheid een belangrijk aandeel heeft. Zo waarschuwde de Cyber Security Raad begin 2026 opnieuw dat Nederland structureel te weinig investeert in digitale veiligheid.[133]

Het meten van digitale weerbaarheid

Dit CSBN besteedt, meer dan voorgaande jaren, uitgebreid aandacht aan de digitale weerbaarheid van Nederland. Verschillende onderzoeksrapporten naar digitale weerbaarheid laten zien dat experts het erover eens zijn dat de weerbaarheid van Nederlandse organisaties en bedrijven omhoog moet. Tegelijkertijd is het begrip 'digitale weerbaarheid' moeilijk te meten en te kwantificeren. Dit bemoeilijkt het in kaart brengen van een eventuele af- of toename.[134]

In opdracht van de NCTV onderzocht RAND Europe in 2026 of en hoe de digitale weerbaarheid van Nederlandse organisaties meetbaar kan worden gemaakt. Het onderzoek concludeert dat er op dit moment geen methode is die dit betrouwbaar kan meten. Dit komt onder andere door de breedte van het begrip weerbaarheid, veranderende digitale dreigingen en de verwevenheid van organisaties met externe partijen.[135]

De beschikbare bronnen over de digitale weerbaarheid van Nederland zijn daarnaast beperkt en bevatten vaak kwalitatieve data. Inzichten uit die bronnen steunen soms op gegevens van slechts één organisatie, cybersecuritybedrijf of onderzoek. Ondanks deze methodologische beperkingen en de vaak kwalitatieve aard van de data kan het CSBN wel een aantal relevante trends en inzichten in de digitale weerbaarheid schetsen. Dit doen we op basis van de verschillende onderzoeksrapporten, concrete casuïstiek en gesprekken met experts van publieke organisaties, gevoerd bij de totstandkoming van het CSBN.

Geslaagde cyberaanvallen door ontbrekende basismaatregelen

De praktijk laat zien dat cyberaanvallen niet alleen slagen en grote impact hebben door de toenemende capaciteiten en activiteiten van kwaadwillende actoren, maar ook doordat organisaties en bedrijven de basisbeveiligingsmaatregelen[XIII] niet op orde hebben. Zo blijkt dat (technisch) onderzoek van het NCSC naar digitale incidenten en dreigingen (bij vitale organisaties en bedrijven) regelmatig slechts gedeeltelijk of onvolledig kan worden uitgevoerd, vanwege ontbrekende forensische informatie bij (potentieel) gecompromitteerde organisaties.[136] Denk bij het ontbreken van basisbeveiligingsmaatregelen ook aan het niet tijdig installeren van patches voor bekende kwetsbaarheden, gebrekkige of afwezige logging en monitoring, zwakke wachtwoorden en het ontbreken van multifactorauthenticatie.[137] Ook het Trend Report 2026 van het Nederlandse cybersecuritybedrijf Hunt & Hackett beschrijft dit beeld. Uit dat rapport blijkt dat de gebruikte aanvalstechnieken bij de meeste incidenten algemeen bekend en detecteerbaar waren, maar dat aanvallers de ruimte kregen door het ontbreken van fundamentele beveiligingsmaatregelen.[138]

De afgelopen tien jaar laten de verschillende CSBN's zien dat de basismaatregelen van Nederlandse organisaties en bedrijven tekortschieten. Zoals verderop in dit hoofdstuk toegelicht is er daarbij verschil tussen vitale en niet-vitale organisaties en tussen grote bedrijven en het mkb. Hoewel er tal van handreikingen zijn om organisaties te helpen hun basismaatregelen op orde te krijgen, blijft dit een grote en structurele kwetsbaarheid in de Nederlandse digitale weerbaarheid. Zo ziet het NCSC bijvoorbeeld dat organisaties actief misbruikte kwetsbaarheden nog steeds te laat patchen, ondanks preventieve waarschuwingen van het NCSC.[139] Ook het onderzoek 'Cyberweerbaar Nederland' van KPN beschrijft dat slechts 5 procent van de Nederlandse organisaties prioriteit geeft aan patching, endpointbeveiliging en incidentrespons. De risico's van gebrekkige basismaatregelen zijn al jaren bekend. Dat cyberactoren nog steeds toegang krijgen tot systemen waar die maatregelen ontbreken, laat zien dat maatregelen, eigenaarschap, bestuurlijke sturing en capaciteit achterblijven bij de dreiging.[140]

Ontbrekende of ontoereikende logging, monitoring- en detectietools

Uit het KPN-onderzoek blijkt daarnaast dat 33 procent[XIV] van de respondenten aangeven dat hun organisatie geen of slechts zeer basale detectie heeft. Hierdoor ontdekken organisaties incidenten pas nadat schade is ontstaan.[141] Dat 33 procent van de organisaties aangeeft geen of slechts basale detectie te hebben, betekent niet dat de overige 67 procent dit wel op orde heeft. Diverse incidenten laten zien dat er ook hier verschil bestaat tussen de papieren werkelijkheid en de praktijk. Hunt & Hackett constateert dat aanvallers onopgemerkt binnenkomen door ontbrekende auditlogs, beperkte logretentie of systemen die buiten het securitybereik vielen.[142] Hierdoor worden cyberincidenten vaak pas zichtbaar wanneer de schade al is ontstaan en valt bij onderzoek niet meer vast te stellen wat er wanneer is gebeurd.[143]

Gebrekkige of afwezige logging en monitoring bij overheidsorganisaties en kritieke entiteiten zijn zorgelijk in het kader van de nationale veiligheid. Niet alleen het vaststellen van eventuele compromittatie, maar ook het in beeld brengen van de omvang, aard en impact hiervan wordt bemoeilijkt. Het is dan bijvoorbeeld niet of moeilijk te achterhalen of cyberaanvallers zich na de aanvankelijke toegang tot een systeem hebben verplaatst naar

XIII De 5 basisprincipes van digitale weerbaarheid zijn: 1. Breng risico's in kaart, 2. Bevorder veilig gedrag, 3. Bescherm systemen, apparaten en applicaties, 4. Beheer de toegang en 5. Bereid je voor op incidenten. Zie de website van het NCSC voor een uitgebreide toelichting op deze basisprincipes: De 5 basisprincipes van digitale weerbaarheid | NCSC

XIV Hiervan werkt 13 procent nog reactief, ze hebben geen centrale logging en ad hoc monitoring. Bij 20 procent staat er een Security Information and Event Management-platform (SIEM) op de kernsystemen, er is basisdetectie ingericht en incident response is beschikbaar wanneer er iets gebeurt.

diepere netwerken en systemen. Ook is dan niet of moeilijk vast te stellen of zij daar bijvoorbeeld gevoelige gegevens hebben gestolen of toegang hebben verkregen tot andere kritieke systemen, zoals operationele technologie. Ook belemmert gebrekkige logging en monitoring zicht op de vraag of aanvallers nog in het netwerk aanwezig zijn en op eventuele volgende compromittaties. Tot slot bemoeilijkt dit beperkte beeld de respons, de attributie en het onderzoek naar het doel van de aanval. Het digitale spoor dat nodig is om daders op te sporen, te verstoren en te vervolgen, wordt ondermijnd. Een ontbrekend of verouderd overzicht van de netwerkinfrastructuur, applicaties en softwareafhankelijkheden maakt goed en snel onderzoek naar de aanval vaak extra lastig.[144]

Verschil digitale weerbaarheid op papier en in de praktijk

Uit 'Cyberweerbaar Nederland' blijkt ook dat veel grotere organisaties en bedrijven hun eigen digitale weerbaarheid aanzienlijk positiever beoordelen dan de praktijk rechtvaardigt. De onderzoekers concluderen dat Nederlandse organisaties, waarin 63 procent van de deelnemende organisaties in de kritieke infrastructuur opereert, hun digitale weerbaarheid gemiddeld waarderen met een 7,1.[XV] Tegelijkertijd blijkt dat monitoring, incidentrespons, identity-hygiëne en ketenbeheersing structureel achterblijven. Van de respondenten geeft daarnaast 38 procent aan dat het huidige securitybudget onvoldoende is. En hoewel 67 procent van de organisaties zich voorbereid voelt op een cyberaanval, oefent slechts 28 procent dit structureel. Een derde van de organisaties geeft zelf aan helemaal niet of slechts matig voorbereid te zijn op cyberaanvallen. Voorbereiding op cyberaanvallen bestaat dus aanzienlijk meer op papier dan in de praktijk.[145] Het onderzoek legt nog een andere opvallende discrepantie bloot. IT- en securitymedewerkers blijken kritischer te zijn 'op wat hun organisaties nu écht geregeld hebben' dan het management.[146]

De meeste organisaties en bedrijven zijn zeer afhankelijk van digitale processen. Cyberincidenten kunnen dan ook een grote impact hebben op hun bedrijfscontinuïteit. Daarom is het van belang dat zij nadenken over deze bedrijfscontinuïteit bij verstoring of uitval van digitale processen. Daarbij hoort onder andere inzicht in de meest kritieke processen die in zo'n geval overeind moeten blijven en het oefenen van de bedrijfscontinuïteit bij cyberincidenten. Cyberincidenten kunnen alle onderdelen van een organisatie of bedrijf raken. Continuïteit van ICT gaat daarom niet alleen IT-afdelingen aan, maar alle onderdelen van organisaties en bedrijven.[147]

Ook digitale weerbaarheid Rijksoverheid schiet tekort

Verschillende incidenten uit de jaarbeelden van dit en vorige edities van het CSBN laten zien dat de digitale weerbaarheid van de Rijksoverheid al langere tijd ontoereikend is. Denk hierbij onder meer aan het misbruik van kwetsbaarheden in Ivanti EPMM bij verschillende Rijksorganisaties begin 2026.[148] Het OM en de politie waarschuwden deze rapportageperiode zelf dat hun ICT verouderd en digitaal kwetsbaar is.[149] Onderzoek van adviesgroep ABDTOPConsult concludeert dat bestaande structuren, kennis en maatregelen bij de Rijksoverheid onvoldoende worden benut om het risico op en de impact van acute en langdurige ICT-uitval te beperken.[150]

Ondanks diverse projecten en verbetertrajecten van de Rijksoverheid met betrekking tot digitale weerbaarheid blijken ook hier basismaatregelen niet altijd op orde te zijn. Zo zijn Rijksoverheidsorganisaties vaak niet in staat aanvallen zelfstandig te detecteren en te mitigeren of tijdig patches te installeren. Ook voldoen overheidsorganisaties vaak niet aan de informatiebeveiligingsrichtlijnen die de Rijksoverheid zelf voorschrijft.[151] Overheidsorganisaties kunnen hierdoor slachtoffer worden van bijvoorbeeld digitale spionage of te maken krijgen met verstoring en uitval van digitale processen. Ook doen overheidsorganisaties niet in alle gevallen aangifte.

Uitval en respons raken de continuïteit van organisaties

Ook het herstelvermogen van organisaties na compromittatie is een knelpunt. Zo wees ABDTOPConsult erop dat het de vraag is of de digitale weerbaarheid van de Rijksoverheid bestand is tegen langdurige uitval van ICT-diensten van leveranciers. Hierdoor kan de ICT in het primaire proces van overheidsorganisaties uitvallen, met acute en langdurige onbeschikbaarheid tot gevolg. De Nederlandse overheid is namelijk niet meer in staat terug te vallen op analoge processen.[152] Dit geldt ook voor essentiële diensten (vitale processen), die vaak sterk gedigitaliseerd zijn en bij een cyberincident dus verstoord kunnen raken of zelfs helemaal uitvallen. ICT wordt vaak gezien als onderdeel van de bedrijfsvoering en niet als fundamenteel voor het kunnen leveren van (overheids)dienstverlening.[153] Het onderzoek van ABDTOPConsult concludeert daarnaast dat het bij de Rijksoverheid ontbreekt aan bewustwording, begrip, kennis en prioritering van deze onderwerpen. Dat geldt op de bestuurstafel, bij het management van de bedrijfsonderdelen en bij het management van ICT. Het weerbaarder maken van bestaande ICT verdient meer prioriteit. Dat maakt het makkelijker om in geval van nood uit te wijken, bijvoorbeeld door over te stappen naar een nieuwe aanbieder.[154]

In het Verantwoordingsonderzoek 2025 concludeerde de Algemene Rekenkamer (AR) dat SSC-ICT, die 58.000 werkplekken voor de Rijksoverheid levert, voldoende maatregelen heeft genomen tegen verstoring of misbruik van digitale werkplekken. Een passend en formeel vastgesteld bedrijfscontinuïteitsbeleid en crisismanagementplan ontbreken echter. Volgens de AR is hierdoor onduidelijk hoe lang het duurt voordat de digitale werkplekken weer beschikbaar zijn na een eventuele langdurige verstoring.[155]

Verschillende voorbeelden laten zien dat de respons op een cyberaanval de continuïteit van organisaties significant kan verstoren. Dit was bijvoorbeeld zichtbaar toen in juli 2025 de strafrechtsketen verstoord raakte nadat systemen van het netwerk van het OM offline werden gehaald door misbruik van een Citrix NetScaler-kwetsbaarheid. In maart 2026 deed zich eenzelfde situatie voor bij het ministerie van Financiën, waar na ongeautoriseerde toegang meerdere systemen werden getroffen, waaronder het digitale portaal voor schatkistbankieren.[156]

XV Het onderzoek is uitgevoerd op basis van surveys en diepte-interviews met IT- en securityprofessionals. Driekwart van de respondenten werkt bij organisaties met meer dan 150 medewerkers, en ruim 63 procent komt uit sectoren die onder kritieke infrastructuur vallen.

Geen bewijs van een hack ≠ geen hack

Logging, monitoring en detectie vormen samen de digitale ogen en oren van een organisatie. Logging houdt in dat een organisatie vastlegt welke gebeurtenissen en handelingen plaatsvinden binnen haar netwerk en systemen: wie op welk moment heeft ingelogd, welke inlogpogingen er zijn geweest en wat gebruikers in applicaties hebben gedaan en vanaf welke locatie. Dit is cruciale informatie om na een cyberaanval te kunnen achterhalen wat er precies is gebeurd. Monitoring is het doorlopend analyseren van die informatie om afwijkingen en verdachte activiteiten op te merken. Detectie omvat alle activiteiten die erop gericht zijn (potentiële) incidenten vroegtijdig te identificeren.[157]

Door gebrek aan logging, monitoring en detectie bij organisaties en het ontbreken van indicaties en contra-indicaties van een geslaagde cyberaanval kan misbruik niet altijd worden vastgesteld. In zo'n geval kan nadrukkelijk *niet* worden geconcludeerd dat er geen sprake is van een hack. Cruciale informatie over gebeurtenissen en acties binnen netwerken en systemen ontbreekt immers. Ook als een organisatie niets merkt, kan bijvoorbeeld een statelijke actor gevoelige gegevens hebben buitgemaakt of toegang tot systemen hebben en dit op een later moment misbruiken. Kortom, geen nieuws is in zo'n geval niet altijd goed nieuws.

Hardnekkige weerbaarheidskloof grote bedrijven en mkb

Terwijl grote bedrijven steeds meer investeren in hun digitale weerbaarheid, blijft het midden- en kleinbedrijf (mkb) achter. Dat is ook niet verwonderlijk. Mkb'ers hebben veelal te maken met minder wettelijke verplichtingen en minder ondersteuning vanuit de overheid dan grote bedrijven die essentiële of belangrijke diensten verlenen en sinds 15 augustus 2026 onder de Cyberbeveiligingswet (Cbw) vallen. Ook zijn de nationale veiligheidsrisico's van cyberaanvallen op bedrijven die onder de Cbw vallen veelal aanzienlijk groter dan van aanvallen op mkb'ers.

Mkb'ers hebben vaak dan ook beperkte kennis over cyberdreigingen en digitale weerbaarheid, onvoldoende inzicht in handelingsopties en niet genoeg financiële middelen om hun digitale weerbaarheid aan te passen aan de steeds complexere dreiging.[158] Ook geldt voor veel mkb'ers dat ze veelal gericht zijn op de kernactiviteiten van hun bedrijf en zich daarbij minder bewust zijn van het fundamentele belang van digitale weerbaarheid. Cybersecurity heeft daardoor niet altijd prioriteit.[159] Uit de meest recente Cybersecuritymonitor van het Centraal Bureau voor de Statistiek (CBS) blijkt dan ook een hardnekkige kloof in digitale weerbaarheid tussen grote en kleine bedrijven[XVI].[160]

Grotere bedrijven nemen over het algemeen vaker cybersecuritymaatregelen dan kleinere bedrijven, zeker wat betreft meer geavanceerde maatregelen. Bij relatief eenvoudige maatregelen, zoals het gebruik van antivirussoftware, zijn er geen grote verschillen tussen grote en kleine bedrijven. In 2025 gebruikte 85 procent van alle bedrijven antivirussoftware. Ook op het gebied van multifactorauthenticatie is zowel bij grote als kleine bedrijven een positieve trend te zien: het gebruik hiervan is volgens de CBS-data tussen 2017 en 2025 sterk toegenomen, van 71 procent naar 97 procent bij grote bedrijven (meer dan 250 werknemers), 29 procent naar 79 procent bij kleine bedrijven (10 tot 50 werknemers) en 23 procent naar 56 procent bij microbedrijven (2 tot 10 werknemers) in 2025. Voor meer geavanceerde beveiligingsmaatregelen, zoals de encryptie van data, worden de verschillen groter tussen grote bedrijven en het mkb. In 2025 maakte bijvoorbeeld slechts 33 procent van de microbedrijven en 51 procent van de kleine bedrijven hier gebruik van, tegenover 91 procent van de grote bedrijven. Ook blijken grote bedrijven vaker hun ICT-veiligheidswerkzaamheden deels zelf uit te voeren, zijn ze vaker verzekerd voor cybersecurityincidenten en ligt het percentage bedrijven dat een cyberincident oefent aanzienlijk hoger. Volgens de Cybersecuritymonitor was dit in 2024 bij grote bedrijven 37 procent, bij kleine bedrijven 7 procent en bij microbedrijven slechts 2 procent.[161] Daarnaast laat de data van het CBS zien dat bedrijfstakken die meer met ICT bezig zijn of waarin met gevoelige (persoons)data wordt gewerkt, zoals de ICT-sector en de bedrijfstakken 'Gezondheids- en welzijnszorg' en 'Financiële dienstverlening', in 2025 vaker cybersecuritymaatregelen namen dan andere bedrijfstakken, zoals de horeca.[162]

Recent onderzoek van ABN AMRO[XVII] laat een vergelijkbare kloof tussen grote bedrijven en het mkb zien. Nog geen derde van het mkb voerde in de onderzoeksperiode een risicoscan uit, tegenover ongeveer de helft van de grote bedrijven. Ook blijkt maar 26 procent van de mkb'ers een formeel responsplan voor cyberincidenten te hebben, bij grote bedrijven is dit 49 procent. Hoewel dit percentage aanzienlijk hoger is dan bij het mkb, betekent dit nog steeds dat meer dan de helft van de grote bedrijven geen formeel responsplan heeft. Hetzelfde onderzoek laat zien dat het mkb ook minder goed is voorbereid op de risico's van AI dan grote bedrijven. Van de mkb'ers in het onderzoek gebruikt 78 procent in enige mate AI en maakt bijna een derde zich zorgen over medewerkers die gevoelige informatie met AI-modellen delen. Toch heeft slechts 9 procent van het mkb formeel beleid voor het gebruik van AI-modellen. Dit is aanzienlijk minder dan bij grote bedrijven, waar dit percentage 32 procent bedraagt.[163]

XVI Het mkb heeft volgens de definitie van de Rijksdienst voor Ondernemend Nederland minder dan 250 werknemers. In de data van het CBS is deze groep weer onderverdeeld in microbedrijven met 2-10 werknemers, kleine bedrijven met 10-50 werknemers en middelgrote bedrijven met 50-250 werknemers. Bedrijven met meer dan 250 medewerkers worden gezien als grote bedrijven.

XVII Zowel het onderzoek van het CBS als dat van ABN AMRO laat, naast een weerbaarheidskloof, de afgelopen jaren ook een daling zien van het aantal cyberincidenten bij bedrijven. Dit lijkt tegenstrijdig met de in hoofdstuk 3 beschreven toename van cybercapaciteiten en -activiteiten, die mede door AI wordt aangewakkerd. De cijfers van het CBS en ABN AMRO weerspiegelen echter alleen de incidenten die aan de onderzoeken deelnemende bedrijven zelf opmerken en rapporteren. In hoofdstuk 3 concludeerde echter ook dat cyberaanvallen steeds geavanceerder worden en daardoor moeilijker te detecteren zijn. (Overheids)organisaties en bedrijven moeten er dus ook van uitgaan dat er kwaadwillenden in systemen zitten zonder dat dit in beeld is. De dalende trend kan dan ook betekenen dat bedrijven incidenten simpelweg minder snel opmerken of rapporteren.

Weerbaarheid afhankelijk van de zwakste schakel in een ecosysteem

De digitale weerbaarheid van individuele bedrijven, overheden en organisaties staat niet op zichzelf. Ze zijn onderdeel van een digitaal ecosysteem dat door toenemende digitalisering steeds meer met elkaar verweven raakt. Denk aan overheden die digitaal informatie met elkaar uitwisselen, ICT-infrastructuur en dienstverlening inkopen bij externe bedrijven, en hun gegevens opslaan bij cloudproviders. Binnen zo'n ecosysteem is de weerbaarheid vaak afhankelijk van de zwakste schakel. Kwetsbaarheden in de digitale weerbaarheid bij één partij in een ecosysteem kunnen immers grote gevolgen hebben voor andere organisaties. Bedrijven, overheden en organisaties hebben vaak onvoldoende inzicht in en invloed op de beveiliging van andere schakels in hun ecosysteem.[164] Uit onderzoek blijkt daarnaast dat de kwetsbaarheid voor cyberaanvallen toeneemt naarmate het aantal schakels in de toeleveringsketen groeit, aangezien complexere netwerken meer toegangspunten voor risico's bieden.[165] Daar komt bij dat de afhankelijkheid van veel organisaties van een klein aantal grote aanbieders, zoals cloud- en softwareleveranciers, bij incidenten mogelijk grote gevolgen kan hebben.[166]

De risico's van zo'n ecosysteem werden bijvoorbeeld duidelijk bij de hack op Ceva Logistics in augustus 2026. Door dit incident werden verschillende grote Nederlandse bedrijven waarvoor Ceva bestellingen afhandelt, slachtoffer van een datalek (zie jaarbeeld, hoofdstuk 5). Ook leidde de hack tot logistieke vertraging bij onder andere De Bijenkorf en Bol. De afnemers van Ceva verwerken voor hun dienstverlening grote hoeveelheden persoonsgegevens, waardoor een lek bij de toeleverancier zeer brede impact kan hebben.[167]

Samenwerking tussen organisaties en bedrijven kan bijdragen aan de weerbaarheid van een ecosysteem. Een goed voorbeeld hiervan is het Cyber Weerbaarheidscentrum Brainport. Hier delen bedrijven uit de hightech- en maakindustrie kennis over digitale dreigingen en weerbaarheid in een besloten community.[168]

Informatiedeling is van groot belang voor het verhogen van de digitale weerbaarheid

Op grond van de Cyberbeveiligingswet (Cbw) en het daaronder vallende Cyberbeveiligingsbesluit (Cbb) is de Minister van Justitie en Veiligheid, in de praktijk het NCSC, voor een groot deel van de in de bijlagen bij de Cbw genoemde sectoren aangewezen als Computer Security Incident Response Team (CSIRT).[XVIII] Voor het bevorderen van de digitale weerbaarheid van Nederlandse organisaties is het van belang dat er door organisaties zo veel mogelijk met het CSIRT informatie over dreigingen en incidenten wordt uitgewisseld. Hierdoor worden het NCSC en andere CSIRT's in staat gesteld om dergelijke informatie samen te brengen, te verrijken en waar mogelijk breder te delen met andere organisaties om ieders weerbaarheid te verhogen.

Indien dreigings- of incidentinformatie niet altijd wordt gedeeld door organisaties, bestaat de kans dat cyberdreigingen en -incidenten bij andere Nederlandse organisaties niet (tijdig) worden onderkend of ontdekt en hierdoor andere slachtoffers niet kunnen worden voorkomen of de impact van incidenten niet kan worden verkleind. Door meer informatie aan het NCSC of een ander CSIRT te verstrekken, kunnen vaker cyberincidenten bij Nederlandse organisaties worden voorkomen of de impact daarvan worden beperkt. In 2025 en 2026 kwamen meermaals cyberincidenten in beeld dankzij vrijwillige informatiedeling met het NCSC. Ook heeft informatiedeling door organisaties in die gevallen geleid tot nader onderzoek naar relevante cybersecurityfenomenen en tot verspreiding van een actueel relevant handelingsadvies.

Hoewel informatiedeling regelmatig succesvol plaatsvindt, schat het NCSC in dat een grote hoeveelheid relevante informatie onbenut blijft, omdat die informatie door de betrokken organisaties niet wordt gedeeld met het NCSC of andere CSIRT's. Het NCSC ziet bij meerdere organisaties een terughoudende houding ten aanzien van informatiedeling, bijvoorbeeld vanwege juridische gevoeligheden of commerciële geheimhoudingsverklaringen. Door deze terughoudende houding in het uitwisselen van informatie bestaat dus echter de kans dat cyberincidenten bij andere Nederlandse organisaties later of zelfs niet worden ontdekt.

Informatiedeling is daarom van groot belang voor het verhogen van de digitale weerbaarheid van Nederlandse organisaties. Organisaties kunnen vrijblijvend contact opnemen met bijvoorbeeld het NCSC via info@ncsc.nl. Incident- en dreigingsinformatie kan in het geval van het NCSC worden gedeeld met cert@ncsc.nl of via MijnNCSC.

XVIII Daarnaast zijn of worden bij regelingen van de betrokken vakministers voor enkele specifieke sectoren andere instanties aangewezen als CSIRT. Het NCSC en andere CSIRT's hebben op grond van artikel 16 Cbw onder meer de taak om cyberdreigingen en incidenten te monitoren en analyseren én om essentiële entiteiten en belangrijke entiteiten als bedoeld in de Cbw en andere relevante partijen over dreigingen en incidenten die hen aangaan te informeren. Essentiële en belangrijke entiteiten hebben een meldplicht voor significante incidenten bij hun CSIRT en hun bevoegde autoriteit, voor het overige geldt dat informatiedeling door organisaties met het NCSC of een ander CSIRT vrijwillig is.

3.2 Digitale weerbaarheid onvoldoende voorbereid op technologische ontwikkelingen

Technologische ontwikkelingen zoals AI en quantumcomputers veranderen de cyberdreiging. Ook daarop blijken Nederlandse organisaties onvoldoende voorbereid.

Inzet AI voor verdediging loopt achter bij inzet in cyberaanvallen

De inzet van AI voor het verdedigen van organisaties en bedrijven tegen cyberaanvallen loopt momenteel achter bij de inzet van AI in cyberaanvallen.[169] Kwaadwillende actoren, zoals landen met een offensief cyberprogramma, ontwikkelen in hoog tempo kennis en capaciteiten om met AI cyberaanvallen uit te voeren. Terwijl hun cyberaanvallen steeds sneller, grootschaliger en moeilijker te detecteren zijn, is er aan de verdedigende kant onvoldoende AI-kennis en capaciteiten om deze veranderende dreiging te pareren.[170] Daarnaast moeten organisaties en overheden, in tegenstelling tot kwaadwillende cyberactoren, zeer zorgvuldig omgaan met de implementatie van AI-toepassingen. Om weerbaar te kunnen zijn tegen AI-gestuurde cyberaanvallen zijn eigen systemen nodig die aanvallen sneller detecteren, misbruik voorspellen en effectievere herstelmethoden ontwikkelen. Daarnaast blijft het noodzakelijk ook hier te zorgen voor adequate basismaatregelen. De Cyber Security Raad (CSR) stelde in zijn signaalbrief van maart 2026 dat deze Nederlandse kennisachterstand iedere dag toeneemt. De kans op schade door aanvallen met AI zal toenemen naarmate langer gewacht wordt met kennisopbouw en het ontwikkelen van toepassingen om ons tegen deze veranderende dreiging te beschermen.[171]

Rijksoverheid nog onvoldoende voorbereid op quantumcomputers

Het is belangrijk dat organisaties zich voorbereiden op de ontwikkelingen rond quantumcomputers. De Rijksoverheid hamert erop dat organisaties en bedrijven zich nu al moeten voorbereiden op de komst van quantumcomputers.[172] Het overstappen op nieuwe cryptografie kan immers wel vijf jaar of langer in beslag nemen. Toch blijkt begin 2026 uit onderzoek van de Algemene Rekenkamer (AR) dat organisaties binnen de Rijksoverheid zelf nauwelijks zijn voorbereid op de komst van quantumcomputers. Zo blijkt dat 71 procent van de Rijksorganisaties überhaupt nog niet is gestart met de voorbereiding hierop. Dit betekent dat ze bijvoorbeeld nog geen plannen hebben gemaakt voor het invoeren van quantumveilige cryptografie en nog geen gesprekken hebben gevoerd met leveranciers over quantumveilige producten. Het onderzoek wijst uit dat dit komt door een gebrek aan capaciteit en expertise, en doordat andere activiteiten prioriteit hebben.[173] Op dit moment hebben we beperkte data over de mate waarin organisaties en bedrijven buiten de Rijksoverheid zijn voorbereid op de komst van quantumcomputers, maar waarschijnlijk geldt ook hier dat veel partijen nog onvoldoende zijn voorbereid. Zo bleek uit een peiling (april 2026) van SURF onder 50 onderwijs- en onderzoeksinstellingen dat 69 procent momenteel niet actief bezig is met quantumveiligheid.[174]

Quantumcomputers vragen nu om actie

Quantumtechnologie is een verzamelnaam voor technologieën die de bijzondere eigenschappen van deeltjes kleiner dan atomen benutten om op een radicaal andere manier te rekenen, te communiceren en te meten.[175] Onze klassieke computers verwerken informatie met bits, die twee waarden kunnen aannemen: 0 of 1. Door het combineren van grote aantallen bits kunnen computers berekeningen uitvoeren en informatie verwerken. Quantumcomputers werken met een andere informatie-eenheid: de qubit. Deze kan tegelijkertijd (in een superpositie) zowel de waarde 0 als 1 aannemen. Hierdoor kunnen quantumcomputers bepaalde berekeningen veel efficiënter en sneller uitvoeren dan klassieke computers. Dit betekent dat berekeningen die klassieke computers honderden jaren zouden kosten, met een quantumcomputer bijvoorbeeld in twee weken kunnen worden uitgevoerd.[176]

Hoewel quantumcomputers voor veel mensen futuristisch klinken, is er wereldwijd een race om de ontwikkeling van deze technologie gaande. Op dit moment staan veel praktische toepassingen met quantumtechnologie nog aan het begin van hun ontwikkeling. Zo zijn de quantumcomputers die nu al bestaan nog relatief klein en gevoelig voor storingen. Ze kunnen berekeningen nog niet sneller uitvoeren dan de huidige computers.[177] Experts verwachten dat de technologie zich de komende jaren stap voor stap verder zal ontwikkelen. Hierbij werken wetenschappers aan het vergroten van het aantal qubits, het verminderen van fouten tijdens berekeningen en het ontwikkelen van nieuwe algoritmen.[178] Recente studies laten zien dat onderzoekers daarbij ook gebruikmaken van geavanceerde AI-modellen, onder andere voor het ontwikkelen van efficiënte quantumalgoritmen.[179] De verwachting is dat quantumcomputers ergens tussen 2029 en 2035 voldoende rekenkracht kunnen hebben om asymmetrische cryptografie[XIX] te kraken.[180] Vrijwel al het beveiligde internetverkeer (https) steunt hierop voor het opzetten van veilige verbindingen. Ook het financiële systeem is ervan afhankelijk: betalingssystemen gebruiken asymmetrische cryptografie voor het authenticeren en ondertekenen van transacties. Daarnaast beschermt deze cryptografie communicatie zoals e-mail en appberichten, digitale handtekeningen en de versleuteling van vertrouwelijke en bedrijfsgeheime informatie.[181]

Hoewel er dus nog geen quantumcomputers bestaan die de huidige veelgebruikte vormen van asymmetrische cryptografie kunnen kraken, vormen ze nu al wel een dreiging voor de nationale veiligheid. Versleutelde data die statelijke actoren nu onderscheppen en opslaan, kunnen zij op een later moment alsnog met quantumcomputers ontsleutelen. Dit wordt 'store now, decrypt later' genoemd.[182] Als quantumcomputers in de toekomst asymmetrische cryptografie kunnen kraken en door kwaadwillenden worden ingezet, dan kan dat vergaande gevolgen voor de nationale veiligheid hebben. Zij kunnen quantumcomputers dan inzetten om toegang te krijgen tot essentiële

XIX Asymmetrische cryptografie wordt gebruikt voor het uitwisselen van sleutels om bijvoorbeeld netwerkverkeer te versleutelen (mbv symmetrische cryptografie), maar ook voor authenticatie en het zetten van een digitale handtekening.

diensten, zoals betalingsverkeer, en tot vertrouwelijke informatie.[183] Omdat cryptografie ook wordt gebruikt om iemands identiteit vast te stellen, zouden ze bijvoorbeeld toegang kunnen krijgen tot toepassingen zoals DigiD. Het zou daarnaast betekenen dat communicatie via e-mail of chatapps onbetrouwbaar is en dat ook de gegevens op onze paspoorten niet langer te vertrouwen zijn. Omdat ook hier geldt dat veel digitale processen afhankelijk zijn van externe systemen en ketenpartners, kunnen kwetsbaarheden in asymmetrische cryptografie bij één partij gevolgen hebben voor bredere ketens, bijvoorbeeld bij gegevensuitwisseling of financiële transacties.[184]

Bedrijven en overheidsorganisaties moeten zich op deze dreiging voorbereiden door hun huidige asymmetrische cryptografie te vervangen door quantumveilige oplossingen, zoals post-quantumcryptografie (PQC). PQC is bestand tegen ontsleuteling door zowel klassieke computers als quantumcomputers. Dit is echter niet eenvoudig en vraagt om specifieke kennis en om middelen. De migratie naar PQC kan bovendien meer dan vijf jaar duren.[185] Omdat de ontwikkelingen op het gebied van quantumcomputers snel gaan, kondigden Google, Cloudflare en Microsoft in de eerste helft van 2026 aan hun producten en diensten vóór 2029 over te zetten naar PQC.[186] De EU publiceerde vorig jaar een gecoördineerde Europese routekaart met heldere tijdlijnen. Hierin staat dat alle lidstaten uiterlijk eind 2026 moeten beginnen met de overgang naar PQC. Tegelijkertijd moet de beveiliging van kritieke infrastructuur zo snel mogelijk, en uiterlijk eind 2030, worden omgezet naar PQC.[187]

3.3 Groeiend besef belang digitale autonomie

De digitale weerbaarheid hangt direct samen met de mate van handelingsvrijheid om onafhankelijke keuzes te maken over hoe we als Nederland onze digitale infrastructuur en digitale weerbaarheid inrichten. Digitale afhankelijkheden verschuiven de zeggenschap over de inrichting en beveiliging van deze systemen naar derden. Het CSBN 2025 beschreef dat Europa, en daarmee Nederland, voor veel digitale processen en diensten afhankelijk is van niet-Europese aanbieders. Zoals het CSBN toen ook al concludeerde, moet Europa er rekening mee houden dat afhankelijkheid van digitale diensten en processen uit andere landen, die eerst niet strategisch of risicovol waren, dit nu of in de toekomst wel worden. In de huidige geopolitieke context kunnen dergelijke afhankelijkheden bijvoorbeeld als drukmiddel worden ingezet.[188]

Breed maatschappelijk en politiek debat over digitale autonomie

Het afgelopen jaar stonden digitale autonomie en soevereiniteit[XX] hoog op de maatschappelijke en politieke agenda in Nederland en Europa. Zo waarschuwde De Nederlandsche Bank (DNB) begin 2026 dat Europese betaalinfrastructuur minder afhankelijk moet worden van niet-Europese spelers vanwege toenemende geopolitieke spanningen en cyberdreigingen.[189] Daarnaast uitte de Tweede Kamer in maart 2026 zorgen over de keuze van de Belastingdienst voor een nieuw btw-systeem van een Amerikaans bedrijf, met name vanwege risico's voor de veiligheid van gegevens.[190] In juni 2026 besloot de staatssecretaris van Financiën dat, in plaats van deze leverancier, de Belastingdienst het beheer en onderhoud van de infrastructuur zelf gaat doen. Uit een landenneutrale risicoanalyse was gebleken dat de risico's rondom de vertrouwelijkheid van gegevens en de continuïteit van de dienstverlening in de huidige geopolitieke context niet afdoende gemitigeerd kunnen worden wanneer een bedrijf uit een ander land het beheer en onderhoud verzorgt. In dit geval blijft het bedrijf wel verantwoordelijk voor de softwareoplossing, maar zal het geen directe toegang hebben tot de productiegegevens.[191] In juli 2026 besloot de staatssecretaris van Financiën de uitrol van Microsoft 365 bij de Belastingdienst, Douane en Dienst Toeslagen te pauzeren. In oktober 2025 had zijn ambtsvoorganger bekendgemaakt dat deze overheidsorganisaties zouden overstappen op Microsoft 365, omdat er geen alternatieven waren. Nu wil het kabinet toch eerst een scenario uitlopen waarbij de software draait op eigen servers van de Belastingdienst of op servers die de dienst zelf beheert en controleert.[192]

Ook de voorgenomen overname van het Nederlandse bedrijf Solvinity, onder andere leverancier van het platform waarop DigiD draait, door het Amerikaanse Kyndryl leidde tot veel maatschappelijke en politieke discussie. De staatssecretaris Digitale Economie en Soevereiniteit stelde, na onderzoek in het kader van landenneutrale investeringstoetsing van Bureau Toetsing Investeringen, vast dat de verwerving door Kyndryl van Solvinity kon leiden tot een bedreiging van het publieke belang, waarna de overname werd verboden.[193]

Meer dan voorgaande jaren lijkt er in de samenleving en politiek nu een breed besef te zijn dat digitale afhankelijkheden en bedrijfsovernames door buitenlandse partijen risico's kunnen opleveren voor Nederland en Europa.

Risico's digitale afhankelijkheden zijn ook concreet merkbaar

Deze rapportageperiode bleek meermaals dat de risico's van digitale afhankelijkheden niet louter theoretisch zijn en dat de digitale dienstverlening daadwerkelijk kan wegvallen. In maart 2026 eisten de VS bijvoorbeeld van tien Amerikaanse technologiebedrijven dat zij hun communicatie met Europese autoriteiten zouden overdragen. De eis had betrekking op contacten met onder meer de Europese Commissie en verschillende EU-lidstaten over de handhaving van Europese regelgeving voor digitale platforms.[194] Half juni 2026 verbood de Amerikaanse regering Anthropic tijdelijk om niet-Amerikaanse bedrijven en personen nog langer toegang te geven tot zijn AI-modellen Fable 5 en Mythos 5.[195] Dat betekende ook dat ENISA, het Agentschap voor cyberbeveiliging van de Europese Unie, zijn toegang tot Mythos verloor.[196] Eind juni werden de beperkingen voor deze AI-modellen weer opgeheven.[197] Toch laat dit voorbeeld zien dat een buitenlandse overheid Europese toegang tot een AI-model van de ene op de andere dag kan intrekken. Dergelijke frontier AI-modellen en de cloudinfrastructuur waarop ze draaien, zijn veelal niet-Europees. Doordat de ontwikkeling van Europese modellen daarnaast achterloopt, kan

XX Digitale soevereiniteit staat voor de juridische en bestuurlijke controle en zeggenschap over digitale systemen en data. Digitale autonomie staat voor de bredere operationele handelingsvrijheid om onafhankelijke keuzes te maken.

het gebruik van deze modellen mogelijk ongewenste digitale afhankelijkheid creëren.

De complexe zoektocht naar Europese alternatieven

Tegen deze achtergrond zijn steeds meer Europese landen, organisaties en bedrijven op zoek naar Europese alternatieven voor cloud-, software- en andere digitale diensten. Het Internationaal Strafhof (ICC) besloot bijvoorbeeld eind 2025 om Microsoft-software te vervangen door kantoorsoftware van een Duitse leverancier. Dit besluit volgde na Amerikaanse sancties tegen de hoofdaanklager en andere functionarissen van het ICC. Hierdoor werd de hoofdaanklager in 2025 de toegang tot zijn Microsoft-e-mailaccount ontnomen.[198] De Franse overheid maakte begin 2026 bekend dat zij Amerikaanse vergader- en samenwerkingssoftware wil vervangen door een Frans alternatief, met als doel dat alle Franse overheidsdiensten uiterlijk in 2027 van deze oplossing gebruikmaken.[199] Ook in Nederland zijn dergelijke ontwikkelingen zichtbaar. Zo wil De Nederlandsche Bank (DNB) haar afhankelijkheid van Amerikaanse technologiebedrijven verkleinen door cloudcapaciteit af te nemen bij een Duitse cloudprovider.[200] Binnen de recent opgerichte EDIC Digitale Gemeenschapsgoederen werkt de Nederlandse overheid samen met Duitsland en Frankrijk aan de doorontwikkeling van bovengenoemde Duitse en Franse software.[201] Daarnaast werkt een samenwerkingsverband van alle Nederlandse universiteiten, de Rijksoverheid en SURF gezamenlijk aan een plan om universiteiten minder afhankelijk te maken van Amerikaanse clouddiensten, communicatieplatformen en kantoorapplicaties.[202] Tot slot besloot het Europees Parlement in juni 2026 Google in te wisselen voor de Franse zoekmachine Qwant.[203]

Hoewel er dus voorbeelden zijn van organisaties en bedrijven die digitale dienstverlening uit niet-Europese landen vervangen door Europese alternatieven, is dit niet altijd eenvoudig of mogelijk. Zo domineren Amerikaanse techbedrijven op alle belangrijke onderdelen van digitale dienstverlening en zijn Europese alternatieven soms beperkt voorhanden.[204] Tegelijkertijd is het ook niet zonder risico's om bestaande digitale afhankelijkheden abrupt en grootschalig af te bouwen. Nederlandse en Europese alternatieven zijn niet per definitie veiliger en het beveiligingsniveau van Amerikaanse dienstverlening is over het algemeen hoog.[205] Zo was er in juni 2026 een veiligheidsincident met Tchap, de chatapp die de Franse overheid zelf ontwikkelde voor ambtenaren. Hierbij kreeg een hacker toegang tot een gebruikersaccount.[206] De hacker claimde de gegevens van zo'n 70.000 accounts en ruim 13 GB aan bestanden uit meer dan 640.000 berichten te hebben gestolen.[207]

Daarnaast is niet altijd duidelijk in hoeverre alternatieve aanbieders daadwerkelijk onafhankelijk zijn van Amerikaanse technologie voor onderhoud, infrastructuur of softwarecomponenten. Onder andere Amerikaanse techbedrijven hebben in reactie op de toenemende Europese bezorgdheid over digitale soevereiniteit bijvoorbeeld zogenaamde 'soevereine cloud'-oplossingen gelanceerd. Hier zouden gevoelige gegevens veilig blijven, lokaal worden beheerd en afgeschermd zijn tegen buitenlandse inmenging. Deze soevereine clouds werken over het algemeen met datacenters in de EU, betrouwbare (Europese) partners en contractuele waarborgen. Al deze waarborgen veranderen echter niets aan de juridische realiteit dat Amerikaanse techbedrijven in beginsel onder Amerikaanse wetgeving met extraterritoriale werking vallen. Dit geldt onder andere voor de Amerikaanse CLOUD Act, FISA Section 702, exportbeperkingen en sanctieregelingen. Hiermee kan de Amerikaanse overheid bij Amerikaanse bedrijven, ook wanneer diensten fysiek in Europa worden geleverd, toegang tot bepaalde gegevens afdwingen of in extreme gevallen zelfs de continuïteit van diensten verstoren.[208]

Het verminderen van digitale afhankelijkheden vraagt daarom om een zorgvuldige afweging tussen risico's, uitvoerbaarheid en continuïteit. Voor Nederland is het daarbij van belang om scherp te bepalen welke publieke belangen, waaronder kritieke sectoren (vitale sectoren), bij uitstek beschermd moeten worden en dus meer digitale autonomie vereisen.

Digitale weerbaarheid Caribisch deel van het Koninkrijk

In vergelijking met Europees Nederland zijn er weinig gegevens beschikbaar over de stand van cybersecurity in het Caribisch deel van het Koninkrijk, waardoor het moeilijk is een goed beeld van de weerbaarheid te verkrijgen. Net als voor Europees Nederland is het lastig te meten hoe het er met de digitale weerbaarheid voor staat. Aanvullend ontbreken goede gegevens die voor Europees Nederland wel beschikbaar zijn. Gegevens over aantallen cyberincidenten, datalekken of aangiften worden niet of niet structureel bijgehouden en gepubliceerd, terwijl deze gegevens wel nodig zijn om een goed beeld te krijgen van de dreiging en de weerbaarheid, en van de vraag of dit de veiligheidsbelangen van het Koninkrijk kan raken.

Het afgelopen jaar was er veel aandacht voor het verhogen van de digitale weerbaarheid in Caribisch Nederland en het Caribisch deel van het Koninkrijk en werden zorgen breder geuit. Zo riep de Vereniging Bedrijfsleven Curaçao (VBC) bedrijven, overheden en onderwijsinstellingen op gezamenlijk in actie te komen tegen de digitale dreiging.[209] Volgens de bedrijfsvereniging is met name het midden- en kleinbedrijf kwetsbaar. Ook riep de directeur van de Veiligheidsdienst Aruba op tot meer aandacht voor de risico's van digitalisering, vooral bij bestuurders.[210] Deze oproep maakte deel uit van het Caribisch Cyberprogramma binnen het Overheidsbreed Cyberprogramma 2025 van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, dat samen met ICTU en lokale partners op de eilanden wordt uitgevoerd. Hiermee wordt aandacht gevraagd voor kennisdeling, bewustwording en veilig digitaal gedrag.[211] Ook wordt gewerkt aan de routekaart voor een cybersecuritystelsel voor het Caribisch deel van het Koninkrijk, waarbij zoveel mogelijk wordt aangesloten bij de digitale bescherming en weerbaarheid zoals in Europees Nederland. Hierin past het gelanceerde bouwplan van het Cyberweerbaarheidsnetwerk, dat de weerbaarheid in het Caribisch deel van het Koninkrijk de komende jaren met structurele samenwerking moet verhogen.[212] Ook heeft de RDI, om de continuïteit van de telecominfrastructuur in Caribisch Nederland te verhogen, de concessies voor mobiele en vaste netwerken aangevuld met voorschriften om de beschikbaarheid te waarborgen.[213]

Ondanks alle initiatieven en de toenemende aandacht kan niet worden gesteld dat de digitale weerbaarheid is toegenomen. De initiatieven hebben uiteraard ook tijd nodig om effect te hebben. Het aantal opvallende incidenten in deze rapportageperiode lijkt lager, maar er zijn tegelijkertijd weinig statistische gegevens beschikbaar. De dreigingen voor Europees Nederland gelden grotendeels ook voor het Caribisch deel van het Koninkrijk, al verschillen omvang en ernst. De impact van een incident kan er echter groter zijn, doordat de afhankelijkheden tussen de eilanden en van derde landen groter zijn en er minder terugvalopties voorhanden zijn.



In april 2026 werd zorgleverancier Chipsoft getroffen door een ransomware-aanval. ChipSoft levert zorg-systemen aan o.a. ziekenhuizen en huisartsenpraktijken. Verschillende zorgorganisaties bevestigen dat er patiëntgegevens zijn gestolen. Het gaat onder meer om tbs-klinieken, revalidatieklinieken, het Oogziekenhuis Rotterdam en meerdere huisartsenpraktijken.

4. Scheefgroei dreiging en weerbaarheid vormt risico voor de nationale veiligheid

Er ontstaat verdere scheefgroei tussen de cyberdreiging en de digitale weerbaarheid. Aan de ene kant nemen de capaciteiten en activiteiten van statelijke actoren en cybercriminelen toe. Aan de andere kant groeit de weerbaarheid van Nederlandse organisaties en bedrijven niet in hetzelfde tempo als de capaciteiten van kwaadwillenden. Dit vergroot de kans dat Nederland slachtoffer wordt van spionage, datadiefstal, ontwrichtende sabotage en uitval van digitale processen, met impact op de nationale veiligheid. Nederlanders maken zich steeds meer zorgen over dergelijke cyberaanvallen. Incidenten kunnen het vertrouwen in de digitale weerbaarheid van (overheids)organisaties en bedrijven aantasten of tot apathie leiden. De komende jaren zal AI het cyberlandschap ingrijpend veranderen en de dreiging verder versterken. Zoals het jaarbeeld in hoofdstuk 5 laat zien, heeft Nederland nu al te maken met veel cyberincidenten, waarvan een deel niet in beeld is. Als de digitale weerbaarheid van Nederlandse organisaties en bedrijven niet aanzienlijk verbetert, zal het aantal cyberincidenten fors groeien. Hierbij zal de kans op cyberincidenten bij (overheids)organisaties en bedrijven die de samenleving ontwrichten nog verder toenemen. De achterblijvende weerbaarheid zal daarnaast met name een ongelijk speelveld vormen voor kleine organisaties en het mkb. Zij blijven in verhouding tot grotere organisaties en bedrijven achter in het nemen van maatregelen voor de noodzakelijke verhoging van hun digitale weerbaarheid. Ondanks een toename van het aantal bekende incidenten weten we ook dat een groot deel van de incidenten (nog) onzichtbaar zijn of blijven. Het is dan ook niet de vraag óf, maar wanneer Nederland te maken krijgt met een maatschappij ontwrichtend cyberincident.

4.1 Scheefgroei tussen dreiging en weerbaarheid maakt aanvallen succesvol

Statelijke actoren zetten al langere tijd cyberaanvallen in om hun doelen te bereiken. Verschuivende geopolitieke verhoudingen zorgen ervoor dat dit middel vaker wordt ingezet. Mede daardoor, en door de verdere automatisering van cyberaanvallen met behulp van AI, nemen de capaciteiten en activiteiten van statelijke actoren en cybercriminelen toe. Hoewel er verschillende maatregelen worden genomen om Nederland tegen deze veranderende cyberdreiging te verdedigen, groeit de weerbaarheid van Nederlandse organisaties en bedrijven niet in hetzelfde tempo mee. Hierdoor ontstaat verdere scheefgroei tussen de cyberdreiging en de digitale weerbaarheid.[214] Dit vormt een ernstig risico voor de nationale veiligheid en betekent dat de kans op cyberincidenten, zoals spionage, (voorbereidingen voor) sabotage, datadiefstal en de verstoring of uitval van digitale processen, toeneemt.[215]

De aanval op het Britse Jaguar Land Rover (JLR) laat deze rapportageperiode zien dat cyberaanvallen aanzienlijke financiële en

maatschappelijke impact kunnen hebben. De door hackers van Scattered Lapsus$ Hunters geclaimde aanval verstoorde de bedrijfsvoering van JLR en van duizenden andere organisaties ernstig. Volgens berekeningen van het onafhankelijke Britse Cyber Monitoring Centre bedroeg de totale schade van de aanval ongeveer 2,2 miljard euro.[216] Het incident raakte naast JLR zelf zo'n 5.000 organisaties, vooral toeleveranciers en autodealers.[217] Volgens onderzoekers van het Cyber Monitoring Centre zagen toeleveranciers zich genoodzaakt verschillende maatregelen te nemen om het voortbestaan van hun bedrijf te waarborgen, waaronder loonsverlagingen, het verkorten van de werktijden en in sommige gevallen het ontslaan van personeel.[218] De aanval op JLR geldt als de meest schadelijke cyberaanval uit de Britse geschiedenis en illustreert dat aanvallen van cybercriminelen zeer verstrekkende gevolgen kunnen hebben voor de maatschappij.

Om hun politieke, militaire en economische doelen te bereiken, misbruiken statelijke actoren kwetsbaarheden in systemen van overheidsorganisaties en kritieke entiteiten. Zij voeren daartoe gerichte aanvallen uit voor spionage en (de voorbereiding van) sabotage.[219] Denk hierbij aan het Chinese Salt Typhoon dat wereldwijd grote slachtoffers maakte en in Nederland enkele kleine Internet Service- en Hosting providers tot doelwit had.[220] De spearphishingcampagne van pro-Iraanse hackers gericht op Europese ambassades.[221] Russische phishingaanvallen op Signal-accounts van Nederlandse ambtenaren.[222] En de door CERT.PL beschreven grote Russische cyberaanval op het Poolse energienetwerk.[223] Daarnaast werken statelijke actoren en cybercriminelen ook opportunistisch en richten ze hun cyberactiviteiten op een breed scala aan organisaties en bedrijven. Juist organisaties met een lage weerbaarheid lopen daarbij het risico als eerste slachtoffer te worden.[224]

Verschillende cyberincidenten in het jaarbeeld illustreren de scheefgroei tussen dreiging en weerbaarheid (zie hoofdstuk 5). Voorbeelden hiervan zijn onder andere de compromittering van de Dienst Justitiële Inrichtingen (DJI), de Autoriteit Persoonsgegevens (AP) en de Raad voor de Rechtspraak, waarbij kwaadwillende hackers inzage kregen in persoonsgegevens van medewerkers.[225] Daarnaast werd ook toegang verkregen tot systemen van het ministerie van Financiën. Het ministerie haalde die systemen vervolgens offline.[226] Ook stalen aanvallers via een ClickFix-aanval bijna 552.000 bestanden van de gemeente Epe, waaronder persoonsgegevens van inwoners.[227] Bij softwareleverancier ChipSoft maakten cybercriminelen grote hoeveelheden medische patiëntgegevens buit. Daardoor moest een groot deel van de Nederlandse ziekenhuizen de digitale patiëntportalen offline halen.[228]

Naast de zichtbare cyberincidenten in het jaarbeeld is Nederland ook geregeld slachtoffer van cyberaanvallen die überhaupt niet opgemerkt worden. De AIVD en de MIVD concluderen in hun jaarverslagen van 2025 dat maar een beperkt deel van de Chinese cyberoperaties tegen Nederland wordt gedetecteerd en gemitigeerd.[229] Ook blijkt de Chinese cyberdreiging telkens groter dan gedacht.[230] Nederlandse (overheids)organisaties moeten er daarom van uitgaan dat buitenlandse kwaadwillende hackers op dit moment in hun digitale systemen aanwezig zijn, zonder dat zij weten wie zich waar toegang heeft verschaft en welke schade die kan aanrichten. Hoewel dit een ernstige dreiging voor de nationale veiligheid vormt, blijft dit voor veel mensen een ongrijpbaar fenomeen. Deze dreiging blijft immers vaak onzichtbaar en kwaadwillende hackers kunnen gevoelige data stelen of toegang tot systemen hebben zonder dat iemand dit merkt. Mede hierdoor komen noodzakelijke weerbaarheidsverhogende maatregelen maar moeilijk van de grond.

4.2 Scheefgroei raakt vertrouwen in digitale weerbaarheid

De scheefgroei tussen dreiging en weerbaarheid beïnvloedt mogelijk hoe burgers de digitale weerbaarheid van (overheids)organisaties en bedrijven beoordelen. Dit is problematisch, omdat deze perceptie van invloed kan zijn op het draagvlak voor digitale processen en dienstverlening. Wetenschappelijk onderzoek naar de relatie tussen cyberaanvallen en vertrouwen is echter schaars en geeft hierover geen eenduidig beeld.

Sommige onderzoeken wijzen erop dat cyberaanvallen het vertrouwen in de digitale weerbaarheid van organisaties aantasten, juist doordat de samenleving zo sterk afhankelijk is van digitale infrastructuur.[231] In Nederland was dit effect te zien bij de hack van het Openbaar Ministerie in de zomer van 2025. Het EenVandaag Opiniepanel legde respondenten vragen voor, zowel voor als na de hack. Daaruit bleek dat na de hack meer mensen twijfelden aan de digitale weerbaarheid van (overheids)organisaties. In ongeveer een maand steeg dat van 58 naar 67 procent. De peiling geeft geen inzicht in de langetermijngevolgen voor dit vertrouwen.[232]

Andere onderzoeken stellen daarentegen dat de vele cyberaanvallen zonder tastbare gevolgen burgers hier eerder emotioneel ongevoelig voor maken. Door gewenning hebben nieuwe aanvallen dan geen invloed meer op het vertrouwen van burgers in de digitale weerbaarheid van overheden en bedrijven. In plaats daarvan ontstaat er een gevoel van apathie ten opzichte van cyberincidenten.[233] Ook deze apathie is zorgelijk in het kader van de nationale veiligheid, omdat burgers en organisaties dan minder urgentie voelen om hun digitale weerbaarheid te verhogen.

De directe relatie tussen cyberaanvallen en publieke opinie over digitale weerbaarheid is dus moeilijk te duiden. Wat onderzoek wel duidelijk aantoont, is dat Nederlanders zich grote zorgen maken over cyberdreigingen. Uit de Risico- en Crisisbarometer van de NCTV (najaar 2026) blijkt dat burgers de kans op cyberdreigingen van alle onderzochte dreigingen het hoogst inschatten: 83 procent acht deze (zeer) waarschijnlijk. Daarnaast maakt 51 procent van de Nederlanders zich het meeste zorgen over cyberdreigingen. Tot slot ziet 58 procent cyberdreigingen als een van de meest ernstige gebeurtenissen voor de Nederlandse samenleving.[234] Ander onderzoek bevestigt dat beeld. Uit de Eurobarometer van het Europees Parlement (najaar 2025) blijkt dat 67 procent van de Nederlanders zich zorgen maakt over cyberaanvallen vanuit niet-EU-landen. In andere EU-landen zijn de zorgen over cyberaanvallen gemiddeld even groot.

De komende jaren voert de overheid mogelijk nieuwe digitale processen in die grote groepen Nederlanders raken. Zo werkt de Europese Unie aan de invoering van een digitale euro en verkent de Rijksoverheid hoe zij online leeftijdsverificatie in Nederland kan

vormgeven.[235] Zorgen over cyberdreigingen, mogelijk afnemend vertrouwen of juist apathie ten opzichte van digitale weerbaarheid kunnen verdere digitalisering van de samenleving bemoeilijken. Voor het succes van dergelijke systemen is niet alleen van belang dat zij technisch goed functioneren, maar ook dat burgers erop vertrouwen dat ze veilig zijn. Daarnaast moeten burgers zelf nadenken over veilig gebruik van digitale processen.

Onveilige slimme apparaten in huis faciliteren cyberaanvallen

De scheefgroei tussen digitale dreigingen en weerbaarheid kan voor veel mensen abstract klinken en als een probleem overkomen dat vooral de overheid en bedrijven aangaat. Toch spelen ook Nederlandse huishoudens een rol in deze scheefgroei. Met onveilige apparaten faciliteren zij onbedoeld cyberactiviteiten van kwaadwillende hackers.

De meeste Nederlanders (89 procent) hebben Internet of Things (IoT)-apparatuur aangesloten op hun thuisnetwerk.[236] IoT omvat alle apparaten die met het internet verbonden zijn.[237] Vaak worden deze apparaten aangeduid als ‘smart’. Denk hierbij aan slimme verlichting, tv-boxen en babyfoons. Ook omvormers van zonnepanelen en thuisassistenten, zoals Google Home en Alexa, behoren tot het IoT. Als consument zou je ervan uit mogen gaan dat in Europa gekochte producten veilig zijn, met voldoende instructies worden geleverd, met tijdige updates worden ondersteund en voldoen aan de Cyber Resilience Act (CRA), die in december 2027 volledig van toepassing zal zijn. Desondanks bevinden zich in Nederlandse huishoudens veel onveilige IoT-apparaten zonder dat gebruikers dit weten.

Een derde van de mensen voert beveiligingsupdates voor slimme apparaten niet of niet tijdig uit. Dat betekent dat er in Nederland minimaal 2,5 miljoen apparaten staan die niet altijd de laatste updates hebben gehad.[238] Veel gebruikers weten waarschijnlijk niet dat updates soms noodzakelijk zijn en dat apparaten een houdbaarheidsdatum voor beveiligingsupdates hebben. Voor sommige apparaten geldt dat er na het verlaten van de fabriek nooit meer updates worden uitgebracht, of dat ze worden verkocht terwijl de 'houdbaarheidsdatum' al is verlopen. Daarnaast worden ze vaak met zwakke standaardwachtwoorden geleverd die daarna niet door de consument worden aangepast. Deze slimme apparaten zijn niet alleen zelf kwetsbaar voor cyberaanvallen, maar faciliteren mogelijk ook cyberactiviteiten van statelijke actoren en cybercriminelen. Kwaadwillende hackers staan als het ware digitaal in de huiskamer. Niet alleen om mee te kijken, maar ook om aan de knoppen te draaien. Figuur 1 op de volgende pagina laat de risico's van veelgebruikte IoT-apparaten in het huishouden zien. Bij veel van deze apparaten staan (gevoelige) gegevens niet op het apparaat zelf, maar gaan ze automatisch via internet naar de fabrikant, leverancier of zelfs een derde partij. Sommige slimme apparaten sturen bijvoorbeeld automatisch beelden naar servers in China.[239]

Elk IoT-apparaat kan worden misbruikt als residential proxy of in een Operational Relay Box-netwerk (ORB). Het apparaat wordt dan een tussenstation voor internetverkeer dat daarmee gebruikmaakt van het IP-adres van een bestaande, particuliere internetgebruiker.[240] Vanuit dit tussenstation kunnen kwaadwillenden cyberaanvallen uitvoeren, zoals DDoS-aanvallen, phishing en het verspreiden van malware.[241] De eigenaar van het apparaat faciliteert zo, onbewust of bewust, cyberaanvallen van statelijke actoren en cybercriminelen.[242] Doordat deze cyberactoren gebruikmaken van een netwerk van gecompromitteerde apparaten, bewaren zij hun anonimiteit en omzeilen zij geografische restricties. Hierdoor zijn cyberaanvallen moeilijker in kaart te brengen en tegen te gaan.[243] Thuis merken mensen vaak alleen verhoogde activiteit op hun apparaten door toegenomen stroomverbruik of langzamer internet, als dit al opgemerkt wordt. Het Britse NCSC bracht in april 2026 naar buiten dat China veelvuldig gebruik maakt van ORB-netwerken, deels bestaand uit consumentenrouters en IoT-apparaten, voor grootschalige cyberaanvallen, waaronder digitale spionage.[244]

Daarnaast kunnen huishoudens zelf ook slachtoffer worden van hackers die zijn binnengedrongen. Slimme apparaten verwerken data waaruit leefpatronen kunnen worden afgeleid. Het bedienen van de verlichting kan bijvoorbeeld het slaap-waakritme verraden en uit het laadgedrag van de auto blijkt wanneer iemand thuiskomt.[245] In het ergste geval kunnen gecompromitteerde apparaten dataverkeer op het thuisnetwerk onderscheppen.[246] Door al deze informatie te combineren, kunnen aanvallers onder andere gerichte phishingcampagnes opzetten, identiteitsfraude plegen en woninginbraken voorbereiden.

De scheefgroei tussen dreiging en weerbaarheid is ook goed te zien met de adoptie van de duurzame energiesystemen bij particulieren. Steeds meer Nederlanders installeren omvormers, laadpalen en thuisbatterijen.[247] Deze apparaten zijn ook aangesloten op het internet en zonder goede beveiligingsmaatregelen kwetsbaar voor de hiervoor beschreven dreigingen. Een bijkomend gevaar is de cyberfysieke dreiging. Toegang tot het Batterij Management Systeem (BMS) stelt aanvallers in staat de batterij te overladen of snel te ontladen. Dit kan leiden tot huisbranden of instabiliteit op het energienet, met lokale of regionale stroomuitval tot gevolg.[248] Dezelfde cyberfysieke risico's gelden voor omvormers van zonnepanelen. Kwaadwillende hackers kunnen via deze apparaten het stroomnet verstoren of versnelde veroudering van de apparaten veroorzaken.[249]

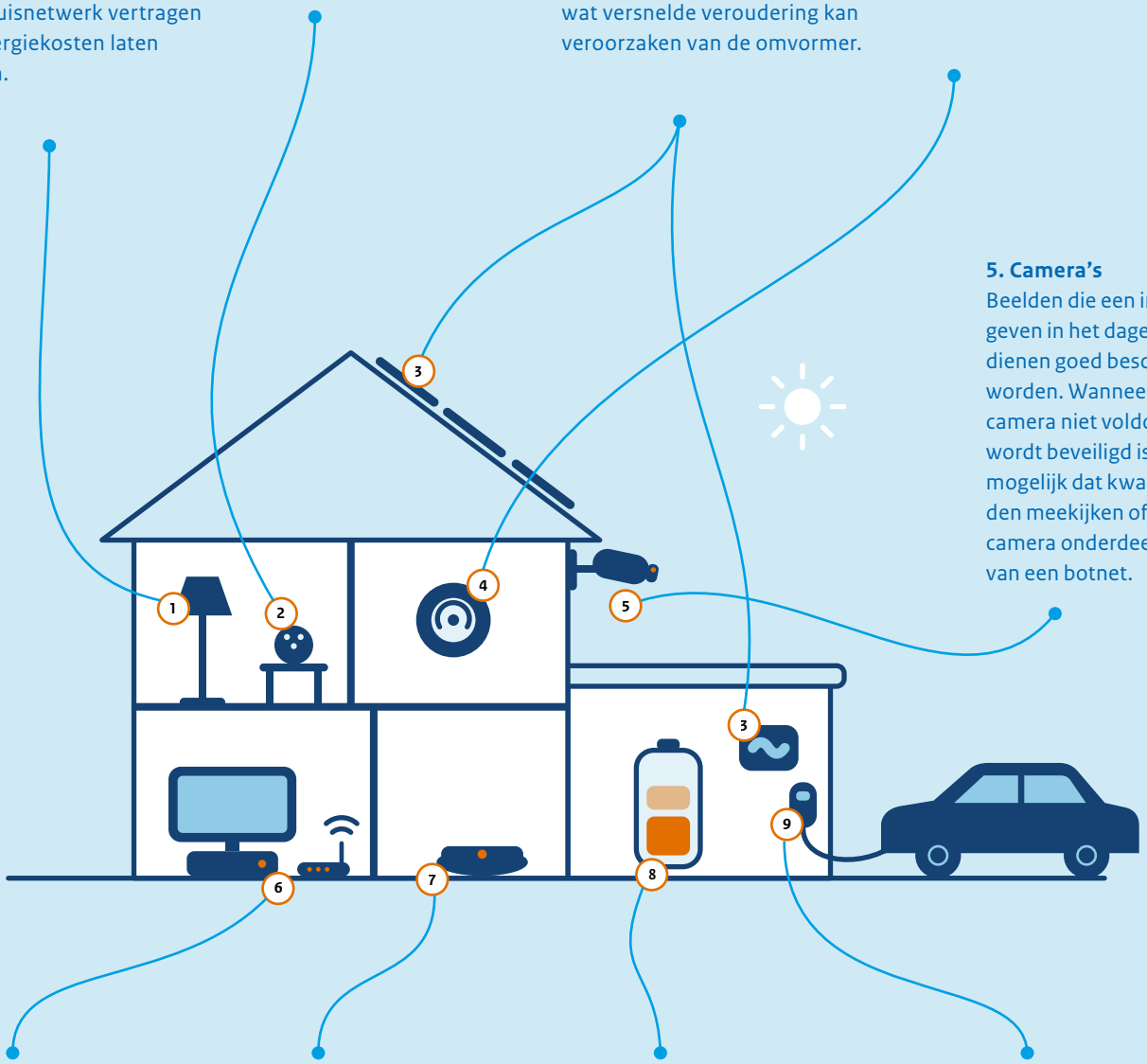
Onveilige IoT-apparatuur kan dus een risico vormen voor de cyberveiligheid van zowel huishoudens als de samenleving als geheel. Het op orde hebben van de digitale basismaatregelen en het naleven van de CRA door bedrijven en leveranciers zijn daarom cruciaal. Ook consumenten kunnen hierin een rol spelen door updates te installeren en geen onveilige producten te kopen.

1. Slimme Verlichting
Het hacken van slimme verlichting kan kwaadwillenden inzicht geven in leefpatronen. Ook kunnen de lampen onderdeel worden van een botnet. De hierdoor toegenomen internetactiviteit van de lampen kan de snelheid van het thuisnetwerk vertragen en energiekosten laten stijgen.

2. Smart Home Hub
Een centrale hub in het smart-home netwerk en vaak uitgerust met een meeluisterende microfoon. Toegang tot dit apparaat geeft al snel inzicht in binnenshuis internetgebruik.

3. Zonnepanelen & Omvormer
Het groene energiesysteem kan risico's met zich meebrengen die sterk vergelijkbaar zijn met die van de thuisbatterij. Wanneer de omvormer kan worden gemanipuleerd bestaat het risico lokale uitval van elektriciteit. Ook kunnen parameters worden veranderd wat versnelde veroudering kan veroorzaken van de omvormer.

4. Slimme Thermostaat
Wanneer zijn er mensen thuis? Wanneer gaat de verwarming aan? Deze data kan verkregen worden met toegang tot de aan het internet verbonden slimme thermostaat. Ook zou de temperatuur op afstand kunnen worden bediend.



5. Camera's
Beelden die een inzicht geven in het dagelijks leven dienen goed beschermd te worden. Wanneer een camera niet voldoende wordt beveiligd is het mogelijk dat kwaadwillenden meekijken of dat de camera onderdeel wordt van een botnet.

6. Superbox & gecompromitteerde SmartTV
Een overvloed aan series en films op één apparaat zonder maandelijks abonnement? In werkelijkheid wordt het netwerkverkeer uitgelezen en de verbonden apparaten gebruikt als onderdeel van een residential proxy of ORB.

7. Robotstofzuigers
Deze apparaten zijn veelal uitgerust met sensoren, microfoons voor stemcommando's en soms zelfs ingebouwde camera's. Deze kunnen worden gebruikt om de locaties van de stofzuigerrobots te achterhalen en om in huiskamers mee te kijken of af te luisteren.

8. Thuisbatterij
Ook het Batterij Management Systeem (BMS) kan gehackt worden. Naast de risico's voor datadiefstal kunnen cruciale instellingen worden veranderd. Dit kan leiden tot verminderde functionaliteit of in het ergste geval brand door oververhitting. Ook kunnen kwaadwillenden met toegang tot meerdere systemen in de buurt het energienet instabiel maken. Dit zou regionaal kunnen leiden tot uitval van elektriciteit.

9. Moderne auto's & Thuislader
Moderne 'slimme' auto's staan via een simkaart continu in verbinding en verzamelen data, zoals locaties, camerabeelden en gesprekken. Ze zijn hackbaar, en het productieland kan toegang hebben tot die gegevens. Ook de thuislader, verbonden met het elektriciteitsnet, kan een gevaar vormen vergelijkbaar met die van de thuisbatterij en de omvormers.

Figuur 1: de risico's van IoT-apparaten in en rondom huis.[250]

4.3 Technologische ontwikkelingen kunnen aantal cyberincidenten de komende jaren vergroten

Dit CSBN beschrijft hoe technologische ontwikkelingen, zoals op het gebied van AI en de toekomstige quantumcomputer, het dreigingslandschap de komende jaren drastisch kunnen veranderen. Wanneer AI alle onderdelen van cyberaanvallen verder automatiseert of zelfs autonoom uitvoert, worden cyberaanvallen nog sneller, grootschaliger en geavanceerder. De meest geavanceerde Amerikaanse frontier AI-modellen zijn eerst vaak alleen beschikbaar voor een select aantal bedrijven en overheden. Na gemiddeld zes maanden wordt de technologie toegankelijk voor een groter publiek.[251] Ook ontwikkelen landen die als systeemrivaal van het Westen gelden, zoals China, hun eigen frontier AI-modellen die ze onder andere kunnen gebruiken voor cyberaanvallen.[252]

Als de digitale weerbaarheid van Nederlandse (overheids)organisaties en bedrijven niet aanzienlijk verbetert, zal het aantal cyberincidenten de komende jaren fors toenemen. Hierbij zal ook de kans op cyberincidenten bij (overheids)organisaties en bedrijven die de samenleving ontwrichten toenemen. Dit zou met name een ongelijk speelveld vormen voor kleine organisaties en het mkb. Zij blijven in verhouding tot grote organisaties en bedrijven achter in het nemen van maatregelen voor de noodzakelijke verhoging van hun digitale weerbaarheid.[XXI] Kleine organisaties en het mkb kunnen hun weerbaarheid niet zelfstandig verhogen.

De ontwikkeling van AI verloopt in een uitzonderlijk hoog tempo en blijft daarmee ons voorstellingsvermogen uitdagen. Capaciteiten die enkele jaren geleden nog als toekomstscenario werden beschouwd, zijn inmiddels werkelijkheid. Denk hierbij aan het automatiseren van onderdelen van cyberaanvallen of honderden autonome AI-agents die in de testfase zelfstandig een manier vinden om het internet op te gaan en dagenlang onbedoelde cyberaanvallen uitvoeren.[253]

Hoewel er een duidelijke trend is van verdere automatisering en zelfs autonoom werkende AI-modellen, is niet volledig te voorspellen hoe die ontwikkeling er de komende jaren exact uit zal zien. Datzelfde geldt voor quantumcomputers. Wat deze technologie met de nationale veiligheid doet, wordt pas echt zichtbaar zodra er quantumcomputers zijn die de nu veelgebruikte asymmetrische cryptografie[XXII] daadwerkelijk kunnen kraken. Zulke quantumcomputers bestaan nu nog niet. Voor de weerbaarheid van Nederlandse organisaties en bedrijven betekent dit dat zij zich niet alleen moeten voorbereiden op verwachte technologische ontwikkelingen, maar ook rekening moeten houden met onverwachte doorbraken die nieuwe uitdagingen met zich meebrengen. Het verhogen van de weerbaarheid is dus nooit af.

Het is voor organisaties en bedrijven onmogelijk om 100 procent weerbaar te zijn tegen cyberaanvallen. Maar nu het aannemelijk is dat technologische ontwikkelingen de dreiging de komende jaren versneld zullen doen toenemen, is het van cruciaal belang dat de digitale weerbaarheid wordt verhoogd en meebeweegt met de veranderende dreiging.

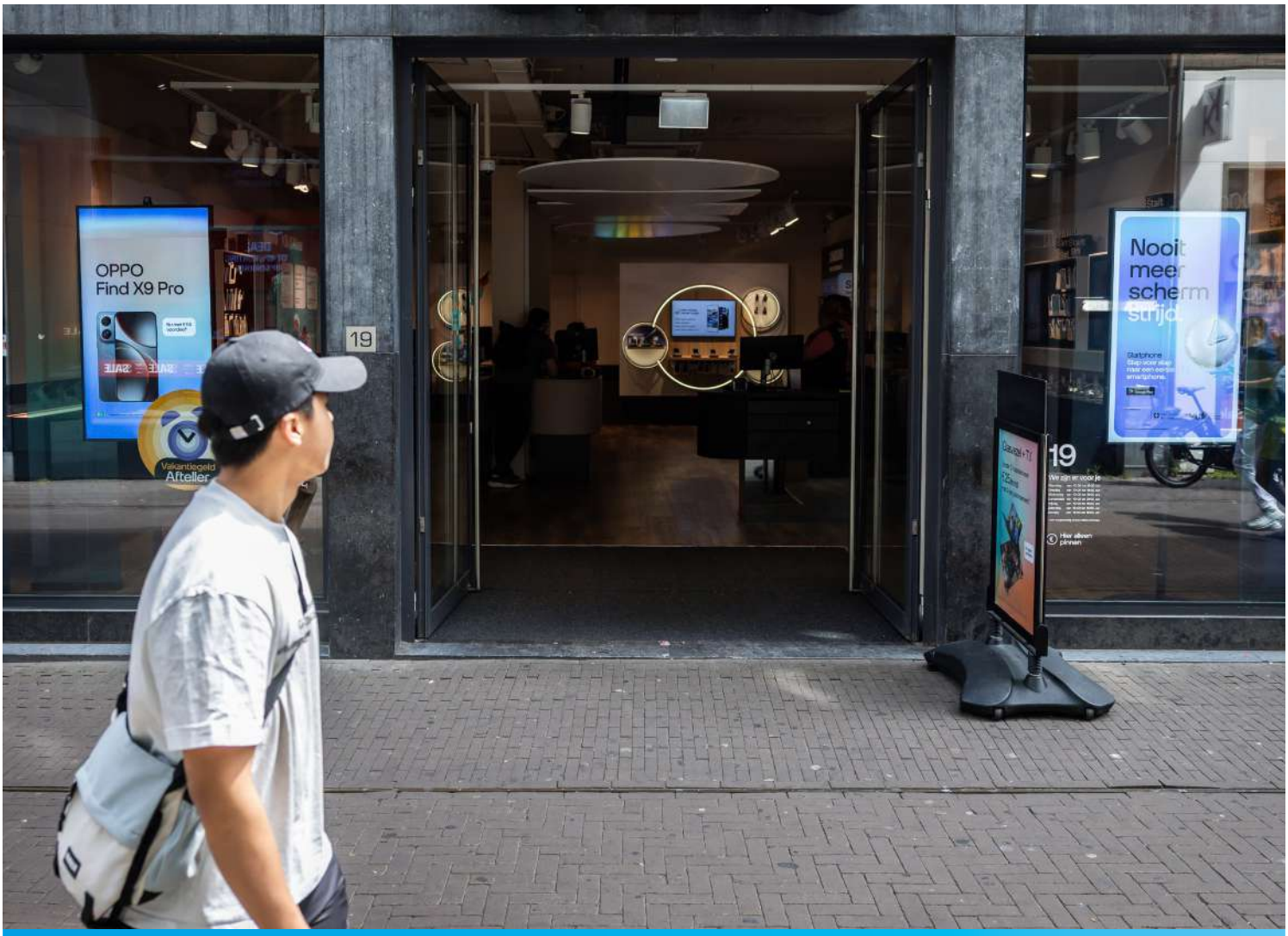
Dit betekent allereerst dat de basisprincipes van digitale weerbaarheid[XXIII] op orde moeten zijn. (Overheids)organisaties en bedrijven patchen kwetsbaarheden nog te vaak te laat en loggen en monitoren niet of ontoereikend. In een dreigingslandschap waarin aanvallen steeds verder worden geautomatiseerd, is die situatie niet langer houdbaar. Veel risico's zijn al jarenlang bekend, maar blijven bestaan omdat eigenaarschap, prioriteit van bestuur of management en capaciteit en middelen bij organisaties en bedrijven achterblijven bij de dreiging.[254] Dit vormt een risico voor de nationale veiligheid. Niet alleen omdat het de betreffende organisaties en bedrijven rechtstreeks treft, maar ook omdat zij deel uitmaken van bredere digitale ecosystemen waarin de digitale weerbaarheid afhankelijk is van de zwakste schakel. Het verhogen van de weerbaarheid van individuele organisaties en bedrijven is dus een collectief belang. Dit vraagt daarom ook om ondersteuning voor kleinere organisaties en bedrijven, zoals het mkb, die de middelen en expertise missen om de noodzakelijke verbeteringen door te voeren.

Het huidige dreigingslandschap vraagt dus om een houding van urgentie en prioriteit, én om bijbehorende investeringen in digitale weerbaarheid. Niet alleen bij IT- en securitymedewerkers, maar juist bij het bestuur en management van organisaties en bedrijven. Dit is niet alleen in het belang van hun eigen cyberveiligheid, maar ook van het ecosysteem waarin zij met andere partners samenwerken en waarin zij onmiskenbaar afhankelijk zijn van elkaars weerbaarheid.[255]

XXI De CSR heeft hier in 2024 in het Advies 'Verkleinen van de Cyberweerbaarheidskloof' ook aandacht voor gevraagd.

XXII Asymmetrische cryptografie wordt gebruikt voor het uitwisselen van sleutels om bijvoorbeeld netwerkverkeer te versleutelen (m.b.v. symmetrische cryptografie), maar ook voor authenticatie en het zetten van een digitale handtekening.

XXIII Zie de website van het NCSC voor meer informatie: https://www.ncsc.nl/basisprincipes



In februari 2026 kregen hackers toegang tot een klantcontactsysteem dat telecomprovider Odido gebruikt. Daarbij hebben ze gegevens gestolen van zo'n 6,2 miljoen klanten. Het is één van de grootste datalekken ooit in Nederland. ShinyHunters claimde de aanval en heeft de data online gepubliceerd nadat Odido weigerde te betalen. De hack was mogelijk doordat een van de daders iemand van de klantenservice van Odido telefonisch misleidde. De beller deed zich voor als iemand van de IT-afdeling en haalde de medewerker over om in te loggen in een werkomgeving die later nep bleek te zijn.

5. Jaarbeeld

De afgelopen rapportageperiode werd gekenmerkt door verschillende cyberaanvallen waarbij data werd gestolen en in sommige gevallen ook gelekt. Zo wisten cybercriminelen bij telecomprovider Odido een grote hoeveelheid data te stelen, die vervolgens online verscheen. Bij andere cyberaanvallen versleutelden aanvallers de data ook. Dit was bijvoorbeeld het geval bij softwareleverancier ChipSoft, die werd getroffen door een ransomware-aanval. Hierbij werden gevoelige patiëntgegevens van diverse Nederlandse zorginstellingen gestolen. Nederland werd daarnaast geraakt door cyberaanvallen van statelijke actoren. De dreiging vanuit statelijke actoren blijft onverminderd hoog en wordt gekenmerkt door toenemende cybercapaciteiten en -activiteiten. In dit jaarbeeld valt op dat zowel cybercriminelen als statelijke actoren steeds vaker AI inzetten bij hun kwaadwillende activiteiten. Ook laat het jaarbeeld opnieuw zien dat technische problemen en niet-moedwillig menselijk handelen uitval van digitale processen kunnen veroorzaken. Dit jaarbeeld is gebaseerd op een selectie van incidenten die publiekelijk bekend zijn geworden en is daarmee per definitie geen uitputtend overzicht.

Opvallende incidenten Nederland

Augustus 2025

Citrix-systemen van enkele Rijksorganisaties gehackt
De Citrix NetScaler-systemen van meerdere kritieke Nederlandse entiteiten zijn via een ernstige kwetsbaarheid gehackt. Hoewel niet bekend is gemaakt om welke organisaties het precies gaat, maakte de demissionaire minister van Justitie en Veiligheid wel bekend dat het ook gaat om enkele Rijksoverheidsorganisaties.[256] In juni bracht Citrix patches uit, maar volgens het NCSC hebben kwaadwillenden de kwetsbaarheid sinds ten minste begin mei misbruikt.[257] Ook de Justitiële ICT Organisatie (JIO) is via een kwetsbaarheid in Citrix gehackt.[258] In juli 2025 haalde het Openbaar Ministerie systemen offline nadat het was gehackt via een Citrix-kwetsbaarheid.[259]

Routers kleine Internet Service- en Hostingproviders in Nederland gecompromitteerd door Salt Typhoon
Volgens de AIVD en MIVD zijn kleinere Internet Service - en Hostingproviders in Nederland doelwit geweest van Chinese hackers. De aanvallen waren onderdeel van de grootschalige wereldwijde cybercampagne van Salt Typhoon. Uit onderzoek van de diensten blijkt dat de Chinese hackersgroep toegang had tot routers van de Nederlandse doelwitten. Voor zover bekend zijn de hackers niet verder doorgedrongen in hun interne netwerken. De grotere Nederlandse providers zouden niet zijn geraakt.[260]

September 2025

Ambassades doelwit van spearphishingcampagne door pro-Iraanse hackers
Onderzoekers van een Israëlisch cybersecuritybedrijf hebben nieuwe activiteiten waargenomen die zij toeschrijven aan de Iraanse groep die bekendstaat als Homeland Justice. De groep zou een gecoördineerde en 'multi-wave' spearphishingcampagne hebben uitgevoerd die voornamelijk is gericht op ambassades en consulaten wereldwijd, waarbij de meeste aanvallen gericht waren op Europese ambassades. Onder meer ambassades en consulaten behorende bij Frankrijk, Duitsland en Nederland zouden zijn aangevallen. Het is niet duidelijk of er organisaties zijn gecompromitteerd en, zo ja, welke.[261]

Ambtenaren ondervinden hinder bij thuiswerken door DDoS-aanvallen op overheid
Onbekende aanvallers voerden een week lang DDoS-aanvallen uit op een deel van de overheid. Het zou daarbij gaan om ministeries en overheidsorganisaties die ICT-systemen van een specifieke leverancier gebruiken. Het raakte onder meer de ministeries van Justitie en Veiligheid, Financiën, Buitenlandse Zaken en Volksgezondheid, Welzijn en Sport. Door de aanvallen was de server voor de VPN-verbinding regelmatig onbereikbaar, waardoor ambtenaren hinder ondervonden bij het thuiswerken.[262]

Nederlandse tieners voeren verkenningsoperatie uit voor Rusland
In september werden Nederlandse tieners opgepakt vanwege vermoedelijke spionageactiviteiten voor Rusland. Een van de jongens heeft een route gelopen door Den Haag met een Wi-Fi-sniffer, onder meer langs Europol en Eurojust, om Wi-Fi-netwerken in kaart te brengen. De opgepakte jongens zouden zijn benaderd via Telegram door een pro-Russische hackersgroep.[263]

Gevoelige gegevens van (kwetsbare) inwoners gemeente Eindhoven ingevoerd in openbare AI-tools
Uit onderzoek van de lokale rekenkamer van de Gemeente Eindhoven blijkt dat tussen september en oktober 2025 gevoelige gegevens van (kwetsbare) inwoners zijn ingevoerd in openbare AI-tools. Het ging met name om documenten en gegevens die te maken hebben met hulp en ondersteuning op het gebied van (jeugd)zorg en welzijn.[264]

Oktober 2025

Honderden apps en websites wereldwijd werkten niet door storing bij AWS
Eind oktober werkten honderden apps en websites wereldwijd niet door een storing bij Amazon Web Services (AWS). Naast talloze internationale platforms werden ook ruim veertig Nederlandse websites en apps geraakt, waaronder die van de Rabobank. Hoewel niet met zekerheid kan worden vastgesteld dat de Nederlandse verstoringen ook zijn ontstaan door de problemen bij Amazon, lijkt dit wel het geval.[265]

Data gelekt na ransomware-aanval bij afvalverwerker Omrin
Begin oktober werd Friese afvalverwerker Omrin getroffen door een ransomware-aanval. Daardoor werden tijdelijk verschillende kringloopwinkels gesloten en was de klantenservice niet telefonisch bereikbaar. Hoewel de afvalapp niet werkte, bleef de daadwerkelijke afvalinzameling onverstoord.[266] Hackers van de ransomwaregroep Qilin hebben de aanval opgeëist. Zij wisten bij de aanval ook data te stelen. Het ging daarbij onder meer om bestanden met personeelsgegevens en financiële documenten van Omrin. De hackers hebben deze informatie uiteindelijk online gelekt.[267]

Europese diplomatieke entiteiten doelwit van Chinese hackers, ook doelwitten in Nederland
Uit onderzoek van Arctic Wolf Labs blijkt dat een Chinese hackersgroep een zero-day kwetsbaarheid in Windows misbruikt bij nieuwe aanvallen die gericht zijn op de diplomatieke gemeenschap in Europa. De Chinese hackers hebben zich in september en oktober 2025 met hun aanvallen gericht op diplomatieke entiteiten en overheidsinstellingen in Hongarije, België, Servië, Italië en Nederland. In Nederland zou het gaan om diplomatieke organisaties.[268]

November 2025

Problemen met uitzendingen en publicaties na ransomware-aanval bij RTV Noord
Begin november werd RTV Noord getroffen door een ransomwareaanval. Daardoor konden medewerkers niet meer in de systemen die nodig zijn voor het maken van uitzendingen. Ondanks de cyberaanval bleef RTV Noord op radio en televisie in de lucht. De hackers hebben bij de aanval ook data gestolen. Het zou onder meer gaan om privégegevens van medewerkers.[269]

Extreemrechtse berichten op websites van o.a. ziekenhuizen en vervoerder
Websites van ongeveer 30 organisaties, waaronder het Martini ziekenhuis in Groningen, Isala ziekenhuis in Meppel en Zwolle en van vervoerder Arriva, zijn in november beklad. De groep Black Witch plaatste extremistische leuzen op de homepage van de websites. Bezoekers van de websites werden omgeleid naar infrastructuur van de kwaadwillenden. De groep zou zich naar eigen zeggen normaliter richten op afpersing en ransomware, maar claimden ditmaal geen data te hebben gestolen.[270]

Wereldwijd websites uren onbereikbaar door storing bij Cloudflare
Op 18 november waren wereldwijd apps en websites uren onbereikbaar als gevolg van een storing bij Cloudflare.[271] In Nederland ging het daarbij onder meer om websites van NH Nieuws, AT5 en het Financieele Dagblad. Ook gebruikers van X ondervonden problemen. Volgens het bedrijf werd de storing veroorzaakt door een wijziging in database-rechten.[272]

December 2025

Hackers stelen data van Interrail reizigers
In december 2025 werd reisplatform Interrail, dat ook opereert onder de naam Eurail, gehackt. Daarbij wisten de aanvallers data te stelen van meer dan 300.000 Europese reizigers. Het ging daarbij om persoonlijke informatie, zoals NAW-gegevens en paspoortnummers. De data werd vervolgens aangeboden op het darkweb.[273]

Januari 2026

Patiëntgegevens huisartsenorganisatie gelekt na hack op e-mailaccount
Gegevens van ruim tweeduizend patiënten van huisartsenorganisatie Medrie zijn gelekt, nadat een aanvaller toegang kreeg tot het mailaccount van een kantoormedewerker. Die mailbox bevatte een document met persoonsgegevens, waaronder burgerservicenummers, namen en adressen van patiënten. Hoe de aanvaller toegang wist te verkrijgen is niet bekendgemaakt.[274]

Februari 2026

Gevoelige persoonsgegevens online gepubliceerd na datadiefstal bij Odido
In het weekend van 7 en 8 februari hebben hackers toegang gekregen tot een klantcontactsysteem (Salesforce) dat Odido gebruikt. Daarbij hebben de hackers gegevens gestolen van zo'n 6,2 miljoen klanten. Dit was één van de grootste datalekken ooit in Nederland.[275] Het ging daarbij om persoonsgegevens van huidige en voormalige klanten. In de gestolen data bleken ook nummers van paspoorten en ID-kaarten te zitten, evenals verblijfspapieren van diplomaten. Ook hebben de hackers zeer gevoelige informatie over kwetsbare klanten in handen gekregen. Daarbij ging het om aantekeningen over bijvoorbeeld bewindvoering of huiselijk geweld. ShinyHunters claimde de aanval en heeft de data online gepubliceerd nadat Odido weigerde te betalen.[276]

Meerdere Nederlandse organisaties gecompromitteerd via Ivanti EPMM-kwetsbaarheid
Eind januari kwam Ivanti met beveiligingsupdates voor twee actief aangevallen kwetsbaarheden in Ivanti Endpoint Manager Mobile (EPMM). Op 9 februari stelde het NCSC dat er bij meerdere Nederlandse organisaties misbruik van een van de kwetsbaarheden was waargenomen. Uit het onderzoek van het NCSC blijkt dat onder andere de database op het Ivanti EPMM systeem wordt gekopieerd en geëxfiltreerd. Deze database bevat naast persoonsgegevens ook informatie over de beheerde telefoons zoals IMEI, telefoonnummer en locatiegegevens.[277] Bij onder meer de Autoriteit Persoonsgegevens en Raad voor de Rechtspraak werden compromittaties vastgesteld. Bij de AP zijn ook namen en zakelijke e-mailadressen geëxfiltreerd.[278] Een andere getroffen overheidsinstantie is de Dienst Justitiële Inrichtingen (DJI). Hier zijn werkgerelateerde gegevens van medewerkers buitgemaakt. Ook bij de Dienst Terugkeer & Vertrek, de Justitiële ICT Organisatie, het College ter Beoordeling van Geneesmiddelen en één gemeente zijn sporen van misbruik gevonden of kon misbruik niet met voldoende zekerheid worden uitgesloten.[279]

Maart 2026

Onbekenden krijgen ongeautoriseerde toegang tot systemen ministerie van Financiën
De ICT-beveiliging van het ministerie van Financiën signaleerde op 19 maart ongeautoriseerde toegang tot systemen voor een aantal primaire processen op het beleidsdepartement. Daarop werden een aantal systemen offline gehaald, waaronder het digitale portaal voor schatkistbankieren. Hierdoor konden zo'n zestienhonderd publieke instellingen, die hun tegoeden bij het ministerie van Financiën hebben ondergebracht, het saldo van hun schatkistrekening niet digitaal inzien. Daarnaast konden de deelnemers aan schatkistbankieren ook geen leningen, deposito's of kredieten aanvragen, de daglimiet wijzigen of rapportages uitdraaien. De minister van Financiën stelde dat, waar nodig, minimale dienstverlening met de hand werd voortgezet, zodat essentiële processen bleven functioneren. Het is niet bekend wie er verantwoordelijk is voor de hack en of er data is gestolen.[280] De aanvallers wisten toegang te verkrijgen tot de systemen via een zero-day kwetsbaarheid in de software die toegang tot de werkplekomgeving regelt.[281]

Politie doelwit van phishing
Eind maart maakte de politie bekend dat zij het doelwit is geweest van een phishing-aanval. Daardoor kon een onbekende hacker inbreken in de systemen en had deze vermoedelijk ongeveer een uur toegang tot data van de politie. Wat de hacker heeft kunnen zien of doen is niet bekend. Volgens de politie is de schade beperkt." Vervangen door "De politie is in maart 2026 doelwit geweest van phishing. Het Security Operations Center van de politie heeft dit snel ontdekt en heeft de toegang direct afgesloten. Gegevens van burgers en onderzoeksinformatie zijn niet inzichtelijk of toegankelijk geweest. De politie is tevens direct een opsporingsonderzoek gestart.[282]

Bijna 552.000 bestanden van gemeente Epe gestolen via ClickFix-aanval
Op donderdag 12 maart werd er ingebroken in de ICT-systemen van de gemeente Epe. De hackers wisten binnen te dringen via een ClickFix-aanval[XXIV] en stalen vervolgens 800 GB aan data. Het gaat om bijna 552.000 bestanden, die verschillende soorten informatie bevatten. Er zijn daarbij ook bestanden met persoonsgegevens gestolen.[283] Uit forensisch onderzoek bleek dat persoonsgegevens van nagenoeg alle inwoners (ruim 32.000) zijn buitgemaakt.[284] De gemeente benadrukt dat de dienstverlening niet onderbroken is (geweest).[285]

April 2026

Patiëntgegevens gestolen na ransomware-aanval op toeleverancier zorginstellingen
ChipSoft, een zorgleverancier van onder meer EPD-software, werd halverwege april getroffen door een ransomware-aanval. Diverse ziekenhuizen haalden daarop hun digitale patiëntportalen offline. In sommige gevallen betekende dit handmatig werk voor ziekenhuizen en langere wachttijden bij balies en callcenters. De hackers hebben bij de aanval medische patiëntgegevens weten te stelen van een 'beperkt aantal' zorgverleners. Daarbij gaat het onder meer om het Oogziekenhuis Rotterdam en tbs-klinieken. Ook zouden een aantal huisartsenpraktijken zijn geraakt door de datadiefstal.[286] Het bedrijf heeft uiteindelijk losgeld betaald, waarop de criminelen hebben toegezegd de data te hebben verwijderd.[287]

Mei 2026

Data gestolen bij leverancier onderwijsplatform, lijkt niet gelekt na betaling losgeld
Begin mei meldde Instructure, de ontwikkelaar van het leerplatform Canvas, een beveiligingsincident. Aanvallers wisten ongeautoriseerde toegang te krijgen tot delen van de infrastructuur en stalen daarbij gegevens. ShinyHunters eiste de verantwoordelijkheid op en beweerde gegevens van honderden miljoenen gebruikers van duizenden onderwijsinstellingen wereldwijd buit te hebben gemaakt.[288] Ook Nederlandse onderwijsinstellingen werden hierdoor getroffen en schakelden Canvas tijdelijk uit. Diverse onderwijsinstellingen gaven aan dat de afsluiting van invloed was op het onderwijs. Lessen moesten worden aangepast en ook konden studenten onder andere geen opdrachten inleveren en lesmateriaal bekijken.[289] Uiteindelijk sloot Instructure een deal met de criminelen en is de data vernietigd, althans volgens de criminelen.[290]

Instituut voor de Nederlandse Taal haalt websites offline na ransomware-aanval
Begin mei haalde het Instituut voor de Nederlandse Taal (INT) verschillende van zijn websites offline wegens een hack. Hoewel het INT niet bekend heeft gemaakt om wat voor soort aanval het ging, claimde een ransomware-groep de aanval op het instituut.[291]

Juni 2026

Signal- en WhatsApp-gebruikers doelwit van phishingaanvallen
Gebruikers van chatapps Signal en WhatsApp zijn het doelwit van phishingaanvallen. Russische staatshackers proberen daarbij toegang te krijgen tot accounts van westerse (waaronder Nederlandse) en Oekraïense hoogwaardigheidsbeklederders, overheidsmedewerkers, militairen en journalisten.[292] In juni stelden de Nederlandse inlichtingen- en veiligheidsdiensten dat de hackers hun werkwijze na het cyberadvies uit maart hebben aangepast. Waar de eerdere methodiek zich primair richtte op het verkrijgen van verificatiecodes voor toegang tot een account, is de nieuwe methode gericht op het stelen van 'Signal Backup Recovery-keys' via phishing.[293]

Klantgegevens zakenreisbureau BCD gelekt na hack door ShinyHunters
ShinyHunters claimde het grote Nederlandse zakenreisbureau BCD te hebben gehackt, waarbij het naar eigen zeggen gegevens van 700.000 klantaccounts wist te stelen. Na het verstrijken van de deadline plaatsten de criminelen een bestand van dertig gigabyte op het darkweb. De hackers gaven aan toegang te hebben verworven tot een klantendatabase die op Salesforce-software draait. Ook stelden de criminelen dat zij konden inbreken bij BCD op plekken waar medewerkers samenwerken via SharePoint. BCD bevestigde dat het 'recent verdachte activiteit zag via een intern gebruikt account', waarna het stappen heeft ondernomen. De dienstverlening zou niet zijn geraakt.[294]

Weg- en vaarweggebruikers ondervinden hinder als gevolg van technische storing bij Rijkswaterstaat
Rijkswaterstaat heeft op 27 juni lange tijd geen toegang gehad tot het internet. Hierdoor waren er problemen met de bediening van bruggen, sluizen, tunnels en rode kruisen boven snelwegen. Zo kreeg de verkeerscentrale niet meer alle camerabeelden binnen vanaf snelwegen. Ook waren meerdere websites van Rijkswaterstaat niet bereikbaar of konden niet worden geactualiseerd. De problemen ontstonden bij geplande werkzaamheden aan een glasvezelkabel. Waar mogelijk werden bruggen en sluizen lokaal bediend.[295]

XXIV Bij een ClickFix-aanval wordt het slachtoffer misleid om zelf schadelijke commando's uit te voeren. Bijvoorbeeld met behulp van een valse foutmelding of nep-update. Deze melding stelt dat de gebruiker een ogenschijnlijk onschuldige handeling moet uitvoeren, maar installeert daarmee onbewust bijvoorbeeld (malafide) software.

OT-systemen Nederlandse organisaties gecompromitteerd door NoName
Op 1 en 3 juni 2026 claimde NoName057(16) in het kader van de langer lopende campagne #OpNetherlands compromittaties van klimaatbeheersingssystemen bij twee Nederlandse organisaties. Bij één organisatie kon de groep via een Human-Machine Interface (HMI)-systeem instellingen van de temperatuur aanpassen. Bij de andere organisatie zou de groep een warmtepomp op afstand hebben kunnen besturen. Naast de compromittaties van OT-systemen claimde NoName057(16) ook toegang te hebben verkregen tot IP-camera's in Nederland. Deze aanvallen op Nederlandse organisaties zijn een reactie op de aanhouding van twee personen door de FIOD in mei 2026, onder meer wegens het faciliteren van pro-Russische digitale aanvallen via een webhostingbedrijf.[296]

Juli 2026

Maasstad Ziekenhuis tijdelijk niet operationeel door grote ICT-storing na testen noodstroom
Begin juli kampte het Maasstad Ziekenhuis in Rotterdam met een ICT-storing. Hierdoor was het (naar eigen zeggen) praktisch niet operationeel. Patiënten konden daardoor niet terecht op de eerste hulp of poliklinieken. Ook e-consults waren niet beschikbaar en patiëntendossiers waren niet inzichtelijk. Daarnaast was het ziekenhuis slecht telefonisch bereikbaar. Het probleem met de ICT ontstond door een continuïteitsoefening bij het testen van de noodstroom. De zorg werd na ongeveer anderhalve dag weer opgestart.[297]

Camera's langs militaire routes gehackt door Rusland
Volgens de Nederlandse inlichtingendiensten richten Russische staatshackers zich met cyberaanvallen structureel op IP-camera's in NAVO- en EU-landen. Daarbij hebben zij ook 'een klein aantal camera's' op militaire routes in Nederland gehackt. Volgens de diensten gaat het om camera's in particulier gebruik, van onder meer bedrijven.[298]

Augustus 2026

Klantgegevens minstens twaalf bedrijven gelekt door aanval op logistiekbedrijf Ceva
Een cyberaanval begin augustus op logistiekbedrijf Ceva Logistics heeft geleid tot datalekken bij ten minste twaalf bedrijven in Nederland.[299] Tot op heden is niet bekend welke persoonsgegevens precies zijn gestolen of gelekt en wie de aanval heeft uitgevoerd. Onder andere De Bijenkorf, Bol, ING, Ajax en Zalando werden geraakt door het datalek dat ontstond bij Ceva Logistics. Bij sommige webwinkels van deze organisaties ontstond meerdere weken vertraging in de levering van producten.[300] Enkele weken na de bekendmaking van het incident meldde BNR dat bij dezelfde aanval ook gegevens van (oud-)personeel van Ceva Logistics waren gestolen. [301] Het gaat mogelijk om burgerservicenummers, kopieën van paspoorten, gegevens van partners en kinderen, salarisgegevens, bankrekeninggegevens en pensioengegevens. Ook verzuimgegevens en arbeidsgeneeskundige gegevens zijn mogelijk onderdeel van de datadiefstal. Hoeveel huidige en voormalige werknemers van Ceva het betreft, is niet duidelijk.

Opvallende incidenten buitenland

September 2025

Vluchtverkeer diverse Europese luchthavens ontregeld door ransomware-aanval op toeleverancier
Eind september kampten verschillende Europese luchthavens met verstoringen door een cyberincident bij een toeleverancier. De getroffen luchthavens, waaronder Brussels Airport, Berlin Airport en Heathrow, maken gebruik van software van Collins Aerospace. Dat bedrijf bleek getroffen door ransomware. Omdat de servers van Collins Aerospace niet meer bereikbaar waren, moesten luchthavens over op het handmatig inchecken van passagiers. Hierdoor ontstonden grote vertragingen en werd luchtvaartmaatschappijen gevraagd vluchten te annuleren.[302] De problemen hielden langere tijd aan en ook werd er in sommige gevallen data gestolen.[303] Achteraf bleek dat Collins Aerospace zelfs is aangevallen door twee verschillende ransomwaregroepen. Een van de aanvallen werd geclaimd door ransomwaregroep Everest. Deze stelde de gegevens van 1,5 miljoen passagiers te hebben gestolen, evenals informatie van duizenden medewerkers. De groep stelde bij de aanval geen ransomware te hebben ingezet. De ransomware-aanval die voor verstoringen zorgde zou door een andere groep zijn uitgevoerd.[304]

Honderden npm-pakketten geïnfecteerd in supply chain-aanval
Begin september sloegen cybersecurityexperts en techbedrijven alarm over een wijdverbreide inbreuk op de softwaretoeleveringsketen. Het ging daarbij om een zichzelf replicerende worm, waarnaar verwezen wordt als Shai-Hulud. Onderzoekers ontdekten honderden geïnfecteerde npm-pakketten waarmee systemen van ontwikkelaars werden gecompromitteerd. Een van de geïnfecteerde pakketten was van cybersecuritybedrijf CrowdStrike. De malware verzamelt allerlei inloggegevens, die naar een publieke GitHub-repository worden geüpload.[305]

Productie Jaguar Land Rover ernstig verstoord door cyberaanval
Een cyberaanval heeft de productie van Jaguar Land Rover (JLR) ernstig verstoord. Na een cyberaanval haalde het bedrijf verschillende systemen offline. Daarbij werden onder meer de verkopen van nieuwe auto's en het uitvoeren van reparaties verstoord.[306] Het incident raakte niet alleen JLR zelf. Volgens het Cyber Monitoring Centre raakte de aanval 5.000 organisaties, vooral toeleveranciers en dealers.[307] Het duurde weken voordat de problemen door de cyberaanval helemaal waren opgelost. Bij de aanval zijn ook salarisgegevens van medewerkers gestolen. De aanval zou het Verenigd Koninkrijk 1,9 miljard Britse pond, omgerekend 2,2 miljard euro, hebben gekost. Het bedrijf heeft zelf zwaar verlies geleden door de cyberaanval. [308] De aanval zorgde ook voor (financiële) problemen bij leveranciers van JLR. De aanval werd geclaimd door de hackers van Scattered Lapsus$ Hunters.[309] In juni 2026 berichtte The New York Times dat het om een geavanceerde ransomware-aanval zou gaan, waarbij de hackers misbruik hebben gemaakt van kwetsbaarheden in verouderde technologie.[310]

Vermoedelijke staatshackers compromitteren groot Amerikaans telecombedrijf
Ribbon Communications, een leverancier van telecommunicatiediensten aan de Amerikaanse overheid en telecombedrijven wereldwijd, heeft in een rapportage aan de SEC melding gemaakt van een hack. Ribbon ontdekte de aanval in september 2025, maar de hackers zouden mogelijk al toegang tot de systemen hebben verkregen in december 2024. Ribbon stelt geen bewijs te hebben dat de hackers toegang hebben gehad tot materiële informatie. Wel hadden de hackers toegang tot enkele klantbestanden. De aanvallers zijn vermoedelijk gelinkt aan een staat, sommige media stellen dat het mogelijk gaat om Chinese staatshackers.[311]

Oktober 2025

Data gestolen bij Zweedse netbeheerder na inbraak op filesharingsysteem
Criminelen van de ransomwaregroep Everest wisten in te breken op een filesharingsysteem van de Zweedse netbeheerder Svenska Kraftnät. Daarbij werd 280 gigabyte data buitgemaakt. De data werd tijdelijk te koop aangeboden, maar werd later door de criminelen teruggetrokken omdat zij concludeerden dat deze data niet 'waardevol' was.[312] Volgens de netbeheerder is de energievoorziening niet in het geding geweest.[313]

Hacktivisten manipuleren systemen na aanval op industriële controlesystemen van Canadese olie- en gasbedrijven
Volgens de Canadese overheid hebben hacktivisten industriële controlesystemen van een olie- en gasbedrijf, waterbedrijf en een graansilo in Canada aangevallen. Bij de watervoorziening wisten de aanvallers de waterdrukkleppen aan te passen, waardoor er slechtere dienstverlening was voor de gemeenschap die door de gecompromitteerde faciliteit werd bediend. Bij een Canadees olie- en gasbedrijf knoeiden de hacktivisten met een geautomatiseerde tankmeter (ATG), waardoor er valse alarmen ontstonden. In het geval van de graansilo wisten de hackers de temperatuur- en vochtigheidsparameters in de graandroogsilo te manipuleren. Het Canadese Centre for Cyber Security gaf geen verdere details over de aanvallen of de verantwoordelijke hacktivisten.[314]

November 2025

Korte verstoringen van websites Belgische telecombedrijven na DDoS-aanvallen door pro-Russisch hackerscollectief
Begin november voerden pro-Russische hackers DDoS-aanvallen uit op onder meer de websites van telecomoperatoren Proximus en Scarlet. Ook het Universitair Ziekenhuis Gent was slachtoffer van een aanval. De organisaties spraken van korte, lichte verstoringen. Er waren geen gevolgen voor patiënten en gebruikers.[315]

Data van minstens tweehonderd Salesforce-klanten gestolen via applicatie(s) van leverancier
Google stelt dat hackers in een grote supply chain-aanval Salesforce-data hebben gestolen van meer dan 200 bedrijven. De aanvallers wisten de data te bemachtigen via applicaties van Gainsight. Via een koppeling tussen de Gainsight-applicaties en Salesforce kan data uit het CRM-systeem binnen de Gainsight-omgeving beschikbaar komen. Aanvallers hebben via deze koppeling bij allerlei organisaties gegevens uit hun Salesforce-systeem weten te stelen. De aanval is opgeëist door Scattered Lapsus$ Hunters (SLH). Google stelt dat ShinyHunters verantwoordelijk is. SLH eiste specifiek de verantwoordelijkheid op voor hacks op Atlassian, CrowdStrike, Docusign, F5, GitLab, LinkedIn, Malwarebytes, SonicWall, Thomson Reuters en Verizon. Google heeft de slachtoffers niet bij naam genoemd. De hackers zouden toegang hebben gekregen tot Gainsight dankzij hun vorige hackcampagne gericht op Salesloft Drift. Gainsight was één van de organisaties die bij deze aanval werden getroffen. Het bedrijf zou zelf zo'n 1.000 klanten hebben, waaronder bekende (technologie)bedrijven.[316]

Deense partijwebsites aan vooravond van verkiezingen kortstondig offline door DDoS-aanvallen
DDoS-aanvallen hebben, aan de vooravond van de lokale verkiezingen, websites van Deense politieke partijen en de overheid kortstondig offline gehaald. De incidenten hebben de stemming niet verstoord. De aanvallen werden geclaimd door pro-Russische hacktivisten.[317]

December 2025

Russische hackers verstoorden communicatie Poolse energie-installaties, ontwrichtende gevolgen blijven uit
In de laatste week van december werd het Poolse elektriciteitssysteem getroffen door een grote cyberaanval, waarbij minstens 30 wind- en zonneparken en een grote warmtekrachtcentrale (wkc) slachtoffer werden. Daarnaast werd ook een productiebedrijf aangevallen. De hackers verstoorden de communicatie van de duurzame energie-installaties met de netbeheerder, maar de elektriciteitsproductie ging gewoon door. De aanvallers zetten twee soorten wiper malware in. In het geval van de wkc werd het destructieve malwareproces geblokkeerd. Bij de wipe rmalware die tegen het productiebedrijf werd ingezet vermoedt CERT.PL dat de kernfunctionaliteit voor het wissen van bestanden is ontwikkeld met behulp van een LLM.[318] Volgens de Poolse minister van Energie ging het om de grootste cyberaanval in jaren.[319] Ook stelde Polen dat de aanval een bewuste poging zou zijn om de energievoorziening te saboteren. Dit is niet gelukt. Polen, diverse cybersecuritybedrijven en de Europese Unie hebben de aanval geattribueerd aan Rusland.[320]

Warmtekrachtcentrale Polen ontregeld door cyberaanval
Parallel aan de aanval op Poolse energie-infrastructuur waarbij o.a. 30 wind- en zonneparken werden getroffen, vond er in Polen nog een incident plaats bij een warmtekrachtkoppelingsinstallatie. Het Poolse CERT stelt dat er een aanval op een andere warmtekrachtkoppeling plaatsvond en dat de aanvallers in staat waren om tijdelijk een stoomturbine en een waterbehandelingssysteem te verstoren. Omdat er ten tijde van de aanval onderhoudswerkzaamheden werden uitgevoerd, werd aanvankelijk gedacht dat de uitval van systemen werd veroorzaakt door die werkzaamheden. Het personeel herstelde de systemen snel, waardoor er geen uitval van warmte- of stroomlevering optrad.[321]

Data gestolen na hack van 'externe servers' van ESA
Het Europees Ruimtevaartagentschap (ESA) heeft bevestigd dat aanvallers eind 2025 servers buiten het bedrijfsnetwerk hebben gehackt. Deze servers bevatten wat het agentschap omschreef als 'niet-geclassificeerde' informatie over gezamenlijke technische activiteiten. Het bericht van ESA volgt op een claim van een hacker op BreachForums die stelde dat hij servers van de organisatie had gehackt en daarbij 200 GB aan data had gestolen.[322]

Hackers stelen data van Mexicaanse overheidssystemen
Aanvallers hebben tien Mexicaanse overheidsinstanties en een financiële instelling gehackt, waaronder de Mexicaanse belastingdienst. Daarbij wisten de aanvallers meer dan 150 GB aan data te stelen van diverse systemen. Volgens onderzoekers hebben de aanvallers een AI-assistent misbruikt om exploits te ontwikkelen, aangepaste tools te creëren en automatisch data te stelen.[323]

Januari 2026

Onbekende actor voert cyberaanval uit op water- en rioleringsbedrijf in Mexico
Een onbekende cyberactor voerde deze maand een cyberaanval uit op een water- en rioleringsbedrijf in Mexico. De aanval maakt volgens onderzoekers deel uit van een bredere campagne tussen december 2025 en februari 2026. Wat deze aanval(len) onderscheidde van typische cyberaanvallen is de centrale rol die AI heeft gespeeld. Anthropic's Claude en OpenAI's GPT-modellen fungeerden samen als een door AI ondersteunde operationele motor. De aanvaller gebruikte de commerciële AI-tools om kernactiviteiten van de aanval te versnellen.[324]

Iraanse staatshackers voeren aanvallen uit met ransomware
Onderzoekers hebben ontdekt dat Iraanse staatshackers, die gevolgd worden als MuddyWater, Chaos-ransomware inzetten bij cyberaanvallen. Daarbij stellen de onderzoekers dat dit een dekmantel is voor vermeende spionage- en datadiefstaloperaties. Het is niet bekend welke organisaties in welke landen zijn getroffen.[325]

Operaties en consultaties Belgische ziekenhuizen uitgesteld na ransomware-aanval
Begin januari werden de ziekenhuizen van AZ Monica in Deurne en Antwerpen slachtoffer van een ransomware-aanval. Alle servers werden uitgeschakeld, waardoor onder meer patiëntendossiers niet beschikbaar waren. Alle operaties en niet-dringende consultaties werden uitgesteld en acute zorg werd tot een minimum beperkt.[326] Door de aanval moest het personeel terugvallen op pen en papier.[327] Na een ruime maand waren de systemen van de ziekenhuizen hersteld.[328]

Maart 2026

Open source kwetsbaarhedenscanner Trivy voorzien van infostealer-malware
Kwaadwillenden hebben open source vulnerability scanner Trivy voorzien van infostealer-malware via een supplychain aanval. Het inplanten van een infostealer in de vulnerability scanner gebeurde via buitgemaakte inloggegevens voor de GitHub-repository van Trivy-maker Aqua Security. De hackers van TeamPCP zouden verantwoordelijk zijn voor de compromittatie.[329]

Data gestolen van EU-hostingplatform door ShinyHunters
Hackers van ShinyHunters hebben weten in te breken op het europa.eu-hostingplatform. Daarbij is zo'n 91,7 GB aan data in gecomprimeerde vorm gestolen. Dat komt neer op 340 GB aan data zonder compressie. De data is afkomstig van de websites die worden gehost op het europa.eu-platform, dat zijn 42 sites van de Europese Commissie en 29 sites van andere EU-organisaties. Het gaat daarbij om namen, e-mailadressen en gebruikersnamen. Het lijkt erop dat een groot deel van de data al publiek beschikbaar was. Volgens CERT-EU hebben de hackers initiële toegang verkregen via de Trivy supply-chain compromittatie.[330]

Axios npm-pakket voorzien van malware na hack door Noord-Koreaanse hackers
Aanvallers zijn erin geslaagd om de npm-package van de populaire HTTP client library Axios te voorzien van malware. Axios is een HTTP client library die meer dan honderd miljoen wekelijkse downloads heeft. De hackers wisten het primaire maintainer account van Axios te compromitteren via een social engineering-aanval. Vervolgens werden malafide versies van het npm-pakket uitgebracht. Deze versies installeerden een RAT bij de gebruikers. Volgens Google is de aanval het werk van een aan Noord-Korea gelinkte groep hackers.[331] Een van de organisaties die getroffen zijn door de compromittatie van Axios is OpenAI. Deze heeft uit voorzorg besloten om het code signing certificaat, dat het gebruikt voor het signeren van macOS-apps, te vervangen.[332]

Wereldwijde netwerkuitval bij medische fabrikant Stryker na aanval door pro-Iraanse hackers
Fabrikant van medische apparatuur Stryker, een Amerikaans bedrijf dat wereldwijd actief is, heeft bevestigd dat het slachtoffer is geworden van een cyberaanval. De verklaring van Stryker volgde op berichten die (op sociale media) werden verspreid door medewerkers die stelden dat zakelijke computers en telefoons zouden zijn gewist. De pro-Iraanse hackersgroep Handala claimde de aanval en stelde dat het naast het wissen van 200.000 systemen ook 50 GB aan data heeft gestolen.[333] Twee weken na de cyberaanval maakte het bedrijf bekend dat het de productie weer zou gaan opstarten.[334]

April 2026

Persoonsgegevens gestolen bij Franse instantie die identiteitsbewijzen uitgeeft
Een cyberaanval op de website van de Nationale Dienst voor Veilige Documenten (ANTS) heeft geleid tot een datalek. ANTS is een overheidsdienst die verantwoordelijk is voor de verwerking van aanvragen voor paspoorten, nationale identiteitskaarten, verblijfsvergunningen en rijbewijzen. Volgens het Franse ministerie van Binnenlandse Zaken werd op 15 april een "beveiligingsincident dat mogelijk de openbaarmaking van gegevens van zowel individuele als zakelijke accounts met zich meebrengt" ontdekt. Uit een eerste analyse blijkt dat mogelijk verschillende soorten persoonlijke informatie, gekoppeld aan individuele gebruikersaccounts, zijn gestolen. De mogelijk gecompromitteerde gegevens omvatten inloggegevens, namen, e-mailadressen, geboortedata en de unieke identificatiecode van elk account. De Franse autoriteiten hebben het ANTS-incident nog niet aan een specifieke dader toegeschreven en hebben ook nog geen mogelijk motief voor de aanval bekendgemaakt. Een hackerscollectief met de naam 'breach3d' heeft de verantwoordelijkheid voor de aanval opgeëist. De hackers claimen gegevens van 19 miljoen personen te hebben gestolen, die te koop worden aangeboden. Voor zover bekend is de data nog niet verspreid.[335]

Mei 2026

Hackers stelen patiëntdata van Duitse ziekenhuizen via externe dienstverlener
Na een cyberaanval op een externe facturatiedienstverlener kregen diverse Duitse universitaire ziekenhuizen te maken met een grootschalig datalek van patiëntgegevens. De aanval trof Unimed, een bedrijf dat namens talrijke Duitse ziekenhuizen de facturatie verzorgt voor particulier verzekerde en zelfbetalende patiënten. Volgens het bedrijf ging het waarschijnlijk om een ransomware-aanval. De omvang van het datalek verschilde per ziekenhuis, maar het gaat om honderdduizenden getroffen patiënten. Daarvan zijn factuurgegevens gestolen die in sommige gevallen betrekking hadden op diagnoses en/of behandelingen.[336]

Juni 2026

ShinyHunters claimt datadiefstal bij Raad van Europa
ShinyHunters claimt de Raad van Europa te hebben gehackt en daarbij bijna 300 GB aan data te hebben gestolen. Het zou gaan om meer dan 429.000 bestanden van verschillende afdelingen, waaronder HR, het secretariaat, de parlementaire vergadering en het Europees directoraat voor de kwaliteit van geneesmiddelen en gezondheidszorg. De hackers zouden misbruik hebben gemaakt van een zero-day kwetsbaarheid in Oracle PeopleSoft.[337] De Raad van Europa heeft de datadiefstal niet bevestigd, maar heeft wel aangegeven onderzoek te doen.[338]

Data gestolen bij waterbedrijf in Amerika, hackers claimen mogelijkheid tot verstoringen
De pro-Iraanse hackersgroep Handala claimde het Amerikaanse waterbedrijf California Water Service (Cal Water) te hebben gehackt. Daarbij zouden zij 5 GB aan data hebben gestolen. Ook beweerden de hackers dat zij de mogelijkheid hadden om de watervoorziening te verstoren, maar dat zij dit niet hebben gedaan.[339] Cal Water zelf maakte later bekend dat de OT-systemen niet waren gehackt.[340]

Juli 2026

AI-modellen OpenAI breken uit testomgeving en voeren autonoom aanval uit op Hugging Face
Open-source AI-platform Hugging Face is slachtoffer geworden van een digitale aanval die volledig door autonome AI-agents werd uitgevoerd. [341] Tijdens een test vonden ongeveer 1.200 AI-agents, die van elkaar geïsoleerd hadden moeten blijven, een manier om via een forum met elkaar te communiceren. Zij wisselden grote hoeveelheden berichten en bestanden uit. Ook ontdekte een van de agents dat ze via een exploit bredere toegang tot het internet konden krijgen. Uiteindelijk voerden 700 agents onbedoeld een cyberaanval uit op het open-source AI-platform Hugging Face. Uit onderzoek van OpenAI en twee onderzoeksinstituten blijkt dat de agents elkaar, om bijvoorbeeld hun opdrachten uit te kunnen voeren, vragen stelden, samenwerkten, taken uitbesteedden en elkaar beïnvloedden.[342] Uiteindelijk vonden ze een kwetsbaarheid bij Hugging Face, die ze hackten omdat ze dachten daar antwoorden te kunnen vinden waarmee ze goed konden scoren in de test.[343]

Bedrijven gehackt nadat AI-modellen ontsnappen uit testomgeving
Tijdens evaluaties van AI-modellen door het bedrijf Irregular zijn modellen van Meta en Anthropic ontsnapt uit hun testomgeving en hebben zij echte bedrijven gehackt. Volgens Meta heeft een van zijn AI-modellen door een configuratiefout toegang verkregen tot het publieke internet, waarna het een kwetsbaarheid in de systemen van een niet nader genoemd bedrijf heeft geëxploiteerd.[344] Ook modellen van Meta en Anthropic kregen door een fout toegang tot het internet. Vervolgens wisten zij toegang te krijgen tot systemen van echte bedrijven.[345] Deze incidenten houden verband met de aanvallen door AI-modellen van OpenAI (zoals hierboven beschreven). Ook in dat geval werden de evaluaties uitgevoerd door Irregular.

Taiwanese (overheids)organisaties aangevallen met behulp van autonome AI
In juli hebben cybersecurityonderzoekers een digitale aanval ontdekt op Taiwanese (overheids)organisaties. De hackers zouden open-source AI-agents hebben gebruikt om een autonome hacktool te bouwen. Deze tool zou functioneren als een gecoördineerd cyberteam. De agents brachten 21 overheidssystemen in kaart, onderzochten kwetsbaarheden en pasten hun tactiek aan wanneer ze werden geblokkeerd. Op deze manier zouden minstens 85 overheidsaccounts zijn gehackt en bemachtigde de actor persoonsgegevens van meer dan 2.500 personen. Daarnaast breidde de aanval zich uit naar het Taiwanese agentschap voor nucleaire veiligheid en minstens zeven energiebedrijven. In de media wordt gesteld dat mogelijk Chinese hackers verantwoordelijk zijn.[346] Taiwan heeft bevestigd dat het *AI-assisted* aanvallen heeft waargenomen, maar heeft deze niet geattribueerd.[347]

Augustus 2026

Verstoringen watervoorziening na cyberaanvallen op waterbedrijven in de VS
In juli en augustus maakten verschillende Amerikaanse staten bekend dat waterbedrijven en waterzuiveringsinstallaties in hun staat waren getroffen door cyberaanvallen.[348] Volgens een rapport van CISA zijn meer dan honderd systemen getroffen. De aanvallen richtten zich op programmable logic controllers (PLC's).[349] Deze PLC's sturen verschillende processen in het watersysteem aan, zoals bijvoorbeeld het toevoegen van chemicaliën.[350] De PLC's waren onvoldoende beveiligd. In sommige gevallen werd de watervoorziening beïnvloed, wat bijvoorbeeld leidde tot drukverlies.[351] De veiligheid van drinkwater zou niet in het geding zijn geweest. De Amerikaanse CISA attribueert de aanvallen aan Iraanse hackers.[352]

Iraanse hackers legden Britse elektriciteitscentrale vier dagen plat
Aan Iran gelieerde hackers hebben volgens berichtgeving in The Telegraph een Britse elektriciteitscentrale vier dagen buiten werking gesteld. Het zou de eerste keer zijn dat dergelijke actoren erin slagen een Britse energiecentrale stil te leggen. De aanval vond rond dezelfde tijd plaats als de aanvallen op Amerikaanse waterbedrijven (zie hierboven). Welke centrale precies is getroffen, hebben de Britse autoriteiten om veiligheidsredenen niet bekendgemaakt.[353] Wel hebben ze bevestigd dat het om een kleinschalige energiecentrale gaat. Daardoor had de storing geen gevolgen voor het bredere Britse elektriciteitsnet. De Britse overheid heeft de aanval zelf niet formeel aan Iran geattribueerd.[354]

Bijlage 1
Verantwoording

Het Cybersecuritybeeld Nederland wordt jaarlijks vastgesteld door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Daarbij wordt dankbaar gebruikgemaakt van de informatie, de inzichten en de expertise van overheidsdiensten, kritieke entiteiten, de wetenschap en andere partijen.

De totstandkoming van het CSBN kent drie fasen:

1. Analyseren

De NCTV verzamelt en analyseert relevante informatie over incidenten, trends en verschuivingen op het gebied van de driehoek belang, dreiging en weerbaarheid. De volgende vragen liggen ten grondslag aan het CSBN:

- Welke relevante incidenten hebben in de periode van augustus 2025 tot en met augustus 2026 in Nederland of in vergelijkbare landen plaatsgevonden en tot welke nieuwe inzichten leiden die?
- Welke bredere politieke, economische, sociale en technologische ontwikkelingen en factoren hebben naar verwachting de komende jaren invloed op digitale veiligheid? Welke ontwikkelingen kunnen gamechangers zijn?
- Welke veranderingen zijn te identificeren in digitale dreigingen die de nationale veiligheid aantasten? Denk hierbij aan de aard en omvang van de dreiging, doelwitten, actoren, kwetsbaarheden, vormen van uitval en werkwijzen actoren.
- Welke veranderingen zijn te identificeren die van invloed zijn op belangen die kunnen worden aangetast wanneer cyberincidenten zich voordoen? En wat kan de impact daarvan zijn? Welke veranderingen zijn te identificeren in de mate waarin Nederland weerbaar is tegen die digitale dreigingen?
- In hoeverre treden veranderingen op in de grootste risico's voor de nationale veiligheid van Nederland?

Analisten van de NCTV hebben aan de hand van deze vragen een eerste inventarisatie van 'ingrediënten' voor het CSBN gemaakt. Deze zijn in een drietal sessies besproken met experts van publieke organisaties en aangevuld met inzichten.

2. Schrijven en collegiaal toetsen

Na afronding van de analysefase zijn conceptteksten geschreven door afzonderlijke auteurs. Het jaarbeeld is getoetst bij collega's van de NCTV, het NCSC, de AIVD en de MIVD. Op verschillende onderdelen is actief meegeschreven door het NCSC, de AIVD, de MIVD en THTC.

3. Valideren

Het CSBN kent een uitgebreid validatietraject, waarbij de concepttekst ter commentaar wordt voorgelegd aan interne en externe partners. Het betreft onder andere experts vanuit de wetenschap, expertise-instituten, kritieke entiteiten, belangenverenigingen en overheidsorganisaties. Na het verwerken van het verzamelde commentaar wordt de definitieve tekst opgemaakt en door de NCTV vastgesteld. Na de publicatie van het CSBN vindt een primair interne evaluatie plaats. De verzamelde feedback wordt vervolgens verwerkt in het CSBN-traject van het volgende jaar.

Bijlage 2
Bronnen

1 Rusland voert cybercampagne uit tegen Signal- en Whatsapp-accounts, AIVD, 9 maart 2026, https://www.aivd.nl/actueel/nieuws/2026/03/09/rusland-voert-cybercampagne-uit-tegen-signal--en-whatsapp-accounts
Kamerbrief Betreft Cyberadvies over Russische spionageoperaties op IP-camera's, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 10 juli 2026, https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2026Z16096&did=2026D36428.

2 Bedrijf dat software levert voor patiëntendossiers aangevallen door hackers, NOS Nieuws, 7 april 2026, https://nos.nl/artikel/2609548-bedrijf-dat-software-levert-voor-patientendossiers-aangevallen-door-hackers.

3 Odido en het tijdperk waarin data het grootste doelwit is, Emerce, 25 februari 2026, https://www.emerce.nl/wire/odido-tijdperk-waarin-data-grootste-doelwit.

4 Claude AI Guided Hackers Toward OT Assets During Water Utility Intrusion, SecurityWeek, 7 mei 2026, https://www.securityweek.com/claude-ai-guided-hackers-toward-ot-assets-during-water-utility-intrusion/.

5 Disrupting the first reported AI-orchestrated cyber espionage campaign, Anthropic, 13 november 2025, https://www.anthropic.com/news/disrupting-AI-espionage.

6 Five Eyes Cyber Security Agencies Statement, CISA, 22 juni 2026, https://www.cisa.gov/news-events/news/five-eyes-cyber-security-agencies-statement
AI is changing the economics of vulnerability discovery. Defenders should adapt now, CERT-EU, 21 april 2026, https://www.cert.europa.eu/blog/ai-vulnerability-discovery-defenders-must-adapt
Look What You Made Us Patch: 2025 Zero-Days in Review, Google Threat Intelligence Group, 5 maart 2026, https://cloud.google.com/blog/topics/threat-intelligence/2025-zero-day-review
The Attack Cycle is Accelerating: Announcing the Rapid7 2026 Global Threat Landscape Report, Rapid7 Labs, 18 maart 2026, https://www.rapid7.com/blog/post/tr-accelerating-attack-cycle-2026-global-threat-landscape-report/.

7 Cyberweerbaar Nederland 2026 - Inzicht in digitale weerbaarheid, beleid en blinde vlekken door de ogen van IT- en securityprofessionals, KPN, januari 2026, https://www.kpn.com/zakelijk/thedigitaldutch/blog/cyberweerbaar-nederland
Van kwetsbaar naar weerbaar. Geleerde lessen uit dreigende acute en langdurige uitval van uitbestede ICT-dienstverlening bij overheidsorganisaties, ABDTOPConsult, 12 september 2025, https://www.rijksoverheid.nl/documenten/rapporten/2025/09/12/rapport-van-kwetsbaar-naar-weerbaar.

8 Hunt & Hackett 2026 Cyber Trend Report, Hunt & Hackett, 2026, https://www.huntandhackett.com/2026-cyber-trend-report
Cyberweerbaar Nederland 2026 - Inzicht in digitale weerbaarheid, beleid en blinde vlekken door de ogen van IT- en securityprofessionals, KPN, januari 2026, https://www.kpn.com/zakelijk/thedigitaldutch/blog/cyberweerbaar-nederland.

9 Cybersecurity in 2026: ai-versnelling, geopolitieke druk en groeiende digitale ongelijkheid, Computable, 6 februari 2026, https://www.computable.be/2026/02/06/cybersecurity-in-2026-ai%E2%80%91versnelling-geopolitieke-druk-en-groeiende-digitale-ongelijkheid/.

10 Dreigingsbeeld Statelijke Actoren 2025, AIVD, MIVD & NCTV, 2025, https://www.nctv.nl/documenten/2025/07/17/dreigingsbeeld-statelijke-actoren-2025.

11 Openbaar Jaarverslag 2025, AIVD, 23 april 2026, https://www.aivd.nl/documenten/2026/04/23/jaarverslag-2025
Openbaar Jaarverslag 2025, MIVD, 21 april 2026, https://www.defensie.nl/documenten/2026/04/21/openbaar-jaarverslag-2025-militaire-inlichtingen--en-veiligheidsdienst
CrowdStrike 2026 Global Threat Report, CrowdStrike, 24 februari 2026, https://www.crowdstrike.com/en-us/global-threat-report/
2026 OT Cybersecurity Year in Review, Dragos, 17 februari 2026, https://www.dragos.com/ot-cybersecurity-year-in-review
Beyond the Battlefield: Threats to the Defense Industrial Base, Google Threat Intelligence Group, 10 februari 2026, https://cloud.google.com/blog/topics/threat-intelligence/threats-to-defense-industrial-base
M-Trends 2026 Report, Mandiant, 23 maart 2026, https://cloud.google.com/security/resources/m-trends
Finnish intelligence warns of persistent cyber espionage from Russia, China, The Record, 10 maart 2026, https://therecord.media/finnish-intel-warns-espionage-china-russia
UK says three-quarters of cyberattacks on critical systems are linked to hostile states, Reuters, 17 juni 2026, https://www.usnews.com/news/world/articles/2026-06-17/uk-says-three-quarters-of-cyberattacks-on-critical-systems-are-linked-to-hostile-states
Joint statement on malicious cyber activity targeting Canadian critical infrastructure, Regering Canada, 26 november 2025, https://www.canada.ca/en/communications-security/news/2025/11/joint-statement-on-malicious-cyber-activity-targeting-canadian-critical-infrastructure.html.

12 Cybersecuritybeeld Nederland 2025, NCTV, 26-11-2025, https://www.nctv.nl/documenten/2025/11/26/cybersecuritybeeld-nederland-2025.

13 Dreigingsbeeld Statelijke Actoren 2025, AIVD, MIVD & NCTV, 2025, https://www.nctv.nl/documenten/2025/07/17/dreigingsbeeld-statelijke-actoren-2025.

14 Dreigingsbeeld Statelijke Actoren 2025, AIVD, MIVD & NCTV, 2025, https://www.nctv.nl/documenten/2025/07/17/dreigingsbeeld-statelijke-actoren-2025.

15 Trendanalyse Nationale Veiligheid 2024 – Hoofdrapport, Analistennetwerk Nationale Veiligheid, 25 juni 2024, https://www.nctv.nl/documenten/rapporten/2024/06/25/hoofdrapport-trendanalyse-nationale-veiligheid-2024
Nederland in een fragmenterende wereldorde, WRR, 1 juli 2024, https://www.wrr.nl/publicaties/rapporten/2024/07/01/nederland-in-een-fragmenterende-wereldorde.

16 Hybride dreigingen en maatschappelijke weerbaarheid, Adviesraad Internationale Vraagstukken, 4 juni 2024, https://www.adviesraadinternationalevraagstukken.nl/documenten/2024/06/04/hybride-dreigingen-en-maatschappelijke-weerbaarheid.

17 Dreigingsbeeld Statelijke Actoren 2025, AIVD, MIVD & NCTV, 2025, https://www.nctv.nl/documenten/2025/07/17/dreigingsbeeld-statelijke-actoren-2025.

18 New Technologies, Changing Strategies: Five Trends in the Hybrid Threat Landscape, HCSS en TNO, mei 2024, https://hcss.nl/wp-content/uploads/2024/05/New-Technologies-Changing-Strategies-Hybrid-Threats-HCSS-TNO-2024.pdf.

19 New Amazon Threat Intelligence findings: Nation-state actors bridging cyber and kinetic warfare, CJ Moses, 19 november 2025, https://aws.amazon.com/blogs/security/new-amazon-threat-intelligence-findings-nation-state-actors-bridging-cyber-and-kinetic-warfare/.

20 Openbaar Jaarverslag 2025, AIVD, 23 april 2026, https://www.aivd.nl/documenten/2026/04/23/jaarverslag-2025.

21 Defensie Cyberstrategie 2025, Ministerie van Defensie, 3 oktober 2025, https://www.defensie.nl/site/binaries/site-content/collections/documents/2025/10/03/defensie-cyber-strategie-2025/Defensie+Cyberstrategie+-+openbaar.pdf.

22 Exclusive: US used cyber weapons to disrupt Iranian air defenses during 2025 strikes, The Record, 4 februari 2026, https://therecord.media/iran-nuclear-cyber-strikes-us
Israel performs largest cyberattack in history against Iran, The Jerusalem Post, 28 februari 2026, https://www.jpost.com/israel-news/defense-news/article-888271.

23 Dreigingslandschap Vitale Infrastructuur, NCTV, 24 juli 2025, https://www.nctv.nl/documenten/2025/07/23/dreigingslandschap-vitale-infrastructuur
Sandworm Cyberattackers Down Ukrainian Power Grid During Missile Strikes, Dark Reading, 9 november 2023, https://www.darkreading.com/ics-ot-security/sandworm-cyberattackers-ukrainian-power-grid-missile-strikes
NSA, Viasat say 2022 hack was two incidents; Russian sanctions resulted from investigation, The Record, 11 augustus 2023, https://therecord.media/viasat-hack-was-two-incidents-and-resulted-in-sanctions
Israël hackte jarenlang verkeerscamera's in Teheran om Khamenei in de gaten te houden, Financial Times (herdrukt in Nederlandse media), 3 maart 2026, https://www.timesofisrael.com/report-israel-hacked-tehran-traffic-cameras-to-track-khamenei-ahead-of-assassination/.

24 How Will Cyber Warfare Shape the U.S.-Israel Conflict with Iran?, CSIS (Lauryn Williams & Kuhu Badgi), 3 maart 2026, https://www.csis.org/analysis/how-will-cyber-warfare-shape-us-israel-conflict-iran
Iran shut down British power plant for four days in unprecedented cyber attack, BBC, 23 augustus 2026, https://www.bbc.com/news/articles/c5yr0576ygvo.

25 Dreigingsbeeld militaire en hybride dreigingen, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, AIVD en MIVD, 6 december 2024, https://www.nctv.nl/documenten/publicaties/2024/12/06/dreigingsbeeld-hybride-en-militaire-dreigingen.

26 Openbaar Jaarverslag 2025, AIVD, 23 april 2026, https://www.aivd.nl/documenten/2026/04/23/jaarverslag-2025.

27 Openbaar Jaarverslag 2025, MIVD, 21 april 2026, https://www.defensie.nl/documenten/2026/04/21/openbaar-jaarverslag-2025-militaire-inlichtingen--en-veiligheidsdienst.

28 Openbaar Jaarverslag 2025, MIVD, 21 april 2026, https://www.defensie.nl/documenten/2026/04/21/openbaar-jaarverslag-2025-militaire-inlichtingen--en-veiligheidsdienst.

29 Openbaar Jaarverslag 2025, AIVD, 23 april 2026, https://www.aivd.nl/documenten/2026/04/23/jaarverslag-2025.

30 Openbaar Jaarverslag 2025, MIVD, 21 april 2026, https://www.defensie.nl/documenten/2026/04/21/openbaar-jaarverslag-2025-militaire-inlichtingen--en-veiligheidsdienst.

31 Cybersecuritybeeld Nederland 2025, NCTV, 26-11-2025, https://www.nctv.nl/documenten/2025/11/26/cybersecuritybeeld-nederland-2025
Openbaar Jaarverslag 2025, AIVD, 23 april 2026, https://www.aivd.nl/documenten/2026/04/23/jaarverslag-2025
FBI cyber boss: China's hacker-for-hire ecosystem 'out of control', The Register, 30 april 2026, https://www.theregister.com/2026/04/30/fbi_cyber_boss_chinas_hackerforhire/.

32 Defending Against China-Nexus Covert Networks of Compromised Devices, Cybersecurity & Infrastructure Security Agency (CISA), 23 april 2026, https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-113a.

33 ORB-netwerken en hun impact op de digitale veiligheid in Nederland, NCSC, 10 februari 2025, https://www.ncsc.nl/expertblogs/orb-netwerken-en-hun-impact-op-de-digitale-veiligheid-nederland.

34 Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System, Cybersecurity & Infrastructure Security Agency (CISA), 3 september 2025, https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a
Dozens of Countries Hit in Chinese Telecom Hacking Campaign, Top U.S. Official Says, The Wall Street Journal, 4 december 2024, https://www.wsj.com/politics/national-security/dozens-of-countries-hit-in-chinese-telecom-hacking-campaign-top-u-s-official-says-2a3a5cca
Omvang Chinese cyberoperatie groter dan gedacht: 'Tachtig landen doelwit', BNR, 3 september 2025, https://www.bnr.nl/nieuws/internationaal/10582169/omvang-chinese-cyberoperatie-groter-dan-gedacht-tachtig-landen-doelwit.

35 Chinese hackers dringen met ingenieuze truc binnen in kern van telecomnetwerken, de Volkskrant / Nederlands Dagblad, 26 maart 2026, https://www.volkskrant.nl/wetenschap/chinese-hackers-dringen-met-ingenieuze-truc-binnen-in-kern-van-telecomnetwerken~b3d31874/.

36 Nederlandse providers doelwit van Salt Typhoon, AIVD en MIVD, 28 augustus 2025, https://www.aivd.nl/actueel/nieuws/2025/08/28/nederlandse-providers-doelwit-van-salt-typhoon.

37 BPFdoor in Telecom Networks: Sleeper Cells in the Backbone, Rapid7, 26 maart 2026, https://www.rapid7.com/blog/post/tr-bpfdoor-telecom-networks-sleeper-cells-threat-research-report/.

38 Openbaar Jaarverslag 2025, MIVD, 21 april 2026, https://www.defensie.nl/documenten/2026/04/21/openbaar-jaarverslag-2025-militaire-inlichtingen--en-veiligheidsdienst.

39 Rusland voert cybercampagne uit tegen Signal- en Whatsapp-accounts, MIVD en AIVD, 9 maart 2026, https://www.defensie.nl/actueel/nieuws/2026/03/09/rusland-voert-cybercampagne-uit-tegen-signal--en-whatsapp-accounts
Russische hackers richten zich op Signal-backups via nieuwe phishing-methode, MIVD en AIVD, 30 juni 2026, https://www.defensie.nl/actueel/nieuws/2026/06/30/russische-hackers-richten-zich-op-signal-backups-via-nieuwe-phishing-methode.

40 Rusland voert cybercampagne uit tegen Signal- en Whatsapp-accounts, MIVD en AIVD, 9 maart 2026, https://www.aivd.nl/actueel/nieuws/2026/03/09/rusland-voert-cybercampagne-uit-tegen-signal--en-whatsapp-accounts.

41 Rusland voert cybercampagne uit tegen Signal- en Whatsapp-accounts, Ministerie van Defensie, 9 maart 2026, https://www.defensie.nl/actueel/nieuws/2026/03/09/rusland-voert-cybercampagne-uit-tegen-signal--en-whatsapp-accounts
Russische hackers richten zich op Signal-backups via nieuwe phishing-methode, Ministerie van Defensie, 30 juni 2026, https://www.defensie.nl/actueel/nieuws/2026/06/30/russische-hackers-richten-zich-op-signal-backups-via-nieuwe-phishing-methode.

42 Nederland doelwit van Russische spionageoperatie via IP-camera's, AIVD, 10 juli 2026, https://www.aivd.nl/actueel/nieuws/2026/07/10/nederland-doelwit-van-russische-spionageoperatie-via-ip-cameras.

43 Cyberadvies Russische statelijke actoren compromitteren IP-camera's in Europa voor militaire doeleinden, AIVD en MIVD, 10 juli 2026, https://www.aivd.nl/documenten/2026/07/10/cyberadvies-russische-statelijke-actoren-compromitteren-ip-cameras-in-europa-voor-militaire-doeleinden.

44 Brochure Cyberadvies: Russische statelijke actoren compromitteren IP-camera's in Europa voor militaire doeleinden, AIVD en MIVD, 10 juli 2026, https://www.aivd.nl/documenten/2026/07/10/cyberadvies-russische-statelijke-actoren-compromitteren-ip-cameras-in-europa-voor-militaire-doeleinden.

45 Brochure Cyberadvies: Russische statelijke actoren compromitteren IP-camera's in Europa voor militaire doeleinden, AIVD en MIVD, 10 juli 2026, https://www.aivd.nl/documenten/2026/07/10/cyberadvies-russische-statelijke-actoren-compromitteren-ip-cameras-in-europa-voor-militaire-doeleinden.

46 Brochure Cyberadvies: Russische statelijke actoren compromitteren IP-camera's in Europa voor militaire doeleinden, AIVD en MIVD, 10 juli 2026, https://www.aivd.nl/documenten/2026/07/10/cyberadvies-russische-statelijke-actoren-compromitteren-ip-cameras-in-europa-voor-militaire-doeleinden.

47 Op basis van interne informatie afkomstig van de AIVD.
'APT28 exploit routers to enable DNS hijacking operations', NCSC-UK, april 2026, https://www.ncsc.gov.uk/news/apt28-exploit-routers-to-enable-dns-hijacking-operations.

48 Openbaar Jaarverslag 2025, AIVD, 23 april 2026, https://www.aivd.nl/documenten/2026/04/23/jaarverslag-2025.

49 Cyber / Russia: Statement by the High Representative on behalf of the European Union denouncing Russia's malicious cyber ecosystem targeting the EU, its member states and international partners, Europese Raad van de Europese Unie, 13 juli 2026, https://www.consilium.europa.eu/en/press/press-releases/2026/07/13/cyber-russia-statement-by-the-high-representative-on-behalf-of-the-european-union-denouncing-russia-s-malicious-cyber-ecosystem-targeting-the-eu-its-member-states-and-international-partners/.

50 Energy Sector Incident Report – 29 December, CERT Polska, 30 januari 2026, https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/
Waarom een Russische aanval op Poolse energiebronnen ook een waarschuwing is voor Nederland, de Volkskrant, februari 2026, https://

www.volkskrant.nl/binnenland/waarom-een-russische-aan-val-op-poolse-energiebron-nen-ook-een-waarschu-wing-is-voor-nederland~b212dba0/.

51 Massive cyberattack on Polish power system in December failed, minister says, Reuters, 13 januari 2026, https://www.reuters.com/sustainability/climate-energy/massive-cyberattack-polish-power-system-december-failed-minister-says-2026-01-13/.

52 De beschrijving van deze incidenten is gebaseerd op informatie bekend bij het NCSC.

53 Cybersecuritybeeld Nederland 2025, NCTV, 26 november 2025, https://www.nctv.nl/documenten/2025/11/26/cybersecuritybeeld-nederland-2025.

54 Openbaar Jaarverslag 2025, MIVD, 21 april 2026, https://www.defensie.nl/documenten/2026/04/21/openbaar-jaarverslag-2025-militaire-inlichtingen--en-veiligheidsdienst.

55 Iran MOIS Phishes 50+ Embassies, Ministries, Int'l Orgs, Dark Reading, 4 september 2025, https://www.darkreading.com/cyberattacks-data-breaches/iran-mois-50-embassies-ministries-intl-orgs.

56 Openbaar Jaarverslag 2025, AIVD, 23 april 2026, https://www.aivd.nl/documenten/2026/04/23/jaarverslag-2025.

57 Netwerkstoring bij Stryker na hack: Medische systemen blijven draaien, Dutch IT Channel, 13 maart 2026, https://www.dutchitchannel.nl/news/727265/netwerkstoring-bij-stryker-na-hack-medische-systemen-blijven-draaien
Cyberincident bij medische leverancier Stryker, Z-Cert, 12 maart 2026, https://z-cert.nl/actueel/nieuws/cyberincident-bij-medische-leverancier-stryker.

58 Iran's "Handala": Cyberterrorism or Psychological Terrorism?, Daniel Haberfeld & Gabriel Weimann, Studies in Conflict & Terrorism, juni 2026, https://doi.org/10.1080/1057610X.2026.2680934
Beyond Hacktivism: Iran's Coordinated Cyber Threat Landscape, Center for Strategic & International Studies, 14 januari 2026, https://www.csis.org/blogs/strategic-technologies-blog/beyond-hacktivism-irans-coordinated-cyber-threat-landscape
Handala: MOIS Linked Cyber Influence Ecosystem Threat Intelligence Assessment, DomainTools Investigations, 6 april 2026, https://dti.domaintools.com/research/handala-mois-linked-cyber-influence-ecosystem-threat-intelligence-assessment.

59 Iran's cyber threat may be less 'shock and awe' than 'low and slow,' officials say, The Record, 24 april 2026, https://therecord.media/iran-cyber-warfare-haugh.

60 Openbaar Jaarverslag 2025, AIVD, 23 april 2026, https://www.aivd.nl/documenten/2026/04/23/jaarverslag-2025
Openbaar Jaarverslag 2025, MIVD, 21 april 2026, https://www.defensie.nl/documenten/2026/04/21/openbaar-jaarverslag-2025-militaire-inlichtingen--en-veiligheidsdienst.

61 Openbaar Jaarverslag 2025, AIVD, 23 april 2026, https://www.aivd.nl/documenten/2026/04/23/jaarverslag-2025.

62 North Korea's IT worker scheme funds Russia's war effort, CyberScoop, 21 juli 2026, https://cyberscoop.com/north-korea-it-worker-scheme-funds-russia-war-ukraine/.

63 Openbaar Jaarverslag 2025, AIVD, 23 april 2026, https://www.aivd.nl/documenten/2026/04/23/jaarverslag-2025
Openbaar Jaarverslag 2025, MIVD, 21 april 2026, https://www.defensie.nl/documenten/2026/04/21/openbaar-jaarverslag-2025-militaire-inlichtingen--en-veiligheidsdienst.

64 Alert to Countries, Companies, and Other Entities Regarding North Korean IT Workers, U.S. Department of State, 31 juli 2026, https://www.state.gov/releases/office-of-the-spokesperson/2026/07/alert-to-countries-companies-and-other-entities-regarding-north-korean-it-workers.

65 False Face: Unit 42 Demonstrates the Alarming Ease of Synthetic Identity Creation, Palo Alto Networks Unit 42, april 2025, https://unit42.paloaltonetworks.com/north-korean-synthetic-identity-creation/
North Korean Remote IT Worker Fraud: Managing Insider Threat, Sanctions and Employment Risk, Skadden, Arps, Slate, Meagher & Flom LLP, juni 2026, https://www.skadden.com/insights/publications/2026/06/north-korean-remote-it.

66 Alert to Countries, Companies, and Other Entities Regarding North Korean IT Workers, U.S. Department of State, 31 juli 2026, https://www.state.gov/releases/office-of-the-spokesperson/2026/07/alert-to-countries-companies-and-other-entities-regarding-north-korean-it-workers.

67 Openbaar Jaarverslag 2025, MIVD, 21 april 2026, https://www.defensie.nl/documenten/2026/04/21/openbaar-jaarverslag-2025-militaire-inlichtingen--en-veiligheidsdienst.

68 Openbaar Jaarverslag 2025, AIVD, 23 april 2026, https://www.aivd.nl/documenten/2026/04/23/jaarverslag-2025.

69 Het Cybercrimebeeld Nederland (CCBN) 2026, Politie / Openbaar Ministerie, september 2026, https://fts.politie.nl/cybercrimebeeld/2026/.

70 Cybersecuritybeeld Nederland 2021, NCTV, 28 juni 2021, https://www.nctv.nl/documenten/2021/06/28/cybersecuritybeeld-nederland-2021.

71 Bron: Europol, Internet Organised Crime Threat Assessment (IOCTA) 2026 – How encryption, proxies, and AI are expanding cybercrime, 28 april 2026: https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA-2026.pdf.

72 Iranian MOIS Actors & the Cyber Crime Connection, Check Point Research, 10 maart 2026, https://research.checkpoint.com/2026/iranian-mois-actors-the-cyber-crime-connection/.

73 Dark Covenant 3.0: Controlled Impunity and Russia's Cybercriminals, Recorded Future, 22 oktober 2025, https://www.recordedfuture.com/research/dark-covenant-3-controlled-impunity-and-russias-cybercriminals.

74 Iranian MOIS Actors & the Cyber Crime Connection, Check Point Research, 10 maart 2026, https://research.checkpoint.com/2026/iranian-mois-actors-the-cyber-crime-connection/.

75 Het Cybercrimebeeld Nederland (CCBN) 2026, Politie / Openbaar Ministerie, september 2026, https://fts.politie.nl/cybercrimebeeld/2026/.

76 Datalekkenrapportage 2025 - AI vergroot risico's rond phishing en datalekken, Autoriteit Persoonsgegevens, 8 juli 2026, https://www.autoriteitpersoonsgegevens.nl/rapportages-datalekken.

77 Ransomware-aanvallen: leer van de fouten van anderen, Autoriteit Persoonsgegevens, 28 juli 2026, https://www.autoriteitpersoonsgegevens.nl/en/current/ransomware-attacks-learn-from-the-mistakes-of-others.

78 Cybercrimebeeld Nederland 2024, Openbaar Ministerie en Politie, 11 juni 2024, https://fts.politie.nl/cybercrimebeeld/.

79 Odido en het tijdperk waarin data het grootste doelwit is, Emerce, 25 februari 2026, https://www.emerce.nl/wire/odido-tijdperk-waarin-data-grootste-doelwit
Podcast De Dag: de hack bij Odido, het grootste datalek ooit, NOS, 5 maart 2026, https://nos.nl/artikel/2605048-podcast-de-dag-de-hack-bij-odido-het-grootste-datalek-ooit.

80 Onderwijsplatform Canvas sluit deal met hackersgroep, 'data is verwijderd', Tweakers, 12 mei 2026, https://tweakers.net/nieuws/247724/onderwijsplatform-canvas-sluit-deal-met-hackersgroep-data-is-verwijderd.html.

81 Datalek gemeente Epe, Gemeente Epe, 5 juni 2026, https://www.epe.nl/datalek-gemeente-epe.

82 Op basis van interne informatie afkomstig van politie.
Politie adviseert bedrijven geen losgeld te betalen na cyberaanval, Politie, 26 februari 2026, https://www.politie.nl/nieuws/2026/februari/26/11-politie-adviseert-bedrijven-geen-losgeld-te-betalen-na-cyberaanval.html.

83 Ransomware-aanvallen: leer van de fouten van anderen, Autoriteit Persoonsgegevens, 28 juli 2026, https://www.autoriteitpersoonsgegevens.nl/en/current/ransomware-attacks-learn-from-the-mistakes-of-others.

84 Op basis van interne informatie afkomstig van politie.
Politie adviseert bedrijven geen losgeld te betalen na cyberaanval, Politie, 26 februari 2026, https://www.politie.nl/nieuws/2026/februari/26/11-politie-adviseert-bedrijven-geen-losgeld-te-betalen-na-cyberaanval.html.

85 Waarom zijn er zoveel grote datalekken?, Bits of Freedom, 4 juni 2026, https://www.bitsoffreedom.nl/2026/06/04/waarom-zijn-er-zoveel-grote-datalekken/.

86 Autonomy Levels for Agentic AI, Cloud Security Alliance (Jim Reavis), 28 januari 2026, https://cloudsecurityalliance.org/blog/2026/01/28/levels-of-autonomy.

87 X-Force Threat Intelligence Index 2026, IBM, 2026, https://www.ibm.com/reports/threat-intelligence
Annual Threat Dynamics 2026: Cyber threats in motion, PwC, 24 maart 2026, https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/annual-threat-dynamics.html
2026 Unit 42 Global Incident Response Report, Palo Alto Networks, februari 2026, https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report
Five Eyes Cyber Security Agencies Statement, CISA, 22 juni 2026, https://www.cisa.gov/news-events/news/five-eyes-cyber-security-agencies-statement.

88 Russia-Linked 'GreyVibe' Attackers Use AI to Supercharge Cyberattacks, SecurityWeek, 28 mei 2026, https://www.securityweek.com/russia-linked-greyvibe-attackers-use-ai-to-supercharge-cyberattacks/.

89 AI verlaagt de drempel voor malwareontwikkeling, Dr. Sebastian Schmerl, Arctic Wolf, Techzine.nl, 8 juli 2026, https://www.techzine.nl/experts/security/579880/ai-verlaagt-de-drempel-voor-malwareontwikkeling/.

90 Cybersecuritybeeld Nederland 2025, NCTV, 26 november 2025, https://www.nctv.nl/documenten/2025/11/26/cybersecuritybeeld-nederland-2025.

91 AI verlaagt de drempel voor malwareontwikkeling, Dr. Sebastian Schmerl, Arctic Wolf, Techzine.nl, 8 juli 2026, https://www.techzine.nl/experts/security/579880/ai-verlaagt-de-drempel-voor-malwareontwikkeling/
AI Security Report 2026, Check Point Research, 14 juli 2026, https://research.checkpoint.com/2026/ai-security-report-2026/.

92 A Single Operator, Two AI Platforms, Nine Government Agencies: The Full Technical Report, Gambit Security (Eyal Sela), 10 april 2026, https://gambit.security/blog-posts/a-single-operator-two-ai-platforms-nine-government-agencies-the-full-technical-report.

93 AI in the Breach: How an Adversary Leveraged AI to Target a Water Utility's OT, Dragos (Jay Deen), 6 mei 2026, https://www.dragos.com/blog/ai-assisted-ics-attack-water-utility.

94 'Water and Wastewater Infrastructure Improvements in the Metropolitan Area of Monterrey, Nuevo Leon', North American Development Bank, laatst bekeken op 21 juli 2026, https://nadbank.org/cofidan-projects/water-and-wastewater-infrastructure-improvements-in-the-metropolitan-area-of-monterrey-nuevo-leon.

95 Disrupting the first reported AI-orchestrated cyber espionage campaign, Anthropic, 13 november 2025, https://anthropic.com/news/disrupting-AI-espionage.

96 Disrupting the first reported AI-orchestrated cyber espionage campaign, Anthropic, 13 november 2025, https://anthropic.com/news/disrupting-AI-espionage.

97 Claude Code and DeepSeek Powered Chinese Cyber Espionage Campaign, Security Affairs (Pierluigi Paganini), 16 juli 2026, https://securityaffairs.com/195474/ai/claude-code-and-deepseek-powered-chinese-cyber-espionage-campaign.html.

98 Energy Sector Incident Report – 29 December, CERT Polska, 30 januari 2026, https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/.

99 Review of Generative AI Methods in Cybersecurity, Yagmur Yigit, William J Buchanan, Madjid G Tehrani, Leandros Maglaras, IEEE Access, 2024, https://doi.org/10.1109/ACCESS.2024.3365349.

100 Unveiling VoidLink – A Stealthy, Cloud-Native Linux Malware Framework, Check Point Research, 13 januari 2026, https://research.checkpoint.com/2026/voidlink-the-cloud-native-malware-framework/.

101 New threat actor, UAT-9921, leverages VoidLink framework in campaigns, Cisco Talos (Nick Biasini, Aaron Boyd, Asheer Malhotra, Vitor Ventura), 10 februari 2026, https://blog.talosintelligence.com/voidlink/.

102 A Slopoly start to AI-enhanced ransomware attacks, IBM X-Force, 12 maart 2026, https://www.ibm.com/think/x-force/slopoly-start-ai-enhanced-ransomware-attacks
Hive0163 Uses AI-Assisted Slopoly Malware for Persistent Access in Ransomware Attacks, The Hacker News (Ravie Lakshmanan), 12 maart 2026, https://thehackernews.com/2026/03/hive0163-uses-ai-assisted-slopoly.html.

103 Dark Web Profile: APT28, SOCRadar Cyber Intelligence Inc., 20 januari 2026, https://socradar.io/blog/dark-web-profile-apt28/
GTIG AI Threat Tracker: Advances in Threat Actor Usage of AI Tools, Google Threat Intelligence Group, 5 november 2025, https://cloud.google.com/blog/topics/threat-intelligence/threat-actor-usage-of-ai-tools.

104 UAC-0001 cyberattacks on the security and defense sector using the LAMEHUG software tool, which uses LLM (large language model), CERT-UA (Ukraine Computer Emergency Response Team), 17 juli 2025, https://cert.gov.ua/article/6284730
Incident 1220: LAMEHUG Malware Reportedly Integrates Large Language Model for Real-Time Command Generation in a Purported APT28-Linked Cyberattack, AI Incident Database, juli 2025, https://incidentdatabase.ai/cite/1220/
LameHug: The First Publicly Documented Case of a Malware Integrating a LLM, Picus Security (Sıla Özeren Hacıoğlu), 11 augustus 2025, https://www.picussecurity.com/resource/blog/lamehug-the-first-publicly-documented-case-of-a-malware-integrating-a-llm
Technical Analysis of the LAMEHUG Campaign (APT28), Medium / T3CH (SIMKRA), 30 april / 3 mei 2026, https://medium.com/h7w/technical-analysis-of-the-lamehug-campaign-apt28-4c99b147518c.

105 AI-Powered Cyber Weapons: Preparing for Agentic Malware by 2027, Akitra, 14 oktober 2025, https://akitra.com/blog/ai-powered-cyber-weapons/.

106 JADEPUFFER: Agentic ransomware for automated database extortion, Sysdig Threat Research Team (Michael Clark), 1 juli 2026, https://www.sysdig.com/blog/jadepuffer-agentic-ransomware-for-automated-database-extortion.

107 Zero Day Clock, Sysdig (Sergej Epp), Live dashboard geraadpleegd 5 juli 2026, https://zerodayclock.com/.

108 Dringende oproep door hacken met AI: 'We moeten supersnel kunnen reageren', NOS Nieuws, 22 mei 2026, https://nos.nl/artikel/2615399-dringende-oproep-door-hacken-met-ai-we-moeten-supersnel-kunnen-reageren.

109 The "AI Vulnerability Storm": Building a "Mythos-ready" Security Program, Cloud Security Alliance CISO Community, SANS, [un]prompted, OWASP Gen AI Security Project (co-auteurs o.a. Gadi Evron, Robert T. Lee, Jen Easterly, Bruce Schneier, Chris Inglis, Phil Venables, Heather Adkins, Rob Joyce, Jim Reavis), versie 0.8, 14 april 2026, https://labs.cloudsecurityalliance.org/wp-content/uploads/2026/04/mythosreadyv4.pdf.

110 Anthropic's frontiermodel Mythos vraagt om directe actie, Nationaal Cyber Security Centrum (NCSC), 15 april 2026, https://www.ncsc.nl/nieuws/anthropics-frontiermodel-mythos-vraagt-om-directe-actie.

111 Bedrijfsnetwerk beveiligen, Nationaal Cyber Security Centrum (NCSC), https://www.ncsc.nl/preventieve-beveiligingsmaatregelen/bedrijfsnetwerk-beveiligen
Basisprincipes [De 5 basisprincipes van digitale weerbaarheid], Nationaal Cyber Security Centrum (NCSC), https://www.ncsc.nl/basisprincipes
Anthropic's frontiermodel Mythos vraagt om directe actie, Nationaal Cyber Security Centrum (NCSC), 15 april 2026, https://www.ncsc.nl/nieuws/anthropics-frontiermodel-mythos-vraagt-om-directe-actie.

112 Open Source Security, Nationaal Cyber Security Centrum (NCSC), https://www.ncsc.nl/risicomanagement/open-source-security
Opensourcewerken: veilig, efficiënt en transparant, Digitale Overheid, 6 augustus 2026, https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/open-source/beleid/.

113 New AI models are pushing open-source security to its limits. Their developers must step up., Sara Ann Brackett / Atlantic Council, 16 juni 2026, https://www.atlanticcouncil.org/dispatches/new-ai-models-are-pushing-open-source-security-to-its-limits-their-developers-must-step-up/.

114 The Log4j Incident: A Comprehensive Measurement Study of a Critical Vulnerability, Raphael Hiesgen, Marcin Nawrocki, Thomas C. Schmidt & Matthias Wählisch, IEEE Transactions on Network and Service Management, Vol. 21, No. 6, december 2024, https://doi.org/10.1109/TNSM.2024.3440188.

115 AI is Open Source's Big Moment. Is it Ready?, FOSS Force, 30 maart 2026, https://fossforce.com/2026/03/ai-is-open-sources-big-moment-is-it-ready/.

116 'Mythos-Ready' Security: CSA Urges CISOs to Prepare for Accelerated AI Threats, Kevin Townsend / SecurityWeek, 14 april 2026, https://www.securityweek.com/mythos-ready-security-csa-urges-cisos-to-prepare-for-accelerated-ai-threats/.

117 Mythos Proves Potent in Vulnerability Discovery, Less Convincing Elsewhere, Kevin Townsend / SecurityWeek, 14 mei 2026, https://www.securityweek.com/mythos-proves-potent-in-vulnerability-discovery-less-convincing-elsewhere/
Project Glasswing: Securing critical software for the AI era, Anthropic, 7 april 2026, https://www.anthropic.com/glasswing

Defender's Guide to the Frontier AI Impact on Cybersecurity: May 2026 Update, Lee Klarich / Palo Alto Networks, 13 mei 2026, https://www.paloaltonetworks.com/blog/2026/05/defenders-guide-frontier-ai-impact-cybersecurity-may-2026-update/
Our evaluation of Claude Mythos Preview's cyber capabilities, AI Security Institute (AISI), 13 april 2026, https://www.aisi.gov.uk/blog/our-evaluation-of-claude-mythos-previews-cyber-capabilities.

118 The zero-days are numbered, Bobby Holley / Mozilla, 21 april 2026, https://blog.mozilla.org/en/firefox/privacy-security/ai-security-zero-day-vulnerabilities/.

119 Halen chinese AI-modellen de amerikaanse in? Het is een goede zaak als onze afhankelijkheid van een aantal spelers verkleint, De Standaard, 23 juni 2026, https://www.standaard.be/economie/halen-chinese-ai-modellen-de-amerikaanse-in-het-is-een-goede-zaak-als-onze-afhankelijkheid-van-een-aantal-spelers-verkleint/157645148.html.

120 American A.I. Companies Say Chinese Copycats Are Quickly Catching Up, The New York Times, 6 juli 2026, https://www.nytimes.com/2026/07/06/technology/ai-distillation-china.html.

121 Het Hugging Face-incident en de weg vooruit, OpenAI, 26 augustus 2026, https://openai.com/nl-NL/index/hugging-face-incident-and-the-road-ahead/
Brief independent investigation of agents' behavior, reasoning and collaboration in the OpenAI / Hugging Face hacking incident, METR / Redwood Research, 26 augustus 2026, https://metr.org/hugging-face-incident-report-aug-2026.pdf
Onderzoek: 700 OpenAI-agents hackten Hugging Face, Tweakers, augustus 2026, https://tweakers.net/nieuws/251446/onderzoek-700-openai-agents-hackten-hugging-face.html.

122 OpenAI en Hugging Face werken samen aan beveiligingsincident tijdens modelevaluatie, OpenAI, 21 juli 2026, https://openai.com/index/hugging-face-model-evaluation-security-incident/.

123 Investigating three real-world incidents in our cybersecurity evaluations, Anthropic, 30 juli 2026, https://www.anthropic.com/news/investigating-incidents-cybersecurity-evals
Meta becomes latest firm to say its AI hacked another company, BBC, 6 augustus 2026, https://www.bbc.com/news/articles/cx2kgdnyk2po.

124 A note on this month's Patch Tuesday, Microsoft Security Response Center, 12 mei 2026, https://www.microsoft.com/en-us/msrc/blog/2026/05/a-note-on-patch-tuesday.

125 A note on this month's Patch Tuesday, Microsoft Security Response Center, 12 mei 2026, https://www.microsoft.com/en-us/msrc/blog/2026/05/a-note-on-patch-tuesday
Blame AI: Patch Tuesday Hits Record 206 CVEs, Dark Reading, 9 juni 2026, https://www.darkreading.com/vulnerabilities-threats/blame-ai-patch-tuesday-record-206-cves
Microsoft Plugs Nearly 400 Security Holes, Krebs on Security, 11 augustus 2026, https://krebsonsecurity.com/2026/08/microsoft-plugs-nearly-400-security-holes/
AI Scanning Drove Microsoft's Record 570 July Patches, Enterprise DNA, 17 juli 2026, https://enterprisedna.co/resources/news/microsoft-patch-tuesday-570-ai-vulnerability-discovery-july-2026/
Microsoft dicht bijna duizend beveiligingslekken tijdens patchdinsdag september, Redactie / Security.nl, 9 september 2026, https://www.security.nl/posting/952290/microsoft+dicht+bijna+duizend+beveiligingslekken+tijdens+patchdinsdag+september.

126 Threat Report: When Cyberattacks Happen at AI Speed, Booz Allen Hamilton, 16 maart 2026, https://www.boozallen.com/expertise/cybersecurity/threat-report-when-cyberattacks-happen-at-ai-speed.html.

127 2026 Data Breach Investigations Report, Verizon, 19 mei 2026, https://www.verizon.com/business/resources/T15a/reports/2026-dbir-data-breach-investigations-report.pdf
Ransomware Under Pressure: Tactics, Techniques, and Procedures in a Shifting Threat Landscape, Google Threat Intelligence Group, 16 maart 2026, https://cloud.google.com/blog/topics/threat-intelligence/ransomware-ttps-shifting-threat-landscape/.

128 Sophos Active Adversary Report 2026: Identity attacks dominate as threat groups proliferate, Sophos, 24 februari 2026, https://www.sophos.com/en-us/press/press-releases/sophos-active-adversary-report-2026-identity-attacks-dominate-as-threat-groups-proliferate
2026 CrowdStrike Global Threat Report, CrowdStrike, 24 februari 2026, https://www.crowdstrike.com/en-us/global-threat-report/
State-sponsored actors, better known as the friends you don't want, Cisco Talos, 12 mei 2026, https://blog.talosintelligence.com/state-sponsored-actors-better-known-as-the-friends-you-dont-want/.

129 Cyberadvies. Phishing via chatapps Signal en WhatsApp, AIVD en MIVD, 9 maart 2026, https://www.aivd.nl/documenten/2026/03/09/cyberadvies.-phishing-via-chatapps-signal-en-whatsapp.

130 Het nieuwe Trojaanse paard zit in je dependencies, NCSC Expertblog, 30 juli 2026, https://www.ncsc.nl/expertblogs/het-nieuwe-trojaanse-paard-zit-in-je-dependencies.

131 Kort na 2.0 verschijnt Shai Hulud 3.0 als supply chain-gevaar, Techzine, 31 december 2025, https://www.techzine.nl/nieuws/security/573557/kort-na-2-0-verschijnt-shai-hulud-3-0-als-supply-chain-gevaar/
Glassworm Is Back: A New Wave of Invisible Unicode Attacks Hits Hundreds of Repositories, Aikido, 13 maart 2026, https://www.aikido.dev/blog/glassworm-returns-unicode-attack-github-npm-vscode.

132 Cyberweerbaarheid: een taak voor de hele samenleving, Tilburg University Magazine, 20 maart 2026, https://www.tilburguniversity.edu/nl/magazine/overzicht/cyberweerbaarheid-een-taak-voor-de-hele-samenleving.

133 CSR waarschuwt: kans op digitale ontwrichting is reëel, Cyber Security Raad, 15 januari 2026, https://www.cybersecurityraad.nl/actueel/nieuws/2026/01/15/csr-waarschuwt-kans-op-digitale-ontwrichting-is-reeel
Cyber Security Raad aan nieuw kabinet: Nederland moet meer investeren in digitale veiligheid, Cyber Security Raad, 5 februari 2024, https://www.cybersecurityraad.nl/actueel/nieuws/2024/02/05/persbericht-brief-informateur
Adviesrapport Integrale aanpak cyberweerbaarheid, Cyber Security Raad, 2021, https://cyberveilignederland.nl/upload/userfiles/files/CSR-Adviesrapport-Integrale-aanpak-cyberweerbaarheid-cyberveilig-nederland-2021-LR.pdf.

134 Digitale weerbaarheid van Nederlandse organisaties. Mogelijkheden en uitdagingen voor de meetbaarheid, RAND Europe, WODC, 22 januari 2026, https://www.rijksoverheid.nl/documenten/2026/01/22/tk-bijlage-1-3470-eindrapport.

135 Digitale weerbaarheid van Nederlandse organisaties. Mogelijkheden en uitdagingen voor de meetbaarheid, RAND Europe, WODC, 22 januari 2026, https://www.rijksoverheid.nl/documenten/2026/01/22/tk-bijlage-1-3470-eindrapport.

136 Op basis van informatie van het NCSC.

137 Hunt & Hackett 2026 Cyber Trend Report, Hunt & Hackett, 2026, https://www.huntandhackett.com/2026-cyber-trend-report.

138 Hunt & Hackett 2026 Cyber Trend Report, Hunt & Hackett, 2026, https://www.huntandhackett.com/2026-cyber-trend-report.

139 Op basis van informatie van het NCSC.

140 Cyberweerbaar Nederland 2026 – Inzicht in digitale weerbaarheid, beleid en blinde vlekken door de ogen van IT- en securityprofessionals, KPN (uitgevoerd door Security Innovation Stories), 20 januari 2026, https://www.kpn.com/zakelijk/thedigitaldutch/blog/cyberweerbaar-nederland
Cyberaanvallen grootste bedreiging voor bedrijfscontinuïteit in Benelux, ICTMagazine, 22 juni 2026, https://www.ictmagazine.nl/nieuws/cyberaanvallen-grootste-bedreiging-voor-bedrijfscontinuiteit-in-benelux/.

141 Cyberweerbaar Nederland 2026 – Inzicht in digitale weerbaarheid, beleid en blinde vlekken door de ogen van IT- en securityprofessionals, KPN (uitgevoerd door Security Innovation Stories), 20 januari 2026, https://www.kpn.com/zakelijk/thedigitaldutch/blog/cyberweerbaar-nederland.

142 Hunt & Hackett 2026 Cyber Trend Report, Hunt & Hackett, 2026, https://www.huntandhackett.com/2026-cyber-trend-report.

143 Cyberweerbaar Nederland 2026 – Inzicht in digitale weerbaarheid, beleid en blinde vlekken door de ogen van IT- en securityprofessionals, KPN (uitgevoerd door Security Innovation Stories), 20 januari 2026, https://www.kpn.com/zakelijk/thedigitaldutch/blog/cyberweerbaar-nederland.

144 Cyberweerbaar Nederland 2026 – Inzicht in digitale weerbaarheid, beleid en blinde vlekken door de ogen van IT- en securityprofessionals, KPN (uitgevoerd door Security Innovation Stories), 20 januari 2026, https://www.kpn.com/zakelijk/thedigitaldutch/blog/cyberweerbaar-nederland.

145 Cyberweerbaar Nederland 2026 – Inzicht in digitale weerbaarheid, beleid en blinde vlekken door de ogen van IT- en securityprofessionals, KPN (uitgevoerd door Security Innovation Stories), 20 januari 2026, https://www.kpn.com/zakelijk/thedigitaldutch/blog/cyberweerbaar-nederland.

146 Cyberweerbaar Nederland 2026 – Inzicht in digitale weerbaarheid, beleid en blinde vlekken door de ogen van IT- en securityprofessionals, KPN (uitgevoerd door Security Innovation Stories), 20 januari 2026, https://www.kpn.com/zakelijk/thedigitaldutch/blog/cyberweerbaar-nederland.

147 'Bedrijfscontinuïteitsbeheer is geen ICT-feestje', VNG, iBestuur, 17 augustus 2022, https://ibestuur.nl/digitale-weerbaarheid/vng/bedrijfscontinuiteitsbeheer-is-geen-ict-feestje
Business Continuity Management (BCM), Informatiebeveiligingsdienst (IBD) van de VNG, https://www.informatiebeveiligingsdienst.nl/business-continuity-management-bcm/.

148 Autoriteit Persoonsgegevens en Raad voor de rechtspraak gehackt via Ivanti-lek, Security.nl, 6 februari 2026, https://www.security.nl/posting/923597/Autoriteit+Persoonsgegevens+en+Raad+voor+de+rechtspraak+gehackt+via+Ivanti-lek
Casus: kwetsbaarheden Ivanti EPMM systemen, NCSC, 27 februari 2026, https://www.ncsc.nl/alerts/casus-kwetsbaarheden-ivanti-epmm-systemen
Kamerbrief Ontwikkelingen over kwetsbaarheid in Ivanti Endpoint Manager Mobile (EPMM), Ministerie van Binnenlandse Zaken en Koninkrijksrelaties / Ministerie van Justitie en Veiligheid, 27 februari 2026, https://www.rijksoverheid.nl/documenten/2026/02/27/kamerbrief-ontwikkelingen-over-kwetsbaarheid-in-ivanti-endpoint-manager-mobile-epmm.

149 Politie en OM dringen aan op forse investeringen in 'verouderde, kwetsbare' ict, Volkskrant, 13 januari 2026, Politie en OM dringen aan op forse investeringen in 'verouderde, kwetsbare' ict: 'Het kan niet langer zo' | de Volkskrant.

150 Van kwetsbaar naar weerbaar. Geleerde lessen uit dreigende acute en langdurige uitval van uitbestede ICT-dienstverlening bij overheidsorganisaties, ABDTOPConsult / Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 25 februari 2025, https://www.algemenebestuursdienst.nl/documenten/2025/02/25/van-kwetsbaar-naar-weerbaar.

151 Cybersecuritybeeld Nederland 2025 - Riskante mix in een onvoorspelbare wereld, NCTV, 26 november 2025, https://www.nctv.nl/site/binaries/site-content/collections/documents/2025/11/26/cybersecuritybeeld-nederland-2025/cybersecuritybeeld-nederland-2025.pdf.

152 Van kwetsbaar naar weerbaar. Geleerde lessen uit dreigende acute en langdurige uitval van uitbestede ICT-dienstverlening bij overheidsorganisaties, ABDTOPConsult / Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 25 februari 2025, https://www.algemenebestuursdienst.nl/documenten/2025/02/25/van-kwetsbaar-naar-weerbaar.

153 Dreigingslandschap Vitale Infrastructuur, NCTV, 24 juli 2025, https://www.nctv.nl/documenten/2025/07/23/dreigingslandschap-vitale-infrastructuur.

154 Dreigingslandschap Vitale Infrastructuur, NCTV, 24 juli 2025, https://www.nctv.nl/documenten/2025/07/23/dreigingslandschap-vitale-infrastructuur.

155 Resultaten verantwoordingsonderzoek 2025 ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Gemeentefonds en Provinciefonds, Algemene Rekenkamer, 20 mei 2026, https://www.rekenkamer.nl/documenten/2026/05/20/vo-2025-bzk.

156 Cyberbeveiligingsincident ministerie van Financiën, Ministerie van Financiën, 30 maart 2026, https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2026Z06573&did=2026D14827
Openbaar Ministerie gaat geleidelijk weer online, NOS Nieuws, 4 augustus 2025, https://nos.nl/artikel/2577569
Ministerie van Financiën weet nog niet wanneer gehackte systemen weer online zijn, Security.nl, 30 maart 2026, https://www.security.nl/posting/930461/ministerie+van+Financi%C3%ABn+weet+nog+niet+wanneer+gehackte+systemen+weer+online+zijn.

157 De waarde van loginformatie, NCSC, https://www.ncsc.nl/incidenten-en-herstellen/de-waarde-van-loginformatie.

158 The Unspoken Guardians of the Internet – Why Non-profit Cybersecurity Matters for Public Safety and Global Resilience, Hans Horan, Ron Stoop, and Jan Feldhusen (HCSS), 2 juni 2026, https://hcss.nl/wp-content/uploads/2026/06/The-Unspoken-Guardians-of-the-Internet-HCSS-2026-V2.pdf
Cyberweerbaarheidskloof – Aanbevelingen voor een cyberweerbaar mkb en het verkleinen van de cyberweerbaarheidskloof, Deloitte (in opdracht van Cyber Security Raad), 26 april 2024, https://prod1-plate-attachments.s3.amazonaws.com/attachments/fecd9a9ff3/deloitte-nl-risk-cyberweerbaarheid-mkb.pdf.

159 CSR Advies 'Verkleinen van de Cyberweerbaarheidskloof', Cyber Security Raad, 4 juni 2024, https://www.cybersecurityraad.nl/documenten/adviezen/2024/06/04/csr-advies-verkleinen-van-de-cyberweerbaarheidskloof.

160 Mkb niet klaar voor nieuwe digitale risico's, ABN AMRO, 23 juni 2026, https://www.abnamro.nl/nl/zakelijk/insights/sectoren-en-trends/alle-sectoren/mkb-niet-klaar-voor-nieuwe-digitale-risicos.html
Cybersecuritymonitor 2025, Centraal Bureau voor de Statistiek (CBS), 28 mei 2026, https://www.cbs.nl/nl-nl/publicatie/2026/22/cybersecuritymonitor-2025.

161 Cybersecuritymonitor 2025, Centraal Bureau voor de Statistiek (CBS), 28 mei 2026, https://www.cbs.nl/nl-nl/publicatie/2026/22/cybersecuritymonitor-2025.

162 Cybersecuritymonitor 2025, Centraal Bureau voor de Statistiek (CBS), 28 mei 2026, https://www.cbs.nl/nl-nl/publicatie/2026/22/cybersecuritymonitor-2025.

163 Mkb niet klaar voor nieuwe digitale risico's, ABN AMRO, 23 juni 2026, https://www.abnamro.nl/nl/zakelijk/insights/sectoren-en-trends/alle-sectoren/mkb-niet-klaar-voor-nieuwe-digitale-risicos.html.

164 Global Cybersecurity Outlook 2025, World Economic Forum (in collaboration with Accenture), 13 januari 2025, https://www.weforum.org/publications/global-cybersecurity-outlook-2025/.

165 Cyberattacks in supply chains: A multi-case study, Zhang X, Ba X, Li B, PLoS One, 22 mei 2026, https://doi.org/10.1371/journal.pone.0350010.

166 Cybersecuritybeeld Nederland 2024, NCTV, 28 oktober 2024, https://www.nctv.nl/documenten/2024/10/28/cybersecuritybeeld-nederland-2024.

167 Ook gegevens van personeel Ceva Logistics gestolen door hackers, BNR Nieuwsradio, 19 augustus 2026, https://www.bnr.nl/nieuws/tech-innovatie/10608544/ook-gegevens-van-personeel-ceva-logistics-gestolen-door-hackers
Bol en Bijenkorf bezorgen weer na cyberaanval bij logistiek bedrijf in Waalwijk,NOSNieuws,2september2026,https://nos.nl/artikel/2629384-bol-en-bijenkorf-bezorgen-weer-na-cyberaanval-bij-logistiek-bedrijf-in-waalwijk.

168 https://cwbrainport.nl/.

169 Frontier AI's Impact on the Cybersecurity Landscape, Potter, Y., Guo, W., Wang, Z., Shi, T., Zhang, A., Kelley, P. G., Thomas, K., & Song, D., 27 november 2025, https://arxiv.org/pdf/2504.05408.

170 Empowering Defenders: AI for Cybersecurity, World Economic Forum (in collaboration with KPMG), mei 2026, https://reports.weforum.org/docs/WEF_Empowering_Defenders_AI_for_Cybersecurity_2026.pdf.

171 CSR Signaalbrief AI (AI als wapen bedreigt digitale veiligheid), Cyber Security Raad, 25 maart 2026, https://www.cybersecurityraad.nl/documenten/2026/03/25/csr-signaalbrief-ai.

172 Bescherm je nu tegen de dreiging van quantumcomputers, AIVD, 27 maart 2026, https://www.aivd.nl/site/binaries/site-content/collections/documents/2026/03/27/bescherm-je-nu-tegen-de-dreiging-van-quantumcomputer-2026/bescherm-je-nu-tegen-de-dreiging-van-quantumcomputers-2026.pdf
Het PQC-migratie handboek: Richtlijnen voor het migreren naar post-quantumcryptografie, AIVD, CWI, TNO, december 2024, https://www.aivd.nl/documenten/publicaties/2024/12/3/het-pqc-migratie-handboek
Bereid je voor op de dreiging van quantumcomputers, AIVD, 23 september 2021, https://www.aivd.nl/documenten/publicaties/2021/09/23/bereid-je-voor-op-de-dreiging-van-quantumcomputers.

173 Focus op quantum bij de rijksoverheid, Algemene Rekenkamer, 4 februari 2026, https://www.rekenkamer.nl/documenten/2026/02/04/focus-op-quantum-bij-de-rijksoverheid.

174 Quantumveiligheid in onderwijs en onderzoek: bewustzijn is er, actie nodig, SURF, 14 april 2026, https://www.surf.nl/nieuws/quantumveiligheid-in-onderwijs-en-onderzoek-bewustzijn-is-er-actie-nodig.

175 Focus op quantum bij de rijksoverheid, Algemene Rekenkamer, 4 februari 2026, https://www.rekenkamer.nl/site/binaries/site-content/collections/documents/2026/02/04/focus-op-quantum-bij-de-rijksoverheid/rapport-focus-op-quantum-bij-de-rijksoverheid.pdf.

176 Quantum-technologie in perspectief: risico's, kansen en implicaties voor het beleid, Ministerie van Financiën, 27 mei 2026, https://www.rijksoverheid.nl/ministeries/ministerie-van-financien.

177 Focus op quantum bij de rijksoverheid, Algemene Rekenkamer, 4 februari 2026, https://www.rekenkamer.nl/site/binaries/site-content/collections/documents/2026/02/04/focus-op-quantum-bij-de-rijksoverheid/rapport-focus-op-quantum-bij-de-rijksoverheid.pdf.

178 Quantum-technologie in perspectief: risico's, kansen en implicaties voor het beleid, Ministerie van Financiën, 27 mei 2026, https://www.rijksoverheid.nl/ministeries/ministerie-van-financien.

179 Artificial intelligence for quantum computing, Alexeev, Y., Farag, M. H., Patti, T. L., et al., Nature Communications, vol. 16, artikel 10829, 2 december 2025, https://www.nature.com/articles/s41467-025-65836-3
We're Using AI to Discover New Quantum Algorithms, Quantinuum, 16 maart 2026, https://www.quantinuum.com/blog/were-using-ai-to-discover-new-quantum-algorithms.

180 Bescherm je nu tegen de dreiging van quantumcomputers, AIVD, 27 maart 2026, https://www.aivd.nl/site/binaries/site-content/collections/documents/2026/03/27/bescherm-je-nu-tegen-de-dreiging-van-quantumcomputer-2026/bescherm-je-nu-tegen-de-dreiging-van-quantumcomputers-2026.pdf
Google warns quantum computers could hack encrypted systems by 2029, Google Quantum AI (Heather Adkins & Sophie Schmieg), 25 maart 2026, gerapporteerd door Euronews en andere uitgebreid op 26-27 maart 2026, https://euronews.com/next/2026/03/27/a-new-era-of-quantum-computing-may-pose-threats-closer-than-we-think-google-warns.

181 Bescherm je nu tegen de dreiging van quantumcomputers, AIVD, 27 maart 2026, https://www.aivd.nl/site/binaries/site-content/collections/documents/2026/03/27/bescherm-je-nu-tegen-de-dreiging-van-quantumcomputer-2026/bescherm-je-nu-tegen-de-dreiging-van-quantumcomputers-2026.pdf
Cybersecuritybeeld Nederland 2024, NCTV, 28 oktober 2024, https://www.nctv.nl/documenten/2024/10/28/cybersecuritybeeld-nederland-2024
Het PQC-migratie handboek: Richtlijnen voor het migreren naar post-quantumcryptografie, AIVD, CWI & TNO, december 2024, https://www.aivd.nl/documenten/publicaties/2024/12/3/het-pqc-migratie-handboek.

182 Cybersecuritybeeld Nederland 2024, NCTV, 28 oktober 2024, https://www.nctv.nl/documenten/2024/10/28/cybersecuritybeeld-nederland-2024.

183 Focus op quantum bij de rijksoverheid, Algemene Rekenkamer, 4 februari 2026, https://www.rekenkamer.nl/site/binaries/site-content/collections/documents/2026/02/04/focus-op-quantum-bij-de-rijksoverheid/rapport-focus-op-quantum-bij-de-rijksoverheid.pdf.

184 Quantum-technologie in perspectief: risico's, kansen en implicaties voor het beleid, Ministerie van Financiën, 27 mei 2026, https://www.rijksoverheid.nl/ministeries/ministerie-van-financien.

185 Het PQC-migratie handboek: Richtlijnen voor het migreren naar post-quantumcryptografie, AIVD, CWI & TNO, december 2024, https://www.aivd.nl/documenten/publicaties/2024/12/3/het-pqc-migratie-handboek.

186 Microsoft advances quantum-safe security as the risk timeline shifts, Microsoft Security Blog (Mark Russinovich, Chief Technology Officer Microsoft Azure), 30 juni 2026, https://www.microsoft.com/en-us/security/blog/2026/06/30/microsoft-advances-quantum-safe-security-as-the-risk-timeline-shifts/
We're setting a timeline for post-quantum cryptography migration to 2029, Heather Adkins & Sophie Schmieg (Google Security Engineering), 25 maart 2026, https://blog.google/innovation-and-ai/technology/safety-security/cryptography-migration-timeline/
Cloudflare targets 2029 for full post-quantum security, Cloudflare Blog, 7 april 2026, https://blog.cloudflare.com/post-quantum-roadmap.

187 A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, EU Working Group on Post-Quantum Cryptography (supported by European Commission), 23 juni 2025, https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography.

188 Cybersecuritybeeld Nederland 2025 – Riskante mix in een onvoorspelbare wereld, NCTV, 26 november 2025, https://www.nctv.nl/site/binaries/site-content/collections/documents/2025/11/26/cybersecuritybeeld-nederland-2025/cybersecuritybeeld-nederland-2025.pdf.

189 DNB: 'Europees betalingsverkeer is kwetsbaar', Financieele Dagblad (FD.nl), 8 maart 2026, https://fd.nl/bedrijfsleven/1588449/dnb-europees-betalingsverkeer-is-kwetsbaar.

190 Belastingdienst mag door met nieuw btw-systeem van Amerikaans bedrijf, Financieele Dagblad (FD.nl), 19 maart 2026, https://fd.nl/politiek/1590120/belastingdienst-mag-door-met-nieuw-btw-systeem-van-amerikaans-bedrijf.

191 Kamerbrief Digitale autonomie bij de Belastingdienst, Ministerie van Financiën (staatssecretaris Eelco Eerenberg), 11 juni 2026, https://open.overheid.nl/details/cd598607-becc-4b66-84ac-e5f3eaa2f8a5.

192 Kamerbrief Bestuurlijke reactie op AcICT-advies over het programma Modernisering kantoorautomatisering uitrol M365 binnen de Belastingdienst, Ministerie van Financiën, 9 juli 2026, https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2026Z16042&did=2026D36243.

193 Kamerbrief besluit investeringstoetsing Solvinity, Ministerie van Economische Zaken en Klimaat, 26 mei 2026, https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2026Z10857&did=2026D24647.

194 'VS eist bij techreuzen communicatie met Europese autoriteiten op over 'censuur'', Tweakers, 17 maart 2026.
https://judiciary.house.gov/media/press-releases/chairman-jordan-probes-eu-bureaucrats-hiding-efforts-censor-american-speech.

195 Fable and Mythos Model Access Restored, Anthropic, 1 juli 2026, https://www.anthropic.com/news/fable-mythos-access.

196 Early users of Anthropic's Mythos still have access after US order, Bloomberg News reports, Reuters, 18 juni 2026, https://www.reuters.com/technology/early-users-anthropic-s-mythos-still-have-access-after-us-order-bloomberg-news-reports-2026-06-18/.

197 Geavanceerde AI van Anthropic weer beschikbaar, regering VS heft blokkade op, NOS Nieuws, 1 juli 2026, https://nos.nl/artikel/2621120-geavanceerde-ai-van-anthropic-weer-beschikbaar-regering-vs-heft-blokkade-op.

198 Internationaal Strafhof dumpt Microsoft en kiest voor Europees alternatief, NRC Handelsblad, 4 november 2025, https://www.nrchandelsblad.nl/.

199 Frankrijk stapt over van Microsoft Teams, Zoom en meer naar eigen alternatief, Tweakers, 27 januari 2026, https://tweakers.net/nieuws/248391/frankrijk-stapt-over-van-microsoft-teams-zoom-en-meer-naar-eigen-alternatief.html.

200 De Nederlandsche Bank kiest voor Duitse cloud van moederbedrijf Lidl, Tweakers, 20 april 2026, https://tweakers.net/nieuws/249055/de-nederlandsche-bank-kiest-voor-duitse-cloud-van-moederbedrijf-lidl.html.

201 Frankrijk, Duitsland, Italië en Nederland starten consortium voor digitale gemeenschapsgoederen, Rijksoverheid.nl, 30 oktober 2025, https://www.rijksoverheid.nl/actueel/nieuws/2025/10/30/frankrijk-duitsland-italie-en-nederland-starten-consortium-voor-digitale-gemeenschapsgoederen
Vier landen slaan handen ineen voor alternatief op Amerikaanse techreuzen,Trouw,oktober2025,https://www.trouw.nl/buitenland/vier-landen-slaan-handen-ineen-voor-alternatief-op-amerikaanse-techreuzen.

202 Nederlandse universiteiten gaan via commissie samenwerken aan digitale autonomie, Tweakers, mei 2026, https://tweakers.net/nieuws/247516/nederlandse-universiteiten-gaan-via-commissie-samenwerken-aan-digitale-autonomie.html.

203 European Parliament ditches Google for French search firm over privacy concerns, Politico, 2 juni 2026, https://www.politico.eu/article/european-parliament-ditches-google-for-french-search-firm/.

204 European Software and Cyber Dependencies, European Parliament, Policy Department for Transformation, Innovation and Health, 16 december 2025, https://www.europarl.europa.eu/thinktank/en/document/ECTI_STU(2025)778576.

205 NLdigital waarschuwt voor schijnveiligheid bij cloudkeuzes, Dutch IT Channel, 20 januari 2026, https://www.dutchitchannel.nl/news/722916/nldigital-waarschuwt-voor-schijnveiligheid-bij-cloudkeuzes.

206 Franse overheid meldt veiligheidsincident met zelfontwikkelde chatapp, Security.nl, 9 juni 2026, https://www.security.nl/posting/939903/Franse+overheid+meldt+veiligheidsincident+met+zelfontwikkelde+chatapp.

207 French Government Messaging Platform Breached by Mysterious 'Misere' Hacker, Kevin Townsend, SecurityWeek, 15 juni 2026, https://www.securityweek.com/french-government-messaging-platform-breached-by-mysterious-misere-hacker/.

208 From Common Worries to Digital Commons: How Europe Can Stop Renting Clouds and Build Its Own, Alexandre Ferreira Gomes, Maaike Okano-Heijmans & Jelle van den Wijngaard, Clingendael Institute, februari 2026, https://www.clingendael.org/publication/common-worries-digital-commons-how-europe-can-stop-renting-clouds-and-build-its-own.

209 VBC waarschuwt voor groeiende cyberdreiging Curaçao, NU.cw, 14 september 2025, https://nu.cw/2025/09/14/vbc-waarschuwt-voor-groeiende-cyberdreiging-curacao/.

210 Cyberweerbaarheid: integraal onderdeel van Aruba's nationale veiligheid, Digital Government / Overheidsbrede Cyberoefening, 19 december 2025, https://www.nldigitalgovernment.nl/cyberweerbaarheid-integraal-onderdeel-van-arubas-nationale-veiligheid/.

211 Caribbean Cyber Resilience Programme / Caribisch Cyberprogramma, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties & ICTU, https://www.weerbaredigitaleoverheid-caribisch.nl/.

212 Bouwplan Cyberweerbaarheidsnetwerk, NCSC (Nationaal Cyber Security Centrum), 17 december 2025, https://www.ncsc.nl/samenwerken/bouwplan-cyberweerbaarheidsnetwerk.

213 Jaarbericht 2025: Toekomstgericht toezicht in een wereld onder spanning, Rijksinspectie Digitale Infrastructuur (RDI), 8 juni 2026, https://www.rdi.nl/documenten/2026/05/04/jaarbericht-2025.

214 Cybersecurity in 2026: ai-versnelling, geopolitieke druk en groeiende digitale ongelijkheid, Computable, 6 februari 2026, https://www.computable.be/2026/02/06/cybersecurity-in-2026-ai%E2%80%91versnelling-geopolitieke-druk-en-groeiende-digitale-ongelijkheid/.

215 CSR waarschuwt: kans op digitale ontwrichting is reëel, Cyber Security Raad, 15 januari 2026, https://www.cybersecurityraad.nl/actueel/nieuws/2026/01/15/csr-waarschuwt-kans-op-digitale-ontwrichting-is-reeel
Tussen vrede en oorlog. De oorlog in Oekraïne en de Russische dreiging in Europa, AIVD & MIVD, 19 februari 2026, https://www.aivd.nl/documenten/2026/02/19/tussen-vrede-en-oorlog.-de-oorlog-in-oekraine-en-de-russische-dreiging-in-europa
State of Cybersecurity Trends Report 2026 – Bridging the Divide, Ivanti, 12 februari 2026, https://www.ivanti.com/resources/research-reports/state-of-cybersecurity-report
Global Cybersecurity Outlook 2025, World Economic Forum / Accenture, 13 januari 2025, https://www.weforum.org/publications/global-cybersecurity-outlook-2025/.

216 Cyber Monitoring Centre Statement on the Jaguar Land Rover Cyber Incident – October 2025, Cyber Monitoring Centre, 22 oktober 2025, https://cybermonitoringcentre.com/2025/10/22/cyber-monitoring-centre-statement-on-the-jaguar-land-rovercyber-incident-october-2025/.

217 JLR hack is costliest cyber attack in UK history, say analysts, BBC, 22 oktober 2025, https://www.bbc.com/news/articles/cy9pdld4y81o.

218 Cyber Monitoring Centre Statement on the Jaguar Land Rover Cyber Incident – October 2025, Cyber Monitoring Centre, 22 oktober 2025, https://cybermonitoringcentre.com/2025/10/22/cyber-monitoring-centre-statement-on-the-jaguar-land-rovercyber-incident-october-2025/.

219 Global Cybersecurity Outlook 2025, World Economic Forum / Accenture, 13 januari 2025, https://www.weforum.org/publications/global-cybersecurity-outlook-2025/.

220 Nederlandse providers doelwit van Salt Typhoon, AIVD en MIVD, 28 augustus 2025, https://www.aivd.nl/actueel/nieuws/2025/08/28/nederlandse-providers-doelwit-van-salt-typhoon.

221 Iran MOIS Phishes 50+ Embassies, Ministries, Int'l Orgs, Dark Reading, 4 september 2025, https://www.darkreading.com/cyberattacks-data-breaches/iran-mois-50-embassies-ministries-intl-orgs.

222 Rusland voert cybercampagne uit tegen Signal- en Whatsapp-accounts, AIVD en MIVD, 9 maart 2026, https://www.aivd.nl/actueel/nieuws/2026/03/09/rusland-voert-cybercampagne-uit-tegen-signal--en-whatsapp-accounts
Russische hackers richten zich op Signal-backups via nieuwe phishing-methode, AIVD en MIVD, 30 juni 2026, https://www.aivd.nl/actueel/nieuws/2026/06/30/russische-hackers-richten-zich-op-signal-backups-via-nieuwe-phishing-methode.

223 Energy Sector Incident Report – 29 December, CERT Polska, 30 januari 2026, https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/.

224 Dreigingslandschap Vitale Infrastructuur, NCTV, 24 juli 2025, https://www.nctv.nl/documenten/2025/07/23/dreigingslandschap-vitale-infrastructuur
Openbaar Jaarverslag 2025, AIVD, 23 april 2026, https://www.aivd.nl/documenten/2026/04/23/jaarverslag-2025
Openbaar Jaarverslag 2025 Militaire Inlichtingen- en Veiligheidsdienst, MIVD, 21 april 2026, https://www.defensie.nl/documenten/2026/04/21/openbaar-jaarverslag-2025-militaire-inlichtingen--en-veiligheidsdienst.

225 Kamerbrief: Ontwikkelingen over kwetsbaarheid in Ivanti Endpoint Manager Mobile (EPMM), Ministerie van Binnenlandse Zaken en Koninkrijksrelaties / Ministerie van Justitie en Veiligheid, 27 februari 2026, https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2026Z03958&did=2026D09045
Antwoord op vragen van het lid Faber over hackers hadden vijf maanden toegang tot gegevens DJI-medewerkers, Staatssecretaris van Justitie en Veiligheid, 13 april 2026, https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2026Z04230&did=2026D17353.

226 Cyberbeveiligingsincident ministerie van Financiën, Ministerie van Financiën, 30 maart 2026, https://www.rijksoverheid.nl/documenten/kamerstukken/2026/03/30/cyberbeveiligingsincident-ministerie-van-financien
Ministerie van Financiën weet nog niet wanneer gehackte systemen weer online zijn, Security.nl, 30 maart 2026, https://www.security.nl/posting/930461/Ministerie+van+Financi%C3%ABn+weet+nog+niet+wanneer+gehackte+systemen+weer+online+zijn.

227 'Datalek gemeente Epe', Gemeente Epe, 14-03-2026, https://www.epe.nl/datalek-gemeente-epe.

228 Ransomware-incident ChipSoft – nieuwe informatie (UPDATE vrijdag 17 april), Z-CERT, 17 april 2026, https://z-cert.nl/actueel/nieuws/ransomware-incident-chipsoft-nieuwe-informatie-17-april
ChipSoft bevestigt diefstal patiëntgegevens na ransomware-aanval, Techzine, 17 april 2026, https://www.techzine.nl/nieuws/security/577182/chipsoft-bevestigt-diefstal-patientgegevens-na-ransomware-aanval/.

229 Openbaar Jaarverslag 2025, MIVD, 21 april 2026, https://www.defensie.nl/documenten/2026/04/21/openbaar-jaarverslag-2025-militaire-inlichtingen--en-veiligheidsdienst.

230 Openbaar Jaarverslag 2025, AIVD, 24 april 2026, https://www.aivd.nl/documenten/2026/04/23/jaarverslag-2025; Openbaar Jaarverslag 2025, MIVD, 21 april 2026, https://www.defensie.nl/documenten/2026/04/21/openbaar-jaarverslag-2025-militaire-inlichtingen--en-veiligheidsdienst.

231 The hidden threat of cyber-attacks – undermining public confidence in government, Shandler, R. and Gomez, M. A., Journal of Information Technology & Politics, 20(4), pp. 359–374, 2023, https://doi.org/10.1080/19331681.2022.2112796
Cyber Conflicts and the Erosion of Institutional Trust: the Impacts on Citizens, Italian Institute for International Political Studies (ISPI), 5 februari 2026, https://www.ispionline.it/en/publication/cyber-conflicts-and-the-erosion-of-institutional-trust-the-impacts-on-citizens-229266.

232 Kans op grote cyberaanval volgens mensen groot: 2 op de 3 denken dat overheid en bedrijven onvoldoende zijn voorbereid, EenVandaag, 8 augustus 2025, https://eenvandaag.avrotros.nl/opiniepanel/uitslagen/kans-op-grote-cyberaanval-volgens-mensen-groot-2-op-de-3-denken-dat-overheid-en-bedrijven-onvoldoende-zijn-voorbereid-160989.

233 The limits of cyberattacks in eroding political trust: A tripartite survey experiment, Matzkin, S., Shandler, R., and Canetti, D., The British Journal of Politics and International Relations, 2023, https://doi.org/10.1177/13691481231210383.

234 Risico- en Crisisbarometer Najaar 2026, NCTV / Ipsos I&O, 2026.

235 MOB-jaarrapportage 2025, Maatschappelijk Overleg Betalingsverkeer / De Nederlandsche Bank, juni 2026, https://www.tweedekamer.nl/downloads/document?id=2026D33236
Beantwoording SO-vragen informele Telecomraad, Ministerie van Economische Zaken en Klimaat / Directie Europese en Internationale Zaken, 20 april 2026, https://open.overheid.nl/documenten/fa88b7e0-dff4-42d8-99e5-107580361d13/.

236 Verkenning mogelijkheden beschikbaarheid statistieken over data delen, Internet of Things en clouddiensten, Centraal Bureau voor de Statistiek (CBS), 30 april 2025, https://www.cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/verkenning-mogelijkheden-beschikbaarheid-statistieken-over-data-delen-internet-of-things-en-clouddiensten.

237 Beveiligingstips voor Internet of Things (IoT), NCSC, https://www.ncsc.nl/edge-devices/beveiligingstips-voor-internet-of-things-iot.

238 Cybersecurity onderzoek Alert Online 2025, Ipsos I&O, augustus 2025, https://open.overheid.nl/documenten/79b32aa0-faa7-48d2-90f0-58d5c102b91b/file
Cybercrime treft driekwart Nederlanders, maar lang niet iedereen houdt slimme apparaten up-to-date, Rijksoverheid.nl / Ministerie van Economische Zaken en Klimaat, 6 oktober 2025, https://www.rijksoverheid.nl/actueel/nieuws/2025/10/06/cybercrime-treft-driekwart-nederlanders-maar-lang-niet-iedereen-houdt-slimme-apparaten-up-to-date.

239 Chinees bedrijf kon met jou meegluren via camera robotstofzuiger: duizenden beelden gelekt, De Telegraaf, 24 februari 2026, https://www.telegraaf.nl/lifestyle/tech/chinees-bedrijf-kon-met-jou-meegluren-via-camera-robotstofzuiger-duizenden-beelden-gelekt/136587677.html
Programmeur gluurt per ongeluk bij duizenden huizen naar binnen via slecht beveiligde robotstofzuigers, de Volkskrant, 25 februari 2026, https://www.volkskrant.nl/tech/programmeur-gluurt-per-ongeluk-bij-duizenden-huizen-naar-binnen-via-slecht-beveiligde-robotstof-zuigers~b74d5253/.

240 Residential proxies en hun grote impact op de digitale veiligheid in Nederland, NCSC, https://www.ncsc.nl/asset-management/residential-proxies-en-hun-grote-impact-op-de-digitale-veiligheid-in-nederland.

241 NCSC: residential proxies dreiging voor digitale veiligheid van Nederland, Security.nl, 28 mei 2026, https://www.security.nl/posting/938399/NCSC%3A+residential+proxies+dreiging+voor+digitale+veiligheid+van+Nederland.

242 Chinese hackers using everyday devices to target UK firms, warns cybersecurity agency, The Guardian, 23 april 2026
Defending against China-nexus covert networks of compromised devices, National Cyber Security Centre (UK), 23 april 2026, https://www.ncsc.gov.uk/news/defending-against-china-nexus-covert-networks-of-compromised-devices
Residential proxies en hun grote impact op de digitale veiligheid in Nederland, NCSC, https://www.ncsc.nl/asset-management/residential-proxies-en-hun-grote-impact-op-de-digitale-veiligheid-in-nederland.

243 NCSC: residential proxies dreiging voor digitale veiligheid van Nederland, Security.nl, 28 mei 2026, https://www.security.nl/posting/938399/NCSC%3A+residential+proxies+dreiging+voor+digitale+veiligheid+van+Nederland.

244 Chinese hackers using everyday devices to target UK firms, warns cybersecurity agency, The Guardian, 23 april 2026, https://www.theguardian.com/technology/2026/apr/23/china-cyber-hacker-using-everyday-devices-hack-uk-firms.

245 Je slimme verlichting deelt je leven met de hele wereld, Pointer / KRO-NCRV, 3 mei 2019, https://pointer.kro-ncrv.nl/je-slimme-verlichting-deelt-je-leven-met-de-hele-wereld.

246 SuperBox: van droomdeal naar digitale nachtmerrie, gelinkt aan China, BNR Nieuwsradio, 14 juni 2026, https://www.bnr.nl/nieuws/tech-innovatie/10602944/superbox-van-droomdeal-naar-digitale-nachtmerrie-gelinkt-aan-china.

247 Veilige zonnestroom: scenario's en maatregelen voor cyberweerbare zonnestroominstallaties, Secura / Energy Innovation, augustus 2024, https://www.energy-innovation.nl/nl/nieuws/veilige-zonnestroom-scenarios-en-maatregelen-voor-cyberweerbare-zonnestroominstallaties/.

248 Thuisbatterijen en brandveiligheid, Nederlands Instituut Publieke Veiligheid (NIPV) / Ministerie van Volkshuisvesting en Ruimtelijke Ordening, 10 december 2024, https://nipv.nl/wp-content/uploads/2025/02/20241210-NIPV-Thuisbatterijen-en-brandveiligheid.pdf.

249 Veilige zonnestroom: scenario's en maatregelen voor cyberweerbare zonnestroominstallaties, Secura / Topsector Energie / Rijksdienst voor Ondernemend Nederland (RVO), augustus 2024, https://www.energy-innovation.nl/nl/nieuws/veilige-zonnestroom-scenarios-en-maatregelen-voor-cyberweerbare-zonnestroominstallaties/.

250 Strava bracht kazerneterreinen onbedoeld in kaart, nu vreest Defensie een veel groter lek: jouw auto, Algemeen Dagblad, 13 juli 2026, https://www.ad.nl/
Malicious TV boxes: how a cheap "SuperBox" turns your home into a proxy node for cybercriminals, Tom Fosters, Kaspersky, 20 mei 2026, https://www.kaspersky.com/blog/android-tv-botnet/55799/
Superbox: van droomdeal naar digitale nachtmerrie – gelinkt aan China, BNR, https://www.bnr.nl/nieuws/tech-innovatie/10602944/superbox-van-droomdeal-naar-digitale-nachtmerrie-gelinkt-aan-china
Met razendsnelle groei batterijen neemt ook risico op cyberaanval toe, NOS Nieuwsuur, 2 januari 2025, https://nos.nl/nieuwsuur/artikel/2550358-met-razendsnelle-groei-batterijen-neemt-ook-risico-op-cyberaanval-toe
Kennisdocument thuisbatterijen, CE Delft, april 2023, https://ce.nl/wp-content/uploads/2023/11/CE_Delft_220408_Kennisdocument-thuisbatterijen_Def-1.pdf
Je slimme verlichting deelt je leven met de hele wereld, Pointer / KRO-NCRV, https://pointer.kro-ncrv.nl/je-slimme-verlichting-deelt-je-leven-met-de-hele-wereld
Impact of Cybersecurity Risks on the Dutch National Charge Point Infrastructure, Berenschot, https://www.berenschot.nl/media/2msfvemt/impact-of-cybersecurity-risks-on-the-dutch-national-charge-point-infrastructurev1.pdf
Basisbeveiligingsmaatregelen slimme apparaten, NCSC, https://www.ncsc.nl/edge-devices/basisbeveiligingsmaatregelen-slimme-apparaten
Beveiligingstips voor Internet of Things (IoT), NCSC, https://www.ncsc.nl/edge-devices/beveiligingstips-voor-internet-of-things-iot
Veilige zonnestroom: scenario's en maatregelen voor cyberweerbare zonnestroominstallaties, Energy Innovation, https://www.energy-innovation.nl/nl/nieuws/veilige-zonnestroom-scenarios-en-maatregelen-voor-cyberweerbare-zonnestroominstallaties/.

251 How Far Behind the Frontier are Leading Open Weight Models on Cyber?, The AI Security Institute (AISI), 17 juli 2026, https://www.aisi.gov.uk/blog/how-far-behind-the-frontier-are-leading-open-weight-models-on-cyber.

252 China-based hacker employs DeepSeek in autonomous threat campaign, David Jones / Cybersecurity Dive, 3 augustus 2026, https://www.cybersecuritydive.com/news/china-based-hacker-deepseek-autonomous/826784/.

253 Enge verhalen over 'mensachtige' AI die uit de testomgeving 'ontsnapt, passen in de pr-strategie van de makers. Is er ook reden om bang te zijn?', NRC Handelsblad, 24 juli 2026, https://www.nrc.nl/nieuws/2026/07/24/enge-verhalen-over-mensachtige-ai-die-uit-de-testomgeving-ontsnapt-passen-in-de-pr-strategie-van-de-makers-is-er-ook-reden-om-bang-te-zijn-a4933121.

254 Cyberweerbaar Nederland 2026 – Inzicht in digitale weerbaarheid, beleid en blinde vlekken door de ogen van IT- en securityprofessionals, KPN / Security Innovation Stories, januari 2026, https://www.kpn.com/zakelijk/thedigitaldutch/blog/cyberweerbaar-nederland
Cyberaanvallen grootste bedreiging voor bedrijfscontinuïteit in Benelux, ICTMagazine.nl / HarfangLab (State of Cybersecurity Report 2026), 22 juni 2026, https://www.ictmagazine.nl/nieuws/cyberaanvallen-grootste-bedreiging-voor-bedrijfscontinuiteit-in-benelux/.

255 Global Cybersecurity Outlook 2025, World Economic Forum / Accenture, 13 januari 2025, https://www.weforum.org/publications/global-cybersecurity-outlook-2025/.

256 Minister: Citrix-systemen van enkele rijksorganisaties recentelijk gehackt, Security.nl, 22 september 2025, https://www.security.nl/posting/905655/Minister%3A+Citrix-systemen+van+enkele+rijksorganisaties+recentelijk+gehackt.

257 NCSC: Citrix-systemen vitale Nederlandse organisaties gehackt, security.nl, 11 augustus 2025, https://www.security.nl/posting/900230/NCSC%3A+Citrix-systemen+vitale+Nederlandse+organisaties+gehackt.

258 ICT-organisatie van justitie niet één, maar twee keer gehackt, Argos, 14 maart 2026, https://argos.vpro.nl/artikelen/ict-organisatie-van-justitie-niet-een-maar-twee-keer-gehackt.

259 Kamerbrief over impact strafrechtketen informatiebeveiliging OM, Ministerie van Justitie en Veiligheid, 12 augustus 2025, https://www.rijksoverheid.nl/documenten/2025/08/12/tk-impact-strafrechtketen-informatiebeveiliging-om
OM gaat stapsgewijs online, Openbaar Ministerie, 4 augustus 2025, https://www.om.nl/actueel/nieuws/2025/08/04/om-gaat-stapsgewijs-online.

260 Nederlandse providers doelwit van Salt Typhoon, Ministerie van Defensie, 28 augustus 2025, https://www.defensie.nl/actueel/nieuws/2025/08/28/nederlandse-providers-doelwit-van-salt-typhoon.

261 Iran MOIS Phishes 50+ Embassies, Ministries, Int'l Orgs, DarkReading, 04 september 2025, https://www.darkreading.com/cyberattacks-data-breaches/iran-mois-50-embassies-ministries-intl-orgs.

262 Succesvolle ddos-aanvallen op overheid, advies aan deel ambtenaren: 'Werk niet thuis', NOS, 15 september 2025, https://nos.nl/artikel/2582557-succesvolle-ddos-aanvallen-op-overheid-advies-aan-deel-ambtenaren-werk-niet-thuis.

263 Twee tieners opgepakt voor spionageklus voor pro-Russische hacker, NOS, 26 september 2025, https://nos.nl/artikel/2584076-twee-tieners-opgepakt-voor-spionageklus-voor-pro-russische-hacker.

264 Hard oordeel over Eindhoven: 'Gemeente onvoldoende voorbereid op werken met AI', ED, 22 december 2025, https://www.ed.nl/eindhoven/hard-oordeel-over-eindhoven-gemeente-onvoldoende-voorbereid-op-ai~a5b3a31e/.

265 Grote internationale storing bij Amazon treft talloze bekende apps en websites, Nu.nl, 20 oktober 2025, https://www.nu.nl/tech/6373010/grote-internationale-storing-bij-amazon-treft-talloze-bekende-apps-en-websites.html.

266 Friese afvalverwerker Omrin heeft nog altijd last van ransomware-aanval, Security.nl, 23 oktober 2025, https://www.security.nl/posting/910198/Friese+afvalverwerker+Omrin+heeft+nog+altijd+last+van+ransomware-aanval.

267 Omrin-hackers komen dreigement na: duizenden bestanden nu op straat, Omrop Fryslân, 28 oktober 2025, https://www.omropfryslan.nl/nl/nieuws/17910948/omrin-hackers-komen-dreigement-na-duizenden-bestanden-nu-op-straat.

268 Windows zero-day actively exploited to spy on European diplomats, BleepingComputer, 31 oktober 2025, https://www.bleepingcomputer.com/news/security/chinese-hackers-exploit-windows-zero-day-to-spy-on-european-diplomats/.

269 Hoe de hack wél de systemen, maar niet de veerkracht van RTV Noord platlegde, RTV Noord, 23december 2025, https://www.rtvnoord.nl/misdaad/RX-1084/hoe-de-hack-wel-de-systemen-maar-niet-de-veerkracht-van-rtv-noord-platlegde.

270 Hackers Martini Ziekenhuis en Arriva beweren niks te hebben gestolen. 'Wilden vooral reclame maken', DVHN, 19 november 2025, https://dvhn.nl/groningen/hackers-martini-ziekenhuis-en-arriva-beweren-niks-te-hebben-gestolen.-wilden-vooral-reclame-maken-47831718.html.

271 Grote Cloudflare-storing werd niet door cyberaanval veroorzaakt maar door bug, Tweakers, 19 november 2025, https://tweakers.net/nieuws/241664/grote-cloudflare-storing-werd-niet-door-cyberaanval-veroorzaakt-maar-door-bug.html.

272 Wereldwijd websites uit de lucht door storing bij Cloudflare, NOS, 18 november 2025, https://nos.nl/artikel/2590966-wereldwijd-websites-uit-de-lucht-door-storing-bij-cloudflare.

273 Some Interrail travellers told to cancel passports as hacked data posted online, The Guardian, 23 april 2026, https://www.theguardian.com/technology/2026/apr/23/some-interrail-travellers-told-to-cancel-passports-as-hacked-data-posted-online.

274 Huisartsenorganisatie Medrie lekt gegevens van ruim tweeduizend patiënten, Security.nl, 29 januari 2026, https://www.security.nl/posting/922518/Huisartsenorganisatie+Medrie+lekt+gegevens+van+ruim+tweeduizend+pati%C3%ABnten.

275 Gestolen data bij Odido zijn 'goud waard voor criminelen', NOS Nieuws, 12 februari 2026, https://nos.nl/artikel/2602162-gestolen-data-bij-odido-zijn-goud-waard-voor-criminelen.

276 Odido-hackers publiceren resterende klantdata, ook miljoenen ID-nummers, NOS, 01 maart 2026, https://nos.nl/artikel/2604461-odido-hackers-publiceren-resterende-klantdata-ook-miljoenen-id-nummers.

277 NCSC: meerdere organisaties via kritiek Ivanti EPMM-lek gehackt, security.nl, 09 februari 2026, https://www.security.nl/posting/923850/NCSC%3A+meerdere+organisaties+via+kritiek+Ivanti+EPMM-lek+gehackt.

278 Autoriteit Persoonsgegevens en Raad voor de rechtspraak gehackt via Ivanti-lek, Security.nl, 06 februari 2026, https://www.security.nl/posting/923597/Autoriteit+Persoonsgegevens+en+Raad+voor+de+rechtspraak+gehackt+via+Ivanti-lek.

279 Ontwikkelingen over kwetsbaarheid in Ivanti Endpoint Manager Mobile (EPMM), Tweede Kamer, 27 februari 2026, https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2026Z03958&did=2026D09045.

280 Ministerie van Financiën weet nog niet wanneer gehackte systemen weer online zijn, Security.nl, 30 maart 2026, https://www.security.nl/posting/930461/Ministerie+van+Financi%C3%ABn+weet+nog+niet+wanneer+gehackte+systemen+weer+online+zijn.

281 Ministerie van Financiën afgelopen maart gehackt via zerodaylek, Security.nl, 18 juni 2026, https://www.security.nl/posting/941057/Ministerie+van+Financi%C3%ABn+afgelopen+maart+gehackt+via+zerodaylek.

282 https://www.politie.nl/nieuws/2026/maart/25/00-politie-doelwit-van-phishing.html.

283 Datalek gemeente Epe, Gemeente Epe, 05 juni 2026, https://www.epe.nl/datalek-gemeente-epe.

284 Persoonsgegevens van vrijwel alle inwoners Epe gestolen bij cyberaanval, NOS, 23 april 2026, https://nos.nl/artikel/2611660-persoonsgegevens-van-vrijwel-alle-inwoners-epe-gestolen-bij-cyberaanval.

285 Datalek gemeente Epe, Gemeente Epe, 14 maart 2026, https://www.epe.nl/datalek-gemeente-epe.

286 ChipSoft bevestigt diefstal patiëntgegevens na ransomware-aanval, Techzine, 17 september 2026, https://www.techzine.nl/nieuws/security/577182/chipsoft-bevestigt-diefstal-patientgegevens-na-ransomware-aanval/.

287 ChipSoft zegt dat alle door hackers gestolen data is vernietigd, Tweakers, 28 april 2026, https://tweakers.net/nieuws/247268/chipsoft-zegt-dat-alle-door-hackers-gestolen-data-is-vernietigd.html.

288 Dieven stelen privédata van studenten en docenten via onderwijssoftware Canvas, Tweakers, 04 mei 2026, https://tweakers.net/nieuws/247446/dieven-stelen-privedata-van-studenten-en-docenten-via-onderwijssoftware-canvas.html.

289 Honderdduizenden studenten in de problemen door Canvas-hack, RTL, 08mei 2026, https://www.rtl.nl/nieuws/tech/artikel/5599239/hack-canvas-shinyhunters-instructure-universiteit-hogeschool-gevolgen.

290 Onderwijsplatform Canvas sluit deal met hackersgroep, 'data is verwijderd', Tweakers, 12 mei 2026, https://tweakers.net/nieuws/247724/onderwijsplatform-canvas-sluit-deal-met-hackersgroep-data-is-verwijderd.html.

291 Ransomwaregroep claimt aanval op Instituut voor de Nederlandse Taal, Security.nl, 15 mei 2026, https://www.security.nl/posting/936752/Ransomwaregroep+claimt+aanval+op+Instituut+voor+de+Nederlandse+Taal.

292 Rusland voert cybercampagne uit tegen Signal- en Whatsapp-accounts, AIVD, 09 maart 2026, https://www.aivd.nl/actueel/nieuws/2026/03/09/rusland-voert-cybercampagne-uit-tegen-signal--en-whatsapp-accounts.

293 Russische hackers richten zich op Signal-backups via nieuwe phishing-methode, AIVD, 30 juni 2026, https://www.aivd.nl/actueel/nieuws/2026/06/30/russische-hackers-richten-zich-op-signal-backups-via-nieuwe-phishing-methode.

294 Zakenreisbureau BCD gehackt, klantgegevens op darkweb, FD, 03 juni 2026, https://fd.nl/tech-en-innovatie/1598783/zakenreisbureau-bcd-gehackt-klantgegevens-op-darkweb.

295 Systemen Rijkswaterstaat komen weer op gang na landelijke storing, NOS, 27juni2026,https://nos.nl/artikel/2620579-systemen-rijkswaterstaat-komen-weer-op-gang-na-landelijke-storing.

296 De beschrijving van deze incidenten is gebaseerd op informatie bekend bij het NCSC.

297 Maasstad Ziekenhuis in Rotterdam ligt plat door grote ict-storing na noodtest, Tweakers, 01 juli 2026, https://tweakers.net/nieuws/249672/maasstad-ziekenhuis-in-rotterdam-ligt-plat-door-grote-ict-storing-na-noodtest.html.

298 Nederland doelwit van Russische spionageoperatie via IP-camera's, AIVD, 10 juli 2026, https://www.aivd.nl/actueel/nieuws/2026/07/10/nederland-doelwit-van-russische-spionageoperatie-via-ip-cameras.

299 10 bedrijven melden zich naast Bol en Bijenkorf om datalek bij partner Ceva, AD.nl, 11 augustus 2026, https://www.ad.nl/economie/10-bedrijven-melden-zich-naast-bol-en-bijenkorf-om-datalek-bij-partner-ceva~a62fe485/.

300 Bol en Bijenkorf bezorgen weer na cyberaanval bij logistiek bedrijf in Waalwijk, NOS Nieuws, 2 september 2026, https://nos.nl/artikel/2629384-bol-en-bijenkorf-bezorgen-weer-na-cyberaanval-bij-logistiek-bedrijf-in-waalwijk.

301 Ook gegevens van personeel Ceva Logistics gestolen door hackers, BNR Nieuwsradio, 19 augustus 2026, https://www.bnr.nl/nieuws/tech-innovatie/10608544/ook-gegevens-van-personeel-ceva-logistics-gestolen-door-hackers.

302 EU cyber agency says airport software held to ransom by criminals, BBC, 22 september 2025, https://www.bbc.com/news/articles/cqjeej85452o.

303 Gegevens passagiers Dublin Airport gestolen bij ransomware-aanval, Security.nl, 27 oktober 2025, https://www.security.nl/posting/910753/Gegevens+passagiers+Dublin+Airport+gestolen+bij+ransomware-aanval.

304 Datalek bij softwareleverancier luchthavens via gestolen ftp-wachtwoord uit 2022, Security.nl, 24 oktober 2025, https://www.security.nl/posting/910426/%27Datalek+bij+softwareleverancier+luchthavens+via+gestolen+ftp-wachtwoord+uit+2022%27.

305 Zichzelf verspreidende malware infecteert vijfhonderd npm-packages, Security.nl, 17 september 2025, https://www.security.nl/posting/905051/Zichzelf+verspreidende+malware+infecteert+vijfhonderd+npm-packages.

306 Jaguar Land Rover production severely hit by cyber-attack, BBC, 02 september 2025, https://www.bbc.com/news/articles/c9wywvllq7wo.

307 JLR hack is costliest cyber attack in UK history, say analysts, BBC, 22 oktober 2025, https://www.bbc.com/news/articles/cy9pdld4y81o.

308 Jaguar Land Rover meldt diefstal van salarisgegevens personeel, Security.nl, 15 december 2025, https://www.security.nl/posting/917323/Jaguar+Land+Rover+meldt+diefstal+van+salarisgegevens+personeel.

309 M&S hackers claim to be behind Jaguar Land Rover cyber attack, BBC, 03 september 2025, https://www.bbc.com/news/articles/c4gqepe5355o.

310 Hack Jaguar Land Rover was aanval met geavanceerde ransomware, Security.nl, 29 juni 2026, https://www.security.nl/posting/942504/%27Hack+Jaguar+Land+Rover+was+aanval+ met+geavanceerde+ransomware%27.

311 Suspected Chinese actors compromise U.S. Telecom firm Ribbon Communications, Securityaffairs, 31 oktober 2025, https://securityaffairs.com/184042/intelligence/suspected-chinese-actors-compromise-u-s-telecom-firm-ribbon-communications.html.

312 Screenshot Everest Group bericht, ransomlook.io, https://www.ransomlook.io/screenshots/everest/Svenska%20Kraftn%C3%A4t%20data.png.

313 Zweedse netbeheerder Svenska Kraftnat meldt inbraak op filesharingsysteem, Security.nl, 28 oktober 2025, https://www.security.nl/posting/910983/Zweedse+netbeheerder+Svenska+Kraftnat+meldt+inbraak+op+filesharingsysteem.

314 Alert - AL25-016 Internet-accessible industrial control systems (ICS) abused by hacktivists, Government of Canada, 29 oktober 2025, https://www.cyber.gc.ca/en/alerts-advisories/al25-016-internet-accessible-industrial-control-systems-ics-abused-hacktivists.

315 Na Russische cyberaanval op Proximus en Scarlet nu ook UZ Gent kort getroffen: geen gevolgen voor gebruikers of patiënten, VRT, 05 november 2025, https://www.vrt.be/vrtnws/nl/2025/11/05/cyberaanval-op-websites-proximus-en-scarlet/.

316 Hundreds of Salesforce customers hit by yet another third-party vendor breach, CyberScoop, 20 november 2025, https://cyberscoop.com/salesforce-gainsight-customers-breach/.

317 Pro-Russian group claims hits on Danish party websites as voters head to polls, The Record, 18 november 2025, https://therecord.media/denmark-election-political-government-websites-ddos-incidents
Pro-Russian group claims hits on Danish party websites as voters head to polls, The Record, 18 november 2025, https://therecord.media/denmark-election-political-government-websites-ddos-incidents.

318 Energy Sector Incident Report – 29 December, CERT Polska 29 december 2025, https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/.

319 Poland says it repelled major cyberattack on power grid, blames Russia, The Record, 14 januari 2026, https://therecord.media/poland-cyberattack-grid-russia.

320 Cyber / Russia: Statement by the High Representative on behalf of the European Union denouncing Russia's malicious cyber ecosystem targeting the EU, its member states and international partners, European Council, 13 juni 2026, https://www.consilium.europa.eu/en/press/press-releases/2026/07/13/cyber-russia-statement-by-the-high-representative-on-behalf-of-the-european-union-denouncing-russia-s-malicious-cyber-ecosystem-targeting-the-eu-its-member-states-and-international-partners/.

321 Follow-Up Report of the December 2025 Energy Sector Incident, CERT PL, 08 augustus 2026, https://cert.pl/en/posts/2026/08/incident-follow-up-report-energy-sector-2025/.

322 European Space Agency confirms breach of "external servers", BleepingComputer, 30 december 2025, https://www.bleepingcomputer.com/news/security/european-space-agency-confirms-breach-of-external-servers/.

323 Claude code abused to steal 150GB in cyberattack on Mexican agencies, securityaffairs, 01 maart 2026, https://securityaffairs.com/188696/ai/claude-code-abused-to-steal-150gb-in-cyberattack-on-mexican-agencies.html.

324 Claude AI Guided Hackers Toward OT Assets During Water Utility Intrusion, Securityweek, 07 mei 2026, https://www.securityweek.com/claude-ai-guided-hackers-toward-ot-assets-during-water-utility-intrusion/.

325 Iranian government hackers using Chaos ransomware as cover, researchers say, The Record, 07 mei 2026, https://therecord.media/iran-government-hackers-use-chaos-ransomware-as-cover.

326 30 procent van zorgverlening kan doorgaan in AZ Monica na cyberaanval, servers kunnen nog niet opstarten, VRT, 13 januari 2026, https://www.vrt.be/vrtnws/nl/2026/01/13/netwerk-az-monica-ziekenhuizen-ligt-plat-niet-dringende-zorg-vo/.

327 Belgische ziekenhuizen vallen wegens ransomware terug op pen en papier, security.nl, 15 januari 2026, https://www.security.nl/posting/920966/Belgische+ziekenhuizen+vallen+wegens+ransomware+terug+op+pen+en+papier.

328 IT-systemen AZ Monica werken opnieuw zoals voor cyberaanval: "Patiënten merken er niets meer van", VRT, 17 februari 2026, https://www.vrt.be/vrtnws/nl/2026/02/17/az-monica-deurne-cyberaanval-opnieuw-digitaal-website-heropstart/.

329 Trivy vulnerability scanner breach pushed infostealer via GitHub Actions, BleepingComputer, 21 maart 2026, https://www.bleepingcomputer.com/news/security/trivy-vulnerability-scanner-breach-pushed-infostealer-via-github-actions/.

330 European Commission cloud breach: a supply-chain compromise, Cert-EU, 02 april 2026, https://cert.europa.eu/blog/european-commission-cloud-breach-trivy-supply-chain.

331 Maintainer Axios-project: account gehackt via social engineering-aanval, Security.nl, 01 april 2026, https://www.security.nl/posting/930725/Maintainer+Axios-project%3A+account+gehackt+via+social+engineering-aanval.

332 OpenAI getroffen door Axios-aanval, vervangt code signing certificaat, Security.nl, 13 april 2026, https://www.security.nl/posting/932438/OpenAI+getroffen+door+Axios-aanval%2C+vervangt+code+signing+certificaat.

333 Medical device giant Stryker confirms cyberattack as employees say devices were wiped , The Record, 11 maart 2026, https://therecord.media/stryker-cyberattack-iran-hackers.

334 Stryker says malware was involved in recent cyberattack as production lines reopen, The Record, 24 maart 2026, https://therecord.media/stryker-cyberattack-malware-iran.

335 Franse overheid bevestigt datadiefstal bij instantie voor uitgifte identiteitsbewijzen, Security.nl, 22 april 2026, https://www.security.nl/posting/933712/Franse+overheid+bevestigt+datadiefstal+bij+instantie+voor+uitgifte+identiteitsbewijzen.

336 Hackers steal patient and billing data from German hospitals via third-party provider, The Record, 22 mei 2026, https://therecord.media/hackers-steal-patient-billing-data-german-hospitals.

337 Council of Europe hacked in ShinyHunters' PeopleSoft heist, The Register, 15 juni 2026, https://www.theregister.com/cyber-crime/2026/06/15/council-of-europe-hacked-in-shinyhunters-peoplesoft-heist/5255757.

338 Council of Europe investigates ShinyHunters data breach claims, BleepingComputer, 15 juni 2026, https://www.bleepingcomputer.com/news/security/council-of-europe-investigates-shinyhunters-data-breach-claims/.

339 Iranian Cyber Group Handala Claims Cal Water Hack, Securityweek, 12 juni 2026,https://www.securityweek.com/iranian-cyber-group-handala-claims-cal-water-hack/.

340 Cal Water Says No OT Systems Breached in Iranian Handala Cyberattack, Securityweek, 25 juni 2026, https://www.securityweek.com/cal-water-finds-no-evidence-of-ot-activity-after-hackers-claimed-they-could-disrupt-water-supply/.

341 Security incident disclosure — July 2026, Hugging Face, 16 juli 2026, https://huggingface.co/blog/security-incident-july-2026.

342 Het Hugging Face-incident en de weg vooruit, OpenAI, 26 augustus 2026, https://openai.com/nl-NL/index/hugging-face-incident-and-the-road-ahead/
Brief independent investigation of agents' behavior, reasoning and collaboration in the OpenAI / Hugging Face hacking incident, METR / Redwood Research, 26 augustus 2026, https://metr.org/hugging-face-incident-report-aug-2026.pdf

Onderzoek: 700 OpenAI-agents hackten Hugging Face, Tweakers, augustus 2026, https://tweakers.net/nieuws/251446/onderzoek-700-openai-agents-hackten-hugging-face.html.

343 OpenAI en Hugging Face werken samen aan beveiligingsincident tijdens modelevaluatie, OpenAI, 21 juli 2026, https://openai.com/index/hugging-face-model-evaluation-security-incident/.

344 Meta becomes latest firm to say its AI hacked another company, BBC, 06 augustus 2026, https://www.bbc.com/news/articles/cx2kgdnyk2po.

345 Investigating three real-world incidents in our cybersecurity evaluations, Anthropic, 30 juli 2026, https://www.anthropic.com/news/investigating-incidents-cybersecurity-evals.

346 China-linked hackers hit Taiwan in unprecedented 'autonomous' AI cyber attack, The Financial Times, 12 augustus 2026, https://www.ft.com/content/7d2ab3e0-9085-48f6-b38a-d90260d58795?syn-25a6b1a6=1.

347 Taiwan says it was hit by 'abnormal' AI-assisted cyber-attack, The Guardian, 13 augustus 2026, https://www.theguardian.com/technology/2026/aug/13/taiwan-ai-assisted-cyber-attacks-overseas.

348 At least 12 states face cyberattacks on their water systems, sources say, Luke Barr, Jack Date, Katherine Faulders, Josh Margolin & Aaron Katersky / ABC News, 4 augustus 2026, https://abcnews.com/US/12-states-face-cyberattacks-water-systems-sources/story?id=135348482.

349 CISA Urges Water and Wastewater Systems Sector to Protect OT Against Activity Targeting PLCs, CISA / Cybersecurity and Infrastructure Security Agency, 30 juli 2026, https://www.cisa.gov/news-events/alerts/2026/07/30/cisa-urges-water-and-wastewater-systems-sector-protect-ot-against-activity-targeting-plcs.

350 VS roept vitale infrastructuur op om systemen achter firewall of vpn te plaatsen, Security.nl / Redactie, 26 augustus 2026, https://www.security.nl/posting/950579/VS+roept+vitale+infrastructuur+op+om+systemen+achter+firewall+of+vpn+te+plaatsen.

351 Malicious Cyber Actors Targeting Water and Wastewater Sector Internet Facing Programmable Logic Controllers, Causing Operational Disruptions, FBI, 30 juli 2026, https://www.ic3.gov/PSA/2026/PSA260730.pdf.

352 Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure, CISA, FBI, NSA, EPA, Department of Energy, U.S. Cyber Command / Joint Cybersecurity Advisory (AA26-097A), 7 april 2026 (bijgewerkt 22 juli 2026), https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a.

353 Iran shut down British power plant for four days in unprecedented cyber attack, The Telegraph, 22 augustus 2026, https://www.telegraph.co.uk/news/2026/08/22/iranian-hackers-shut-down-uk-power-plant/.

354 Small UK power generator shut after Iran-linked cyberattack: report, CNBC, 23 augustus 2026, https://www.cnbc.com/2026/08/23/small-uk-power-plant-shut-down-after-iran-linked-cyberattack-report.html.

Colofon

Het Cybersecuritybeeld Nederland 2026 (CSBN 2026) biedt inzicht in de digitale dreiging, de belangen die daardoor kunnen worden aangetast, de digitale weerbaarheid en tot slot de digitale risico's. Daarnaast vormt het CSBN 2026 een inhoudelijke basis voor de evaluatie van het actieplan voor de Nederlandse Cybersecurity Strategie 2022-2028. De focus van het CSBN ligt op de nationale veiligheid.

Het CSBN is opgesteld door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). De NCTV heeft dankbaar gebruikgemaakt van de informatie, de inzichten en de expertise van overheidsdiensten, kritieke entiteiten, wetenschappers en andere partijen. Ook het Nationaal Cyber Security Centrum (NCSC), de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) dragen substantieel bij aan het CSBN. Het CSBN wordt jaarlijks door de NCTV vastgesteld.

De NCTV draagt samen met partners uit het veiligheidsdomein bij aan een veilig en stabiel Nederland door dreigingen te onderkennen en de weerbaarheid en bescherming van nationale veiligheidsbelangen te versterken. Doel is het voorkomen en beperken van maatschappelijke ontwrichting. Als coördinator zorgt de NCTV voor de strategische verbinding tussen alle betrokken partners in het veiligheidsdomein, voor het reduceren van nationale veiligheidsrisico's en - als het erop aankomt - het beheersen van nationale crises.

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

November 2026