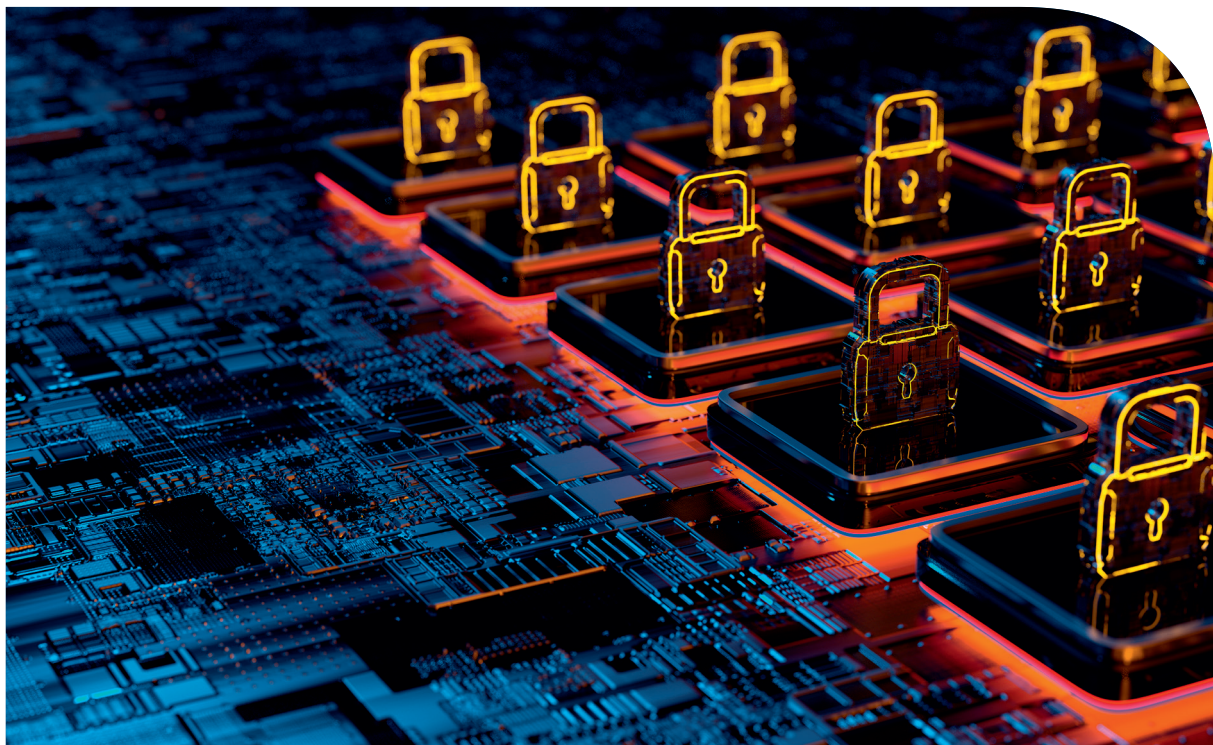




Cyberadvies

*Edge devices structureel doelwit
van Chinese cyberactoren*

Algemene Inlichtingen- en Veiligheidsdienst (AIVD)

Militaire Inlichtingen- en Veiligheidsdienst (MIVD)

Nationaal Cyber Security Centrum (NCSC)

oktober 2026

Cyberadvies

Edge devices structureel doelwit van Chinese cyberactoren

Essentie

- De Militaire Inlichtingen- en Veiligheidsdienst (MIVD) heeft in zijn Openbaar Jaarverslag over 2025 gewaarschuwd voor een verdere toename van Chinese cybercampagnes waarbij misbruik wordt gemaakt van kwetsbaarheden in *edge devices*.
- Chinese cyberactoren investeren in diepgaande kennis over *edge devices*.
- Naast het onderzoeken van technische specificaties van westerse producten via *reverse engineering*, verkrijgen Chinese actoren ook kennis over (de werking van) westerse producten via cyberspionage. Een voorbeeld hiervan is dat Chinese actoren beschikken over broncode van bepaalde westerse producten.
- De combinatie van diepgaande kennis over (de werking van) westerse producten (waaronder broncode), de intensieve ondersteuning door een wijldvertakt netwerk van Chinese bedrijven en kennisinstellingen en de ontwikkelingen op het gebied van kunstmatige intelligentie in het cyberdomein, zal naar verwachting leiden tot meer misbruik van *edge devices* door Chinese cyberactoren.
- De combinatie van deze factoren stelt Chinese cyberactoren niet alleen in staat om jaarlijks een groot aantal onbekende kwetsbaarheden te ontdekken en uit te buiten maar ook om reeds bekende kwetsbaarheden snel te operationaliseren voor cyberspionage.
- Uw organisatie moet dus voorbereid zijn op misbruik van zowel (kortgeleden) bekendgemaakte als van onbekende kwetsbaarheden.
- Ga na of de voordelen van het snel mitigeren van een kwetsbaarheid opweegt tegen de nadelen, zoals het risico op instabiliteit van applicaties of systemen. Misbruik en schade van zowel bekende als onbekende kwetsbaarheden kan worden voorkomen of verminderd door: *defense in depth*, leveranciersdiversiteit, gecentraliseerde logging, *security monitoring/response* en *forensic readiness*.

Cyberadvies

Edge devices structureel doelwit van Chinese cyberactoren

Context

Misbruik kwetsbare *edge devices* door Chinese actoren

De Militaire Inlichtingen- en Veiligheidsdienst (MIVD) heeft in zijn Openbaar Jaarverslag (2025) gewaarschuwd voor een verdere toename van Chinese cybercampagnes waarbij misbruik wordt gemaakt van kwetsbaarheden in *edge devices*.¹ *Edge devices* zijn apparaten die zich aan de rand van een netwerk bevinden en direct verbonden zijn met het internet, zoals firewalls, proxies, portals en VPN-gateways. Door deze positionering bevinden *edge devices* zich op een kwetsbare plek in het netwerk waarbij deze vanaf het internet aangevallen kunnen worden. Hoewel diverse cyberactoren kwetsbaarheden in *edge devices* misbruiken, is het met name een gekende werkwijze van Chinese cyberactoren. Chinese cyberactoren troffen de afgelopen jaren via kwetsbare *edge devices* tal van netwerken van verschillende slachtoffers, waaronder Nederlandse organisaties.

In dit cyberadvies zal verder toegelicht worden welke factoren leiden tot de waarschuwing dat misbruik van kwetsbare *edge devices* door Chinese actoren verder zal toenemen en hoe organisaties zich hiertegen kunnen weren.

Factoren van invloed op (toename) misbruik kwetsbare *edge devices*

Er is sprake van diepgaande kennis van *edge devices* bij Chinese actoren. Chinese actoren bestuderen (de werking van) westerse producten. Door middel van reverse engineering verkrijgen Chinese actoren de nodige inzichten om kwetsbaarheden in *edge devices* te kunnen misbruiken. Chinese actoren vinden ook kwetsbaarheden in *edge devices* door middel van cyberspionage, bijvoorbeeld door het bemachtigen van broncode van bepaalde westerse producten.

Sinds 2021 bestaat er wetgeving in China die partijen verplicht stelt om kwetsbaarheden te melden. Daarnaast zijn er China specifieke opleidingsprogramma's ontwikkeld en kennisinstellingen ingericht, met als doel het hacken van *edge devices* die deel uitmaken van westerse digitale infrastructuur. Daarnaast voeren Chinese bedrijven niet alleen gericht onderzoek uit naar kwetsbaarheden in (westerse) producten maar leveren ze ook direct inzetbare exploits.

¹ Eerder waarschuwde de MIVD al in samenwerking met het NCSC voor grootschalig misbruik van *edge devices* tijdens de COATHANGER campagne.

Cyberadvies

Edge devices structureel doelwit van Chinese cyberactoren

Het Chinese ecosysteem draagt op deze manier bij aan de kennisontwikkeling binnen China over kwetsbaarheden in westerse digitale infrastructuur en aan het vermogen van Chinese actoren om offensieve cyberoperaties uit te voeren tegen westerse doelwitten.

De Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en Algemene Inlichtingen- en Veiligheidsdienst (AIVD) waarschuwen in de openbare jaarverslagen van 2025 voor de mogelijkheden die kunstmatige intelligentie biedt op het gebied van cyberaanvallen. De ontwikkeling en beschikbaarheid van kunstmatige intelligentie zal naar verwachting bijdragen aan een toename van misbruik van kwetsbare *edge devices*, ook door Chinese actoren.

De combinatie van deze factoren stelt Chinese cyberactoren niet alleen in staat om jaarlijks een groot aantal onbekende kwetsbaarheden te ontdekken en uit te buiten maar ook om reeds bekende kwetsbaarheden snel te operationaliseren.

Wat kunnen actoren met broncode?

Wanneer actoren toegang weten te krijgen tot de broncode van een product, stelt dit de actor in staat om het product waar deze code op draait grondig te analyseren. De broncode laat in detail zien hoe een product werkt, waardoor fouten in de code opgespoord kunnen worden. Daarna kan een actor, met de fouten in de code, aanvalstools bouwen om onbekende kwetsbaarheden (zero-days) uit te buiten. De ondersteuning van het Chinese ecosysteem en de inzet van kunstmatige intelligentie op broncode van een product leiden ertoe dat actoren kwetsbaarheden in producten steeds sneller en makkelijker kunnen misbruiken.

Cyberadvies

Edge devices structureel doelwit van Chinese cyberactoren

Advies

Dit cyberadvies is geen oplossing om volledig te voorkomen dat aanvallen met bekende en onbekende kwetsbaarheden gemitigeerd kunnen worden. Het doel van onderstaand advies is om een handelingsperspectief te bieden waarbij het risico op compromittatie of eventuele verdere schade na een succesvolle compromittatie verlaagd kan worden. Daarbij is het in de eerste plaats belangrijk om de te beschermen belangen van uw organisatie in kaart te brengen om deze voldoende te kunnen beschermen.²

Omgaan met kwetsbaarheden

Op het moment dat een kwetsbaarheid in een bepaald type *edge device* bekend wordt, neemt het risico op uitbuiting van die kwetsbaarheid exponentieel toe. Uit inlichtingen van de AIVD en MIVD blijkt dat Chinese actoren niet alleen zero-days inzetten, maar ook vaak misbruik maken van reeds bekende kwetsbaarheden. Dit onderschrijft het belang om de door de leverancier beschikbaar gestelde beveiligingsupdates door te voeren. Omdat vaak niet bekend is wat de impact van een beveiligingsupdate op een productie-omgeving is, is het niet altijd verstandig om beveiligingsupdates direct te implementeren. Ga na of de voordelen van het snel mitigeren van een kwetsbaarheid opwegen tegen de nadelen, zoals het risico op instabiliteit van applicaties of systemen.

Onderstaande handelingsperspectieven zijn vooral gericht op het verlagen van het risico in de situatie waarbij een actor een onbekende kwetsbaarheid inzet, of wanneer het niet mogelijk is beveiligingsupdates door te voeren om bekende kwetsbaarheden te mitigeren.

² Meer informatie hierover is te vinden op: <https://www.ncsc.nl/risicomanagement/hoe-breng-ik-mijn-te-beschermen-belangen-kaart>

Cyberadvies

Edge devices structureel doelwit van Chinese cyberactoren

Defence in depth

Om schade te beperken nadat een actor toegang heeft gekregen tot het netwerk en snelle detectie mogelijk te maken, is defense in depth effectief. Defense in depth bouwt de informatiebeveiliging van een netwerk gelaagd op. Wanneer een actor een laag van beveiliging doorbreekt, vertragen de andere beveiligingslagen de actor.

Voorbeelden van *defense in depth* zijn onder andere, maar niet uitsluitend:

- Voor de organisatie op maat geconfigureerde firewalls
- *Intrusion detection systems*
- Organisatiebrede multi-factorauthenticatie
- Netwerksegmentatie
- Versleutelen van data op verschillende lagen binnen het netwerk

Aanvullend hierop adviseren de diensten meer leveranciersdiversiteit binnen de verschillende defensieve lagen van het netwerk. Het inzetten van apparatuur van diverse leveranciers kan de verdediging versterken. In het scenario waarbij een actor diepgaand onderzoek heeft gedaan naar specifieke productlijnen, kan de variatie in apparatuur voorkomen dat actoren met gerichte aanvalsmethodes door meerdere beveiligingslagen breken.

Detectie en incident management

Gecentraliseerde logging

Uit ervaring van de diensten blijkt dat slachtoffers van incidenten vaak niet in staat zijn om de benodigde logbestanden aan te leveren. Het komt vaak voor dat logging niet, of met een zeer korte retentietijd, opgeslagen wordt. Daarnaast is de ervaring van de diensten dat incidentlogging lokaal op de apparaten staat opgeslagen. Actoren die het apparaat hebben gecompromitteerd kunnen de logbestanden aanpassen of wissen.

Cyberadvies

Edge devices structureel doelwit van Chinese cyberactoren

Het advies is om een centraal logsysteem in een afgeschermd segment van het netwerk in te richten, bijvoorbeeld bij het Security Operations Center (SOC). Alle essentiële apparaten in het netwerk dienen de logbestanden naar dit centrale systeem te sturen. Zo wordt voorkomen dat tijdens incidenten, door een gebrek aan logging, onduidelijk blijft wat de schade is. Daarnaast is het van belang om logbestanden gedurende een langere periode te bewaren. Het advies is om een retentietijd aan te houden van minimaal een halfjaar, maar bij voorkeur een jaar of langer.

Security monitoring/response

Zorg voor een volwassen en gedegen security monitoring-ecosysteem binnen het netwerk van uw organisatie, inclusief een opgeleid en getraind SOC. Uit ervaring blijkt dat wanneer de *security monitoring* effectief is en het SOC dreigingen op het netwerk snel signaleert en adequaat reageert op ongebruikelijke activiteiten, de schade en impact beperkt kunnen blijven. Om de effectiviteit van de securitymonitoring en -response te verhogen is het advies om aanvalspaden binnen het netwerk periodiek te testen en dan te kijken of het SOC de gesimuleerde aanvallen en incidenten herkent en hier goed op wordt gereageerd.

Forensic readiness

Bij cyberincidenten zijn organisaties vaak niet startklaar voor het uitvoeren van een digitaal forensisch onderzoek. Hier is voordeel te behalen door goed voorbereid te zijn op het onderzoeken van cyberincidenten, door personeel te trainen en periodiek te laten oefenen met digitaal forensisch onderzoek en voorbereid te zijn op cyberincidenten.

Met een goede voorbereiding kan sneller en effectiever aan het onderzoek begonnen worden. Dit resulteert uiteindelijk in lagere kosten voor de uitvoering van het onderzoek. Ook kan dan de doorlooptijd van digitale forensische onderzoeken worden verkort.

Analyse van de totale impact van incidenten op de organisatie en de infrastructuur (oftewel: *damage assessment*) helpt om passende maatregelen nemen voor effectieve mitigatie van incidenten en forensic readiness.

Cyberadvies

Edge devices structureel doelwit van Chinese cyberactoren

Verder lezen

Raadpleeg onderstaande bronnen voor verdere verdieping:

- AIVD, Verdedigbaar Netwerk – Hoe doe je dat?, 19 augustus 2024, www.aivd.nl/documenten/2024/08/19/aivd-publicatie-verdedigbaar-netwerk-hoe-doe-je-dat.
- AIVD/MIVD, Logging Essentials, <https://github.com/JSCU-NL/logging-essentials>.
- NCSC, Infosheet Basismaatregelen, d.d. 1 oktober 2023, www.ncsc.nl/documenten/publicaties/2023/december/01/infosheet_basismaatregelen.
- NCSC, Disaster Recovery Plan, d.d. 5 februari 2026, www.ncsc.nl/incidenten-en-herstellen/disaster-recovery-plan.
- NCSC, Beheerlijst voor Edge Devices, d.d. 15 januari 2026, www.ncsc.nl/edge-devices/beheerlijst-voor-edge-devices.
- NCSC, SOC van de Toekomst, d.d. 9 december 2025, www.ncsc.nl/incidenten-en-herstellen/soc-van-de-toekomst.
- NCSC, Bent u al klaar voor Forensic Readiness?, d.d. 12 mei 2021, www.ncsc.nl/actueel/weblog/weblog/2021/bent-u-al-klaar-voor-forensic-readiness.
- NCSC, Bereid u voor op Zero Trust, d.d. 18 augustus 2021, https://www.ncsc.nl/binaries/ncsc/documenten/factsheets/2021/augustus/18/factsheet-bereid-u-voor-op-zero-trust/Factsheet_bereid+u+voor+op+Zero+Trust+v1.0_aug21_NL.pdf.
- NCSC, Factsheet SOC inrichten, d.d. 3 mei 2023, www.ncsc.nl/documenten/factsheets/2019/juni/01/soc-inrichten.
- NCSC, Aanhoudende statelijke cyberspionagecampagne via kwetsbare edge devices, d.d. 10 juni 2024, <https://www.ncsc.nl/actueel/nieuws/2024/juni/10/aanhoudende-stataelijke-cyberspionagecampagne-via-kwetsbare-edge-devices>.

Cyberadvies

Edge devices structureel doelwit van Chinese cyberactoren

Over dit cyberadvies

De AIVD en MIVD publiceren regelmatig adviezen die voortkomen uit inlichtingenonderzoeken van beide diensten. Deze publicaties zijn te vinden op de websites van Defensie (MIVD) en AIVD. Het doel van een cyberadvies (CA) is om afnemers door middel van beveiligingsmaatregelen, in nauwe samenwerking met het NCSC, concreet handelingsperspectief te bieden zodat de weerbaarheid wordt verhoogd. Dit handelingsperspectief is gebaseerd op getoetste inlichtingen, kennis en expertise.

Verspreiding cyberadvies

Dit document heeft de merking **TLP:CLEAR**

Onder voorbehoud van de regels op het gebied van auteursrechten kan TLP:CLEAR-informatie onbeperkt worden verspreid (met inachtneming van de toepasselijke voorschriften en procedures voor openbaarmaking van informatie).

Algemene Inlichtingen- en Veiligheidsdienst (AIVD)
aivd.nl

Militaire Inlichtingen- en Veiligheidsdienst (MIVD)
defensie.nl

Nationaal Cyber Security Centrum (NCSC)
ncsc.nl

oktober 2026