TLP:CLEAR



Cyberadvies

Russische statelijke actoren compromitteren IP-camera's in Europa voor militaire doeleinden

Algemene Inlichtingen- en Veiligheidsdienst (AIVD)
Militaire Inlichtingen- en Veiligheidsdienst (MIVD)

juli 2026

Cyberadvies

Russische statelijke actoren compromitteren IP-camera's in Europa voor militaire doeleinden

Essentie

- Russische statelijke actoren voeren stelselmatig **digitale spionageoperaties** uit via camera's die toegang hebben tot het internet, zogenoemde **IP-camera's**.
- Zo voert ten minste één **Russische inlichtingen- en veiligheidsdienst** digitale spionageoperaties uit via IP-camera's **in Nederland**, verschillende **andere EU- en NAVO-lidstaten en Oekraïne**.
- Deze actor analyseert de beelden geautomatiseerd met behulp van beeldherkenningssoftware, om zo gericht te zoeken naar militaire voertuigen en de (militaire) ladingen die deze vervoeren.
- Zo verkrijgt de actor onder andere **militair relevante gegevens**, zoals militaire transportroutes van de EU en de NAVO, wapenleveringen aan Oekraïne en de locaties van Oekraïens militair personeel.
- De informatie van IP-camera's in Oekraïne wordt onder andere gebruikt voor pogingen om **Oekraïense militairen uit te schakelen en hun militair materiaal te vernietigen**.
- Daarnaast gebruikt de Russische dienst de toegang tot IP-camera's om militair relevante inlichtingen te verwerven in Europese lidstaten, ook wanneer deze niet relevant zijn voor de oorlog in Oekraïne.
- Op basis van inlichtingen blijkt dat het aantal digitale spionageoperaties van Russische statelijke actoren ter ondersteuning van militaire operaties tijdens de oorlog met Oekraïne stelselmatig is toegenomen.
- Mensen en organisaties in Nederland en Europa kunnen de **risico's op spionage verkleinen** door zelf **maatregelen te treffen** bij het gebruik van IP-camera's, zoals:
  - Beperk directe toegang tot de IP-camera vanaf het internet.
  - Beperk het gezichtsveld van de IP-camera.
  - Beheer de toegang en authenticatie van gebruikers van de IP-camera.
  - Onderhoud de firm- en software van de IP-camera.

Cyberadvies

Russische statelijke actoren compromitteren IP-camera's in Europa voor militaire doeleinden

Context

Russische digitale spionageoperaties via IP-camera's

Inlichtingen van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) laten zien dat Russische statelijke actoren stelselmatig digitale spionageoperaties uitvoeren via camera's die toegang hebben tot het internet (IP-camera's). Dit gebeurt in Nederland, verschillende andere EU- en NAVO-lidstaten en Oekraïne, door ten minste één Russische inlichtingen- en veiligheidsdienst. Dit cyberadvies sluit af met concrete adviezen die kunnen worden toegepast om de risico's op spionage via IP-camera's te verkleinen.

De informatie die de Russische statelijke actor weet te verkrijgen via digitale spionageoperaties met IP-camera's geeft onder andere inzicht in militair relevante gegevens, zoals militaire transportroutes van Europa en de NAVO, en wapenleveringen aan Oekraïne. De Russische statelijke actor gebruikt beeldherkenningssoftware om gericht te zoeken naar militaire voertuigen en (militaire) ladingen.

De toegang tot IP-camera's die de Russische statelijke actor in Oekraïne weet te bemachtigen wordt in sommige gevallen gebruikt om locaties van Oekraïens militair personeel te identificeren. Inlichtingen tonen aan dat deze informatie vervolgens wordt gebruikt om Oekraïense militairen en militair materiaal in gebruik van de Oekraïense krijgsmacht uit te schakelen. Verder stellen de diensten vast dat de Russische dienst de toegang tot IP-camera's gebruikt om militair relevante inlichtingen te verwerven in NAVO- en EU-lidstaten, ook wanneer deze niet relevant zijn voor de oorlog in Oekraïne.

Tot nu toe hebben de AIVD en de MIVD niet waargenomen dat de Russische statelijke actor dergelijke informatie gebruikt voor militaire aanvallen buiten Oekraïne. Wel laat dit zien dat de Russische dienst in staat is om relevante inlichtingen te vergaren uit IP-camera's en dat dezelfde tactieken mogelijk gebruikt kunnen worden door Russische militaire eenheden in een eventueel toekomstig conflict.

Cyberadvies

Russische statelijke actoren compromitteren IP-camera's in Europa voor militaire doeleinden

Digitale spionage ter ondersteuning van de Russische oorlog in Oekraïne

Naar inschatting van de AIVD en MIVD is het aantal digitale spionageoperaties van Russische statelijke actoren ter ondersteuning van militaire operaties sinds het begin van de oorlog met Oekraïne stelselmatig toegenomen. De digitale activiteiten gericht tegen IP-camera's vormen daar slechts een onderdeel van. De Russische autoriteiten halen veel tactisch en strategisch voordeel uit de inzet van cyberoperaties, zowel vanuit defensief als offensief oogpunt. Zo heeft de MIVD eerder al gewaarschuwd voor verkenningsactiviteiten door Russische statelijke actoren gericht op logistieke routes, waaronder in Nederland.[1] [2]

De AIVD en MIVD hebben de afgelopen jaren meerdere activiteiten waargenomen waarbij Russische statelijke actoren cyberoperaties hebben ingezet om Oekraïens militair personeel en materiaal van de Oekraïense krijgsmacht te identificeren en uit te schakelen. Ook achten de diensten het zeer waarschijnlijk dat de dreiging richting de Oekraïense strijdkrachten door Russische cyberoperaties in vrijwel heel Oekraïne toeneemt. Daarnaast is het mogelijk dat Oekraïense operaties en troepenbewegingen door deze cyberoperaties vroegtijdig onderkend worden en daardoor verstoord of minder effectief kunnen worden.

Hoe krijgen Russische actoren toegang tot IP-camera's?

Op internet zijn verschillende diensten beschikbaar die het mogelijk maken om gemakkelijk, snel en gericht een omgeving te scannen op apparaten. Op basis van de kenmerken van de apparaten, zoals merknamen, kunnen vervolgens IP-camera's worden geïdentificeerd.[3]

Wanneer de IP-camera is geïdentificeerd, kan de kwaadwillende partij via het internet proberen toegang te krijgen tot de IP-camera. Dit lukt vaak relatief eenvoudig, omdat veel IP-camera's die op het internet zijn aangesloten onvoldoende beveiligd zijn. Zo hebben ze vaak standaard wachtwoorden, verouderde firmware en standaardconfiguraties.

[1] MIVD, Russian GRU Targeting Western Logistics Entities and Technology Companies, d.d. 13 mei 2025 https://www.defensie.nl/documenten/2025/05/21/russian-gru-targeting-western-logistics-entities-and-technology-companies.

[2] CISA, Russian GRU Targeting Western Logistics Entities and Technology Companies, d.d. 17 april 2026, https://www.cisa.gov/news-events/cybersecurity-advisories/aa25014 1a.

[3] NCSC, Het internet wordt gescand, https://www.ncsc.nl/edge-devices/het-internet-wordt-gescand.

Cyberadvies

Russische statelijke actoren compromitteren IP-camera's in Europa voor militaire doeleinden

Advies

Publieke en private partijen kunnen zelf maatregelen nemen om het risico op spionage zo klein mogelijk te maken. Hierbij zijn met name het gezichtsveld en de toegankelijkheid van de IP-camera vanaf het internet belangrijk.

Beperk directe toegang tot IP-camera's vanaf het internet

- Zorg dat livestreams niet publiek toegankelijk zijn via het internet, tenzij deze streams een noodzakelijk doel dienen.
- Gebruik geen portforwarding[4]-functionaliteiten op de router van het netwerk om de IP-camera van buitenaf beschikbaar te maken.
- Schakel Universal Plug and Play (UPnP) uit op de IP-camera. Deze instelling zorgt ervoor dat portforwarding geautomatiseerd wordt.
- Configureer het eigen lokale netwerk zodanig dat een Virtual Private Network (VPN)-verbinding gebruikt kan worden om via het internet connectie te maken met het eigen lokale netwerk. Vervolgens kan de IP-camera via de VPN-verbinding benaderd worden.
- Schakel protocollen die niet nodig zijn voor het gebruik van de IP-camera uit. Denk aan protocollen zoals SSH, Bonjour, FTP, UPnP en Telnet. Gebruik indien mogelijk alleen beveiligde protocollen zoals HTTPS en RTSPS.[5]

Beperk het gezichtsveld van de IP-camera

- Zorg dat de plaats van de IP-camera aansluit bij het doel en houd irrelevante objecten zoveel mogelijk uit beeld.
- Richt op internet aangesloten IP-camera's bij voorkeur op locaties en objecten die geen onderdeel zijn van logistieke doorstroming of openbare infrastructuur. Hierdoor verkleint het risico op digitale spionage gericht op cruciale routes, havens of laadzones.
- Maskeer gevoelige zones die in beeld zijn, bijvoorbeeld door deze te vervagen (blurren). De software van sommige IP-camera's maakt het mogelijk om specifieke delen van het beeld af te schermen.
- Beperk zichtbare details zoals GPS-locatie op de beelden van de stream.

[4] Portforwarding is een techniek om inkomend internetverkeer via een specifieke poort direct door te sturen naar een daarvoor geconfigureerd apparaat.

[5] Raadpleeg de handleiding van het apparaat en/of de leverancier voor een overzicht van de beschikbare instellingen en hoe deze geconfigureerd kunnen worden.

Cyberadvies

Russische statelijke actoren compromitteren IP-camera's in Europa voor militaire doeleinden

Toegangsbeheer en authenticatie

- Verander bij ingebruikname van een IP-camera direct de standaardwachtwoorden. Gebruik complexe, unieke wachtwoorden die niet in databases van gelekte wachtwoorden voorkomen.[6]
- Plaats IP-camera's in een (eigen) Virtual Local Area Network (VLAN), gescheiden van de rest van het netwerk.
- Gebruik het beheeraccount uitsluitend voor beheerzaken en niet voor toegang tot de stream van de IP-camera. Gebruik hiervoor enkel gebruikersaccounts met beperkte rechten.
- Maak voor toegang tot de stream van de IP-camera gebruik van Multi-Factor Authenticatie (MFA).

Onderhoud de firm- en software van de IP-camera

- Kies voor een IP-camera met meerdere jaren beveiligingsondersteuning op de firm- en software.
- Check periodiek op nieuwe beveiligingsupdates voor de firm- en software van de IP-camera.

Herkomst van de IP-camera

- Wees alert op de herkomst van de IP-camera. Een aantal landen, zoals China, Rusland en Iran, voeren actief een offensief cyberprogramma tegen Nederlandse belangen.[7]

Onbekende IP-camera's

- Wees alert op de aanwezigheid van onbekende IP-camera's op eigen terrein, of die gericht staan op eigen terrein. Deze IP-camera's zouden door externe actoren geplaatst kunnen zijn.

[6] Voor het checken of een wachtwoord voorkomt in een database van gelekte wachtwoorden kan gebruik worden gemaakt van diensten zoals https://haveibeenpwned.com/passwords.

[7] AIVD, Wat is een offensief cyberprogramma?, https://www.aivd.nl/vraag-en-antwoord/cyberdreiging/wat-is-een-offensief-cyberprogramma.

Cyberadvies

Russische statelijke actoren compromitteren IP-camera's in Europa voor militaire doeleinden

Verder lezen

Raadpleeg onderstaande bronnen voor verdere verdieping:

- AIVD, Wat is een offensief cyberprogramma?, https://www.aivd.nl/vraag-en-antwoord/cyberdreiging/wat-is-een-offensief-cyberprogramma.
- AIVD, Offensief cyberprogramma: een ideaal businessmodel voor staten, d.d. 27 juni 2019, https://www.aivd.nl/documenten/2019/06/27/offensief-cyberprogramma-een-ideaal-businessmodel-voor-staten.
- NCSC, Het internet wordt gescand, d.d. 13 november 2025, https://www.ncsc.nl/edge-devices/het-internet-wordt-gescand.
- NCSC, Wat is een VPN?, d.d. 18 november 2025, https://www.ncsc.nl/databeveiliging/wat-is-een-vpn.
- NCSC, Beveiligingstips voor Internet of Things (IoT), d.d. 29 mei 2026, https://www.ncsc.nl/edge-devices/beveiligingstips-voor-internet-of-things-iot.
- NCSC, Asset management, d.d. 16 december 2025, https://www.ncsc.nl/asset-management.
- NCSC UK, 'Smart' security cameras: Using them safely in your home, d.d. 3 maart 2020, https://www.ncsc.gov.uk/guidance/smart-security-cameras-using-them-safely-in-your-home.

Over dit cyberadvies

De AIVD en MIVD publiceren regelmatig adviezen die voortkomen uit inlichtingenonderzoeken van beide diensten. Deze publicaties zijn te vinden op de website van de AIVD, aivd.nl/cyberadviezen. Het doel van een cyberadvies (CA) is om afnemers door middel van beveiligingsmaatregelen concreet handelingsperspectief te bieden, zodat de weerbaarheid tegen statelijke actoren wordt verhoogd. De diensten bieden dit handelingsperspectief op basis van getoetste inlichtingen, kennis en expertise. Het accent ligt hierbij op de Europese veiligheid.

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)
Postbus 20010 | 2500 EA Den Haag
aivd.nl

Militaire Inlichtingen- en Veiligheidsdienst (MIVD)
defensie.nl

juli 2026