Week 02-2026

# Strategisch Dreigingsrapport: Analyse van het Actuele Cyberlandschap

## 1.0 Inleiding: Het Veranderende Dreigingslandschap

Het cyberdreigingslandschap evolueert in een versneld tempo en wordt gekenmerkt door een voortdurende professionalisering van cybercriminaliteit, geavanceerde en geopolitiek gemotiveerde staatscampagnes, en de opkomst van nieuwe technologieën zoals kunstmatige intelligentie (AI) als aanvalsvector. Criminele netwerken opereren steeds vaker volgens efficiënte, industriële maatstaven, terwijl statelijke actoren hun digitale capaciteiten integreren in multi-domein operaties. Dit rapport is opgesteld om strategische besluitvormers inzicht te geven in de meest relevante dreigingen en hun implicaties, en om een basis te bieden voor het versterken van de digitale weerbaarheid van de organisatie.De analyse in dit rapport concentreert zich op drie centrale thema's die het huidige en toekomstige dreigingsbeeld bepalen:

1. **De intensivering van geopolitieke spanningen in het digitale domein** , waarbij staten kritieke infrastructuur en overheidsinstanties targeten voor spionage en strategische positionering.
2. **De industrialisatie van cybercriminaliteit via 'as-a-service'-modellen** , die geavanceerde aanvalsmethoden toegankelijk maken voor een bredere groep kwaadwillenden en de efficiëntie van aanvallen verhogen.
3. **De strategische risico's en kansen die voortkomen uit opkomende technologieën** , met een specifieke focus op de dubbele rol van AI als zowel een defensief als offensief wapen.Het doorgronden van deze thema's vereist een diepgaande analyse van de actoren die deze trends aansturen, wier motivaties en methoden de contouren van het hedendaagse digitale conflict bepalen.

## 2.0 Analyse van Dreigingsactoren en Campagnes

Een effectieve verdedigingsstrategie berust op een fundamenteel inzicht in de motivaties en tactieken van de dreigingsactoren. De strategische calculus achter een staatsoperatie verschilt immers wezenlijk van de commerciële logica van een ransomware-aanval. Dit hoofdstuk analyseert daarom de meest significante statelijke en cybercriminele operaties die het huidige dreigingsbeeld definiëren.

### 2.1 Statelijke Actoren en Geopolitieke Spionage

Door China ondersteunde groepen voeren geavanceerde en langdurige spionagecampagnes uit, die de kwetsbaarheid van Europese en Amerikaanse strategische sectoren blootleggen. Zo richt de groep **UAT-7290** zich sinds 2022 op de Europese telecomsector door te infiltreren via kwetsbaarheden in edge-apparatuur zoals routers en firewalls. Eenmaal binnen maken zij gebruik van een gespecialiseerde Linux-malware suite, waaronder het modulaire implantaat **SilentRaid** , om persistente toegang te verkrijgen en inlichtingen te verzamelen. Een andere groep, **Salt Typhoon** , heeft de e-mailsystemen van medewerkers van het

Amerikaanse Huis van Afgevaardigden geïnfiltreerd. Deze operatie was niet alleen gericht op spionage, maar ook op strategische 'pre-positioning' om vitale netwerken in de toekomst te kunnen verstoren.Tegelijkertijd intensiveerde de aan de Russische militaire inlichtingendienst GRU gelieerde groep **BlueDelta** tussen februari en september 2025 haar operaties voor het verzamelen van inloggegevens. De groep richtte zich op Europese overheidsinstanties en de energiesector met geavanceerde phishing-campagnes. Hun tactiek omvat het misbruiken van legitieme documenten en het gebruik van gratis hostingdiensten (zoals ngrok en InfinityFree) om snel vervalste inlogportalen voor Microsoft OWA, Google en Sophos VPN op te zetten. Door deze aanpak kunnen ze hun infrastructuur snel opbouwen en afbreken, wat detectie bemoeilijkt.De Amerikaanse CyberCom-operatie **'Absolute Resolve'** illustreert op haar beurt de geavanceerde capaciteiten van westerse statelijke actoren en de verregaande integratie van digitale en fysieke oorlogsvoering. De operatie, die cruciaal was bij de arrestatie van de Venezolaanse president Maduro, integreerde digitale oorlogsvoering met een fysieke interventie. Door de industriële controlesystemen (ICS) van het elektriciteitsnet in Caracas over te nemen, kon de stroomvoorziening op het moment van de inval worden uitgeschakeld. Dit incident onderstreept de kwetsbaarheid van kritieke infrastructuur en de strategische impact die digitale interventies kunnen hebben op de soevereiniteit van een land.Collectief tonen deze campagnes van China, Rusland en de VS aan dat cyberspace niet langer een ondersteunend, maar een primair en beslissend domein is in geopolitieke conflicten, waar digitale superioriteit direct vertaald wordt naar strategisch voordeel.

### 2.2 Geprofessionaliseerde Cybercriminele Groeperingen

Terwijl statelijke actoren zich richten op geopolitieke dominantie, opereert een parallel dreigingsuniversum met een al even geavanceerd, maar commercieel gedreven, businessmodel dat de veerkracht van de private sector op de proef stelt. De **LockBit 5.0** -variant illustreert de technische verfijning binnen het Ransomware-as-a-Service (RaaS)-model. De malware maakt gebruik van geavanceerde encryptie (ChaCha20-Poly1305) en verfijnde anti-analysetechnieken om detectie te bemoeilijken. Om herstel te dwarsbomen, schakelt LockBit 5.0 systematisch processen uit die gerelateerd zijn aan back-updiensten, zoals de Volume Shadow Copy Service en oplossingen van Veeam.Andere groepen specialiseren zich in de infiltratiefase. De **Black Cat** -groepering zet zoekmachineoptimalisatie (SEO-poisoning) in om gebruikers te verleiden vervalste installatiebestanden van populaire software zoals Notepad++ en WinSCP te downloaden. Hun multi-stage infectieketen is ontworpen om detectie te omzeilen, onder meer door het gebruik van DLL side-loading en het direct laden van de uiteindelijke payload in het systeemgeheugen, waardoor traditionele scans van de harde schijf worden ontweken.Binnen dit ecosysteem fungeren actoren zoals **Storm-0249** als *Initial Access Broker* . Zij richten zich uitsluitend op het verkrijgen van initiële toegang tot bedrijfsnetwerken, die vervolgens wordt verkocht aan ransomware-groepen. Storm-0249 hanteert een bijzonder verraderlijke 'living-off-the-land'-tactiek door legitieme Windows-tools zoals PowerShell en curl te misbruiken om scripts op te halen en uit te voeren. Deze methode is strategisch significant omdat zij de grens tussen kwaadaardige en legitieme systeemactiviteit doelbewust vervaagt.De specialisatie en industrialisatie van cybercrime, van toegang tot encryptie, leiden

tot efficiëntere, veerkrachtigere en moeilijker te detecteren aanvalsketens die een fundamentele uitdaging vormen voor traditionele verdedigingsmechanismen.

## 3.0 Analyse van Aanvalsvectoren en Technieken

Ongeacht de motivatie van de actor—spionage, sabotage of financieel gewin—convergeren hun methoden naar een reeks fundamentele aanvalsvectoren. Het doorgronden van deze vectoren is de sleutel tot een proactieve en actor-agnostische verdediging. Dit hoofdstuk onderzoekt de meest prevalente en impactvolle technieken, van software-exploits tot geavanceerde social engineering en misbruik van digitale identiteiten.

### 3.1 Infiltratie via Software- en Hardwarekwetsbaarheden

Het niet tijdig installeren van beveiligingsupdates voor kritieke kwetsbaarheden blijft een significant risico. De kwetsbaarheid in **HPE OneView (CVE-2025-37164)** , met een CVSS-score van 10.0, maakt Remote Code Execution (RCE) mogelijk en wordt volgens het Amerikaanse agentschap CISA actief misbruikt. Ook de **Ni8mare** -kwetsbaarheid **(CVE-2026-21858)** in de automatiseringssoftware **n8n** (CVSS 10.0) stelt ongeauthenticeerde aanvallers in staat om servers volledig over te nemen.Kwetsbaarheden in het Internet of Things (IoT) kunnen directe fysieke gevolgen hebben. Een casus die dit illustreert, is de kwetsbaarheid in **elektrische rolstoelen van Whill (CVE-2025-14346)** . De Bluetooth-verbinding vereist geen authenticatie, waardoor een aanvaller binnen bereik de volledige besturing van de rolstoel kan overnemen, wat een ernstig veiligheidsrisico voor de gebruiker vormt. Bovendien vormt hardware waarvoor de fabrikant geen ondersteuning meer biedt, een permanent risico. Een recent ontdekte kwetsbaarheid in verouderde **D-Link DSL-modems** is hier een voorbeeld van. Omdat deze apparaten de end-of-life-status hebben bereikt, worden er geen beveiligingsupdates meer voor uitgebracht, waardoor ze een gemakkelijk doelwit blijven.Deze voorbeelden, variërend van enterprise software tot consumenten-IoT, illustreren een fundamentele en onveranderlijke zwakte in de digitale keten: de onvermijdelijke aanwezigheid van kwetsbaarheden en de kritieke, vaak verloren, race tussen patching en exploitatie.

### 3.2 Compromittering via Social Engineering en Phishing

De FBI waarschuwt voor de opkomst van 'quishing', ofwel phishing via QR-codes. Deze techniek is effectief omdat het de zakelijke beveiliging, zoals Endpoint Detection and Response (EDR), omzeilt. Een medewerker ontvangt de e-mail op een beveiligde computer, maar scant de QR-code met een persoonlijk, onbeheerd mobiel apparaat, waardoor de aanval buiten het zicht van de bedrijfsbeveiliging plaatsvindt.Aanvallers vergroten de geloofwaardigheid van hun phishing-aanvallen door legitieme clouddiensten te misbruiken. In een recente campagne werd **Google Cloud Application Integration** ingezet om e-mails te versturen vanaf een geverifieerd Google-domein, waardoor spamfilters werden gepasseerd. De aanvalsketen bevatte tevens een CAPTCHA-stap om geautomatiseerde scanners te misleiden voordat de gebruiker naar de nagemaakte Microsoft 365-inlogpagina werd geleid.Daarnaast maken opportunistische phishing-aanvallen vaak misbruik van actuele gebeurtenissen. Een recent voorbeeld is de waarschuwing van **KLM na een reeks vluchtannuleringen** . Cybercriminelen deden zich voor als medewerkers van de

klantenservice en benaderden gedupeerde reizigers met valse compensatie-aanbiedingen, inspelend op de urgentie en onzekerheid van de passagiers.Naast het misleiden van gebruikers vormt het compromitteren van hun digitale identiteit een andere cruciale en steeds vaker voorkomende aanvalsvector.

### 3.3 Misbruik van Identiteits- en Toegangsbeheer

De exponentiële groei van bots, serviceaccounts en AI-agenten introduceert een nieuwe categorie van **niet-menselijke identiteiten** . Deze vallen vaak buiten traditioneel beheer, beschikken over overmatige rechten en gebruiken statische, zelden gewijzigde credentials. Dit maakt hen tot een primair en vaak onzichtbaar doelwit voor aanvallers die op zoek zijn naar persistente toegang tot systemen.Het ontbreken van Multi-Factor Authenticatie (MFA) blijft een kritieke zwakte die dit risico verergert. Dit werd geïllustreerd bij **ownCloud** , waar aanvallers toegang kregen tot systemen door inloggegevens te gebruiken die waren gestolen van medewerkers via infostealer-malware zoals RedLine en Vidar. De aanval was succesvol omdat de betreffende accounts niet met MFA waren beveiligd.Aanvallers ontwikkelen methoden om niet de systemen zelf, maar de vertrouwensrelaties daartussen aan te vallen. De **ConsentFix-aanvalsmethode** is hier een treffend voorbeeld van, waarbij het legitieme OAuth-authenticatieproces in Microsoft Entra wordt gekaapt. Door een slachtoffer te verleiden een authenticatieproces te doorlopen en vervolgens de resulterende autorisatiecode uit de URL van de browser te kopiëren, kunnen aanvallers deze code inwisselen voor toegangstokens. Hiermee omzeilen ze Conditional Access-beleid en verkrijgen ze toegang tot de cloudomgeving van het slachtoffer.De analyse van deze fundamentele aanvalsvectoren legt de basis voor het begrijpen van de strategische impact die cyberdreigingen hebben op specifieke sectoren.

## 4.0 Strategische Implicaties per Sector

Hoewel de geanalyseerde dreigingen een universeel karakter hebben, verschillen de impact en de meest waarschijnlijke aanvalsvectoren aanzienlijk per sector. Een verstoring in de kritieke infrastructuur heeft andere maatschappelijke gevolgen dan een datalek in de commerciële sector. Het is daarom essentieel om een sector-specifieke risicoanalyse uit te voeren.

### 4.1 Kritieke Infrastructuur en Overheidsinstanties

Digitale aanvallen op vitale diensten kunnen de openbare veiligheid direct in gevaar brengen. De recente **DDoS-aanval op het 112-noodnummer** in Nederland, die de telefoonlijnen tijdelijk blokkeerde, is hiervan een sprekend voorbeeld. Ook de **netwerkstoring bij Vodafone** in de regio Eindhoven, die de communicatie van hulpdiensten zoals de brandweer trof, illustreert de kwetsbaarheid van operationele communicatie.De telecommunicatiesector blijft een primair doelwit voor spionage en sabotage. Het rapport van Cyble bevestigt dat deze sector in het vizier is van een combinatie van financieel, statelijk en ideologisch gemotiveerde actoren. De campagnes van de Chinese groep **UAT-7290** tegen Europese telecomproviders onderstrepen de aanhoudende dreiging van langdurige infiltratie.De infiltratie van de e-mailsystemen van **Amerikaans Congrespersoneel** door de Chinese groep **Salt Typhoon** legt de kwetsbaarheid van overheidscommunicatie bloot en

onderstreept het strategische risico van 'pre-positioning', waarbij aanvallers zich in systemen nestelen om in de toekomst disruptieve acties uit te kunnen voeren.

### 4.2 Commerciële en Financiële Sector

Een cyberaanval kan verwoestende gevolgen hebben voor productiebedrijven. De casus van **Jaguar Land Rover** illustreert dit duidelijk: een aanval leidde tot een langdurige productiestilstand en logistieke verstoringen. Dit vertaalde zich direct in een significante daling van de kwartaal- en verkoopcijfers, met een genoteerd verlies van omgerekend 550 miljoen euro.Het midden- en kleinbedrijf (MKB) is een aantrekkelijk en vaak onderbelicht doelwit. De **SafePay-ransomware** richt zich voor meer dan 90% op MKB-bedrijven, met name in regio's met een hoog bruto binnenlands product zoals Noord-Amerika en West-Europa. Deze groepen speculeren erop dat kleinere bedrijven vaak minder middelen hebben voor geavanceerde beveiliging.Malware gericht op eindgebruikers blijft een directe financiële dreiging. De **Astaroth-bankentrojans** , die zich verspreiden via een WhatsApp-worm, zijn ontworpen om webbrowsing-activiteiten te monitoren. Zodra een gebruiker een bankwebsite bezoekt, wordt de malware actief om inloggegevens te stelen en financiële transacties te onderscheppen.De technologiesector is niet alleen een doelwit, maar ook de bron van veel kwetsbaarheden en de motor achter de volgende generatie dreigingen.

## 5.0 Opkomende Dreigingen en Toekomstperspectief

Strategische planning vereist dat men vooruitkijkt naar opkomende dreigingen die het landschap fundamenteel kunnen veranderen. Dit hoofdstuk richt zich op twee cruciale ontwikkelingen: de transformerende rol van kunstmatige intelligentie, die zowel nieuwe aanvalsmogelijkheden creëert als nieuwe aanvalsoppervlakken introduceert, en de toenemende professionalisering van desinformatie als onderdeel van cybercampagnes.

### 5.1 De Dubbele Rol van Kunstmatige Intelligentie

Kunstmatige intelligentie wordt steeds vaker ingezet als een offensief wapen. Beveiligingsbedrijf VIPRE waarschuwt voor de opkomst van **AI-native malware** , die autonoom kan opereren en zich in realtime kan aanpassen aan de omgeving om detectie te omzeilen. Tegelijkertijd wordt het fenomeen **'vibe coding'** waargenomen, waarbij cybercriminelen AI gebruiken om snel ransomware te genereren. Hoewel deze AI-gegenereerde code vaak nog beperkingen kent, zoals 'hallucinaties' die tot fouten leiden, verlaagt het de drempel voor het creëren van malware.Het wijdverbreide gebruik van AI-platformen creëert tevens een nieuw, waardevol aanvalsoppervlak. Een recente casus van **kwaadaardige Chrome-extensies** illustreert dit risico: meer dan 900.000 gebruikers installeerden extensies die heimelijk hun gesprekken met AI-chatbots zoals ChatGPT en DeepSeek stalen. De buitgemaakte conversaties bevatten vaak vertrouwelijke informatie, zoals bedrijfseigen programmacode en zakelijke strategieën.Het misbruik van generatieve AI leidt tot aanzienlijke maatschappelijke risico's. De AI-chatbot **Grok (X)** wordt op grote schaal ingezet voor het creëren van non-consensuele, seksueel getinte beelden. De omvang van dit misbruik heeft geleid tot juridische acties van de Europese Commissie, die het platform heeft gesommeerd alle data te bewaren in het kader van een onderzoek onder de Digital Services Act (DSA).

### 5.2 De Professionalisering van Desinformatie en Misleiding

Een opkomende trend is het publiceren van valse claims door dreigingsactoren om reputatie op te bouwen of verwarring te zaaien. Dit werd zichtbaar bij de valse hackclaim tegen chipmachinefabrikant **ASML** . Een vergelijkbare situatie deed zich voor bij beveiligingsbedrijf **Resecurity** , waar een groep genaamd Scattered Lapsus$ Hunters een inbreuk claimde die nooit had plaatsgevonden.De casus van Resecurity toont een geavanceerde, proactieve verdedigingsstrategie. In plaats van de aanvallers te blokkeren, lokte het bedrijf hen in een geavanceerde **honeypot** gevuld met **synthetische data** , waaronder tienduizenden nep-klantrecords. Dit stelde Resecurity in staat om de aanvallers te misleiden, hun tactieken, technieken en procedures (TTP's) te bestuderen en hun infrastructuur te identificeren. De verzamelde inlichtingen leidden uiteindelijk tot een dagvaarding door opsporingsdiensten.De strijd om informatie en perceptie is een integraal onderdeel geworden van het cyberdreigingslandschap. Deze ontwikkelingen vormen de basis voor de strategische conclusies en aanbevelingen van dit rapport.

## 6.0 Conclusie en Strategische Aanbevelingen

De analyses in dit rapport schetsen een beeld van een complex en dynamisch dreigingslandschap. De belangrijkste bevindingen wijzen op een convergentie van geopolitieke en criminele dreigingen, een diepgewortelde kwetsbaarheid in zowel software- als identiteitsinfrastructuren, en de disruptieve impact van kunstmatige intelligentie. Statelijke actoren tonen de capaciteit om kritieke infrastructuur te ontregelen, terwijl geprofessionaliseerde cybercriminelen een industrieel ecosysteem hebben opgebouwd dat efficiënt en moeilijk te bestrijden is. Tegelijkertijd creëert AI nieuwe aanvalsmogelijkheden en aanvalsoppervlakken die traditionele beveiligingsmodellen uitdagen.Het hoofd bieden aan dit dreigingslandschap is geen louter technische opgave meer, maar een strategische noodzaak die een fundamentele herijking van het risicobeleid vereist. Op basis van de gepresenteerde analyses worden de volgende strategische aanbevelingen gedaan voor besluitvormers:

1. **Prioriteer Identity-First Security** De grens tussen menselijke en niet-menselijke gebruikers vervaagt. Het is cruciaal om een 'identity-first' beveiligingsstrategie te implementeren die zowel menselijke als niet-menselijke identiteiten (zoals serviceaccounts en AI-agenten) omvat. Dit vereist strikte toegangscontroles op basis van het 'least privilege'-principe en het verplicht stellen van Multi-Factor Authenticatie (MFA) voor alle accounts, in het bijzonder voor die met verhoogde rechten.
2. **Versterk de Weerbaarheid van Kritieke Infrastructuur** De bewezen capaciteit van statelijke actoren om vitale diensten zoals elektriciteitsnetwerken te manipuleren, vereist een geïntegreerde aanpak voor de bescherming van zowel IT- als Operationele Technologie (OT), inclusief Industriële Controlesystemen (ICS). Organisaties moeten uitgaan van een scenario waarin deze systemen doelwit zijn en de verdediging hierop inrichten met een focus op segmentatie, monitoring en snelle respons.
3. **Implementeer een Proactief Vulnerability Management Programma** De actieve exploitatie van kritieke kwetsbaarheden en de aanhoudende risico's van end-of-life systemen benadrukken de noodzaak van een robuust en proactief programma voor kwetsbaarheidsbeheer. Het tijdig patchen van systemen met een hoge CVSS-score

en het planmatig uitfaseren van verouderde hardware en software moeten kernonderdelen zijn van het IT-beleid.

4. **Bereid de Organisatie voor op AI-Gedreven Dreigingen** De opkomst van AI als zowel aanvalsvector als aanvalsoppervlak vraagt om een vooruitziende blik. Organisaties moeten beleid ontwikkelen voor het veilige gebruik van AI-tools door medewerkers om datadiefstal via malafide applicaties te voorkomen. Daarnaast is het essentieel om personeel te trainen in het herkennen van nieuwe, door AI aangedreven aanvalsvormen, zoals geavanceerde deepfakes en hyper-gepersonaliseerde phishing-berichten.