Week 01-2026

Strategisch Dreigingsrapport: Analyse Eindejaar 2025

1.0 Inleiding: Het Dreigingslandschap in Transitie

Het cyberdreigingslandschap van 2025 wordt gekenmerkt door een fundamentele transitie. De voorheen duidelijke scheidslijnen tussen digitale en fysieke dreigingen, en tussen financieel gemotiveerde cybercrime en statelijke operaties, vervagen in een alarmerend tempo. De geopolitieke situatie bevindt zich in een grijs gebied tussen vrede en oorlog, wat leidt tot een structurele onzekerheid. Deze convergentie, waarbij criminele netwerken verweven raken met geopolitieke belangen en digitale aanvallen concrete fysieke gevolgen hebben, creëert een complex risicoprofiel. Dit vraagt om een herziening van het strategisch risicobeheer, waarbij niet langer kan worden volstaan met uitsluitend technische beveiliging. Deze analyse duidt de meest significante geopolitieke dreigingen die deze nieuwe realiteit vormgeven.

2.0 Analyse van Statelijke en Geopolitieke Dreigingen

Statelijke cyberoperaties zijn een integraal onderdeel geworden van modern buitenlands beleid, waarbij nationale belangen worden geprojecteerd via digitale middelen. De methoden variëren van geavanceerde spionage en voorbereidingshandelingen voor sabotage tot grootschalige hybride oorlogsvoering. Deze operaties zijn veelal gericht op het destabiliseren van de Europese veiligheidsarchitectuur, het beïnvloeden van de publieke opinie en het ondermijnen van de westerse economische en politieke stabiliteit.

2.1 Hybride Druk en Sabotage door de Russische Federatie

De Russische strategie blijft gericht op het ondermijnen van de westerse stabiliteit, los van de ontwikkelingen op het fysieke front. Voor Nederland en België manifesteert deze dreiging zich via een combinatie van digitale operaties en het exploiteren van strategische kwetsbaarheden.

- **Hybride Strategieën:** Naast digitale aanvallen worden politieke druk, desinformatie en de exploitatie van economische afhankelijkheden ingezet. De aanhoudende import van Russisch vloeibaar aardgas (LNG) via de terminal in Zeebrugge, die in 2025

recordhoogtes bereikte, creëert een potentieel drukmiddel om het nationale beleid te beïnvloeden.
- **Spionage en Sabotage:** Inlichtingendiensten, waaronder de MIVD, constateren dat **Rusland** actief voorbereidingshandelingen treft voor de sabotage van vitale processen. Deze operaties richten zich op kritieke infrastructuur zoals energievoorzieningen en de onderzeese communicatieverbindingen in de Noordzee.
- **Inschakelen van Fysieke Actoren:** De grens tussen de digitale en fysieke wereld vervaagt verder door het inschakelen van lokale actoren voor spionageactiviteiten. De vervolging van een 17-jarige havo-scholier die werd ingeschakeld voor fysiek "veldwerk" door pro-Russische hackers, illustreert hoe kwetsbare individuen worden gerekruteerd voor operaties op de grond.

2.2 Geavanceerde Spionageoperaties vanuit China

Actoren gelinkt aan **China** onderscheiden zich door de inzet van technisch geavanceerde malware, ontworpen om diep in systemen te penetreren en detectie langdurig te ontwijken. Deze operaties richten zich veelal op spionage bij overheidsinstanties en technologische sectoren.

- **Mustang Panda (HoneyMyte):** Deze groep verspreidt de ToneShell-backdoor met behulp van een geavanceerde kernel-mode rootkit. Deze rootkit saboteert de beveiliging van het doelsysteem door de `WdFilter`-driver, een cruciaal onderdeel van Microsoft Defender, te manipuleren. Hierdoor wordt de antivirussoftware feitelijk uitgeschakeld, waardoor de malware onzichtbaar kan opereren.
- **Silver Fox (Void Arachne):** Deze actor distribueert de modulaire ValleyRAT-trojan via een combinatie van SEO-poisoning en gerichte phishing. Door de installatiebestanden van legitieme en populaire software, zoals Microsoft Teams en Telegram, te imiteren, worden slachtoffers verleid om de malware zelf te installeren.

2.3 Gerichte Inlichtingenoperaties vanuit Iran

De operaties vanuit **Iran** kenmerken zich door gerichte aanvallen op hooggeplaatste politieke en militaire doelwitten. Deze campagnes zijn niet alleen gericht op het verzamelen van inlichtingen, maar ook op het uitoefenen van psychologische druk via informatieoperaties.

- **Handala Groep:** Deze actor claimde een succesvolle inbraak op de smartphone van de stafchef van de Israëlische premier. Als bewijs werden documenten, contactlijsten en persoonlijke communicatie gepubliceerd, wat de operatie het karakter van een gerichte psychologische aanval geeft.
- **APT42 (Charming Kitten):** Via een spear-phishing-campagne op WhatsApp richtte deze groep zich op experts binnen de defensie- en veiligheidssector. De

aanvalsinfrastructuur, die onder andere gebruikmaakte van servers die in Nederland en Duitsland waren gehost, lokte doelwitten naar vervalste registratiepagina's voor conferenties om hun gegevens te bemachtigen.

Terwijl statelijke actoren de geopolitieke arena domineren, opereren cybercriminele groeperingen met een vergelijkbare strategische impact, waarbij de grens tussen staatsbelang en financieel gewin steeds vaker vervaagt.

3.0 Dominante Cybercriminele Campagnes en Actoren

De moderne cybercriminaliteit heeft zich ontwikkeld tot een professionele en georganiseerde industrie. Deze actoren opereren met een bedrijfsmatige precisie, waarbij ze geavanceerde technieken en gestructureerde businessmodellen inzetten om financiële winst en operationele verstoring te maximaliseren. Van ransomware-as-a-service tot de verkoop van gecompromitteerde toegang, het criminele ecosysteem wordt steeds toegankelijker en efficiënter.

3.1 Ransomware: Een Aanhoudende Bedreiging voor de Bedrijfscontinuïteit

Ransomware blijft een van de meest disruptieve dreigingen voor organisaties in alle sectoren. De tactiek van 'double extortion' – waarbij data niet alleen worden versleuteld maar ook gestolen en met publicatie wordt gedreigd – verhoogt de druk op slachtoffers aanzienlijk. Prominente groeperingen hanteren publieke slachtofferlijsten en opereren vaak via een affiliate-model, waarbij de technische drempel voor aanvallers wordt verlaagd.

Ransomware Groep	Getroffen Organisaties (Sector)	Kenmerkende Werkwijze
Lockbit5	RD Metals (Metaalrecycling), Fresh2You (AGF-sector), JEF (Non-profit)	Publiceert slachtoffers op een publieke lijst en dreigt met datalekken om betaling af te dwingen.
Safepay	Van Venrooy (Productie utiliteitsvoertuigen)	Hanteert de 'double extortion'-methode, waarbij systemen worden versleuteld en data worden ontvreemd.
Gentlemen	Complexul Energetic Oltenia (Energiesector)	Dringt binnen via gecompromitteerde inloggegevens en versleutelt bestanden met specifieke extensies.

Nova	Clinical Diagnostics (Medische sector)	Voert datadiefstal uit bij organisaties die gevoelige medische en persoonsgegevens verwerken.
BlackCat/ALPHV	Amerikaanse bedrijven (Farmacie, Medische apparatuur)	Maakt gebruik van een affiliate-model, waarbij in recente gevallen zelfs cybersecurity-experts werden ingezet om aanvallen op Amerikaanse organisaties uit te voeren.

3.2 Phishing en Social Engineering: De Toenemende Geraffineerdheid

Phishing- en social engineering-technieken evolueren continu, waarbij aanvallers steeds geraffineerdere methoden gebruiken om traditionele beveiligingsfilters en het menselijk oordeel te omzeilen.

1. **Misbruik van Legitieme Infrastructuur:** Aanvallers maken steeds vaker gebruik van de infrastructuur van vertrouwde organisaties om de geloofwaardigheid van hun aanvallen te vergroten en detectie te bemoeilijken.
    - *Google Cloud:* Een omvangrijke campagne maakte misbruik van Google Cloud Application Integration om phishing-mails te verzenden vanaf een legitiem `google.com`-adres, waardoor de berichten moeiteloos door spamfilters kwamen.
    - *Grubhub:* Een legitiem subdomein van maaltijdbezorger Grubhub, normaal gebruikt voor partnercommunicatie, werd gekaapt voor een grootschalige crypto-phishingcampagne.
2. **Gespecialiseerde Crypto-Phishing:** De focus op de cryptosector is in 2025 met 83,4% toegenomen. Criminelen zetten specifieke technieken in zoals `approval phishing` (het verkrijgen van onbeperkte toegang tot tokens), `transactie-phishing` (het misleiden tot het ondertekenen van kwaadaardige smart contracts) en `address poisoning` (het gebruik van sterk gelijkende wallet-adressen om transacties te onderscheppen).
3. **Smishing en Vishing:** De aanvallen verplaatsen zich ook naar andere communicatiekanalen. Er werd een actieve smishing-campagne (phishing via sms) waargenomen namens MijnOverheid. Tegelijkertijd illustreert de aanhouding van een 17-jarige verdachte in Capelle, die zich via de telefoon (vishing) voordeed als rechercheur, de aanhoudende dreiging van directe sociale manipulatie.

3.3 Supply Chain Compromittering: Het Aanvallen van de Vertrouwensketen

Supply chain-aanvallen hebben een hoge strategische waarde voor criminelen, omdat het compromitteren van één softwareleverancier of code-repository een exponentieel groot aantal slachtoffers kan maken. Door de vertrouwensketen aan te vallen, omzeilen kwaadwillenden de directe verdedigingslinies van hun einddoelwitten.

- **Gecompromitteerde Software-updates:** Een gemanipuleerde update van de **Trust Wallet**-browserextensie, verspreid via de officiële Chrome Web Store, leidde tot de diefstal van $7 miljoen aan cryptovaluta. Op vergelijkbare wijze werd een met infostealer-malware besmette versie van de teksteditor **EmEditor** verspreid via de officiële website van de ontwikkelaar.
- **Infiltratie van Code-repositories: Maven Central**, een cruciale opslagplaats voor Java-ontwikkelaars, werd geïnfiltreerd met een kwaadaardige bibliotheek. De aanval toonde een zorgvuldige planning: acht dagen voor publicatie werd het typosquatted domein `fasterxml.org` geregistreerd. De malware, gepubliceerd als een extensie van de `Jackson`-bibliotheek, gebruikte geavanceerde obfuscatietechnieken zoals prompt-injection-achtige commentaren en Unicode-tekens om analyse te ontwijken. In Spring Boot-omgevingen werd de code uitgevoerd via de klasse `JacksonSpringAutoConfiguration`, waarna op Unix-systemen **Cobalt Strike-beacons** als uiteindelijke payload werden geïnstalleerd.

Deze geavanceerde aanvallen worden mogelijk gemaakt door de exploitatie van onderliggende technologische kwetsbaarheden in software en infrastructuur.

4.0 Technologische Kwetsbaarheden met Hoge Impact

Proactief kwetsbaarhedenbeheer is een hoeksteen van een effectieve cyberverdediging. Een enkele kritieke kwetsbaarheid in wijdverspreide software of infrastructuur kan leiden tot grootschalige compromitteringen met aanzienlijke operationele en financiële risico's. De volgende kwetsbaarheden hebben in de recente periode een hoge impact gehad.

4.1 Database- en Infrastructuurkwetsbaarheden

Kwetsbaarheden in de kerncomponenten van de IT-infrastructuur, zoals databases en web-frameworks, vormen een direct risico omdat zij de fundamenten van vele applicaties en diensten raken.

- **MongoBleed (CVE-2025-14847):** Deze kritieke kwetsbaarheid in MongoDB stelt een ongeauthenticeerde aanvaller in staat om op afstand het werkgeheugen van de server uit te lezen. Dit kan leiden tot de diefstal van gevoelige data zoals sessietokens, wachtwoorden en persoonsgegevens. Met een geschat aantal van circa 3.400

kwetsbare servers in de Benelux is de potentiële impact aanzienlijk. De kwetsbaarheid wordt direct in verband gebracht met de recente, grootschalige inbreuk bij game-uitgever Ubisoft.

- **Next.js (Operatie PCPcat):** Een aanvalscampagne die misbruik maakte van twee kritieke kwetsbaarheden (CVE-2025-29927 en CVE-2025-66478) in het populaire Next.js-framework. In minder dan 48 uur werden meer dan 59.000 servers gecompromitteerd voor de extractie van gevoelige data, waaronder SSH-sleutels en cloud-configuraties.

4.2 Kwetsbaarheden in Software en Applicaties

Specifieke softwarepakketten en frameworks introduceren risico's die, indien niet tijdig verholpen, wijdverbreid misbruik mogelijk maken. De situatie wordt verergerd wanneer fabrikanten niet reageren op meldingen, waardoor organisaties kwetsbaar blijven.

- **LangChain Core (CVE-2025-68664):** Dit AI-framework bevatte een kritieke kwetsbaarheid (CVSS 9.3) die voortkomt uit een serialisatie-injectiefout. Deze fout kan via *prompt injection* worden misbruikt om geheime sleutels en omgevingsvariabelen te stelen.
- **SmarterMail (CVE-2025-52691):** Deze mailserversoftware was kwetsbaar voor een lek met de maximale risicoscore (CVSS 10.0), waardoor een ongeauthenticeerde aanvaller op afstand willekeurige code kon uitvoeren (RCE) op de server.
- **SXZOS Firmware (CVE-2025-54322):** Een kritiek zero-day lek (CVSS 9.8) in de firmware van circa 70.000 edge-apparaten, waaronder SD-WAN-appliances en routers. De fabrikant, XSpeeder, heeft na zeven maanden nog niet gereageerd op de melding, waardoor er geen officiële patch beschikbaar is.

Naast de exploitatie van bestaande kwetsbaarheden, geven opkomende trends een indicatie van hoe het dreigingslandschap zich in de nabije toekomst zal ontwikkelen.

5.0 Opkomende Trends en de Evolutie van het Dreigingslandschap

Het cyberdreigingslandschap is uiterst dynamisch. Strategische planning vereist dat organisaties verder kijken dan de incidenten van vandaag en zich voorbereiden op de methoden, technologieën en ecosystemen van morgen. De opkomst van kunstmatige intelligentie, de verdere professionalisering van criminele netwerken en de aanhoudende exploitatie van de menselijke factor zijn de belangrijkste trends die de komende periode zullen domineren.

5.1 De Impact van Kunstmatige Intelligentie (AI)

Kunstmatige intelligentie speelt een tweeledige rol in het dreigingslandschap: het is zowel een krachtig instrument voor aanvallers als een nieuwe, kwetsbare infrastructuur die beschermd moet worden.

- **Offensieve AI:** AI wordt op industriële schaal ingezet om aanvallen te automatiseren en te verfijnen. Voorbeelden zijn de AI-hacking-aanval op het socialemediaplatform Kuaishou, waarbij contentfilters systematisch werden omzeild, en de ontwikkeling van AI-gestuurde phishingkits. Deze trend manifesteert zich reeds in de praktijk, zoals geïllustreerd door de in sectie 3.2 geanalyseerde AI-gestuurde phishingkits die met minimale menselijke inspanning zeer overtuigende aanvallen genereren.
- **Nieuwe Aanvalsvectoren:** Traditionele beveiligingskaders zoals NIST en ISO schieten tekort in het afdekken van AI-specifieke dreigingen. Aanvallen zoals *prompt-injectie* (het manipuleren van AI-modellen via taal) en aanvallen op de AI-toeleveringsketen (het compromitteren van trainingsdata of modellen) vallen buiten de scope van conventionele controles.
- **Onbedoelde Datalekken:** Een significant en groeiend risico is het onbewust lekken van data door werknemers. Het incident bij de gemeente Eindhoven, waar duizenden bestanden met gevoelige persoons- en gezondheidsgegevens werden geüpload naar publieke AI-chatbots, illustreert de noodzaak voor strikt intern beleid en bewustwording.

5.2 Professionalisering van Criminele Ecosystemen

De infrastructuur van de georganiseerde misdaad verplaatst zich en wordt steeds professioneler, met een focus op laagdrempelige 'Crime-as-a-Service'-modellen.

- **Verschuiving naar Telegram:** Het zwaartepunt van grootschalige cyberfraude verschuift van het traditionele dark web naar toegankelijke platformen zoals Telegram. Met name Chinese taalgroepen hebben hier een illegaal ecosysteem gecreëerd dat in handelsvolume de historische dark web-markten overtreft. Deze groepen faciliteren fraude door diensten aan te bieden als witwasconstructies, valse identiteitsgegevens en geavanceerde AI-tools voor stem- en beeldmanipulatie.
- **Handel in Toegangsgegevens:** De handel in gecompromitteerde toegangsdata is verder geprofessionaliseerd. Op illegale marktplaatsen worden specifieke datasets aangeboden die directe toegang verschaffen tot waardevolle systemen, zoals privésleutels van crypto-wallets, inloggegevens voor 275.000 WordPress-accounts en GitHub API-sleutels met beheerdersrechten voor grote e-commerceplatformen.

5.3 De Menselijke Factor: Van Corruptie tot Social Engineering

Ondanks de technologische vooruitgang blijft de menselijke schakel een centraal doelwit voor criminelen, zowel door externe manipulatie als door interne compromittering.

1. **Corruptie op Hoog Niveau:** De verwevenheid van georganiseerde misdaad met staatsstructuren ondermijnt de rechtshandhaving. De arrestatie van de voormalige chef van de Georgische Staatsveiligheidsdienst, die illegale callcenters beschermde in ruil voor steekpenningen, is een schrijnend voorbeeld van hoe corruptie grootschalige fraude mogelijk maakt.
2. **Insider Threats en Expertise Misbruik:** Het risico komt niet altijd van buitenaf. De zaak van twee cybersecurity-experts die hun kennis misbruikten om als BlackCat-ransomware-affiliates te opereren, toont het gevaar van kwaadwillende insiders. Ook het datalek bij e-commercegigant Coupang, veroorzaakt door een ex-medewerker die zijn toegang behield, benadrukt de noodzaak van strikte offboarding-protocollen.
3. **Exploitatie van de Digitale Identiteit:** Het mobiele telefoonnummer is de centrale spil van de digitale identiteit geworden. Via *sim-swapping* proberen criminelen de controle over dit nummer over te nemen door telecomproviders te misleiden. Een succesvolle aanval geeft hen direct toegang tot verificatiecodes voor banken, sociale media en overheidsdiensten.

Deze trends en incidenten leiden tot een aantal onvermijdelijke strategische conclusies voor effectief risicobeheer.

6.0 Strategische Conclusies en Implicaties voor Risicobeheer

De analyse van het dreigingslandschap eind 2025 toont een complexe en geconvergeerde realiteit. De vervagende grenzen tussen statelijke actoren en cybercriminelen, de opkomst van AI als aanvalswapen en de aanhoudende professionalisering van de ondergrondse economie vereisen een holistische en adaptieve beveiligingsstrategie. Organisaties kunnen niet langer volstaan met traditionele technische maatregelen, maar moeten hun risicobeheer verbreden naar de strategische, menselijke en procesmatige dimensies.

1. **Integreer de Verdediging tegen Gelaagde Dreigingen** De silo's tussen fysieke beveiliging, cybersecurity en fraudepreventie moeten worden doorbroken. Aanvallers combineren steeds vaker verschillende tactieken, zoals het gebruik van DDoS-aanvallen als afleidingsmanoeuvre voor datadiefstal op de achtergrond. Een geïntegreerde aanpak, waarbij monitoring van beschikbaarheid wordt gekoppeld aan de controle op dataintegriteit en verdacht intern verkeer, is essentieel om deze gelaagde aanvallen te detecteren.

2. **Beheers de Risico's van de AI-Revolutie met Nieuw Beleid** Organisaties moeten met urgentie duidelijke richtlijnen opstellen voor het gebruik van (generatieve) AI-tools door werknemers. Het risico op onbedoelde datalekken, zoals het uploaden van gevoelige bedrijfsinformatie naar publieke chatbots, is te groot om te negeren. Tegelijkertijd vereist de bescherming van de eigen AI-infrastructuur de implementatie van AI-specifieke beveiligingscontroles die verder gaan dan traditionele frameworks en bescherming bieden tegen dreigingen als prompt-injectie en aanvallen op de AI-toeleveringsketen.
3. **Maak Ketenverantwoordelijkheid een Niet-Onderhandelbare Prioriteit** Het risico van de software supply chain is een directe bedreiging voor de eigen bedrijfscontinuïteit. Incidenten zoals de infiltratie van code-repositories en de verspreiding van malware via legitieme software-updates tonen aan dat de beveiliging van externe leveranciers en open-source componenten een directe verantwoordelijkheid is geworden. Juridische druk, onder meer vanuit regelgeving zoals de NIS2-richtlijn, versterkt deze noodzaak en dwingt organisaties tot een striktere governance en aantoonbare controle over hun volledige digitale keten.
4. **Versterk de Menselijke Verdedigingslinie als Kerncomponent** Ondanks de toenemende technologische complexiteit van aanvallen, blijven social engineering en de exploitatie van de menselijke factor centraal staan. Phishing, insider threats en sociale manipulatie zijn verantwoordelijk voor een groot deel van de succesvolle inbraken. Dit pleit voor een structurele investering in de menselijke verdedigingslinie. Continue training, strikte identiteits- en toegangsbeheerprotocollen (IAM) en het bevorderen van een sterke, organisatiebrede beveiligingscultuur zijn onmisbaar om de weerbaarheid effectief te verhogen.