Week 46-2025

Strategisch Dreigingsrapport: Analyse van het Cyberlandschap, November 2025

Inleiding: Het Digitale Slagveld in Versnelling

Dit rapport biedt een strategische analyse van het cyberdreigingslandschap van november 2025. Dit landschap wordt niet langer primair gedefinieerd door financieel gemotiveerde misdaad, maar door een complexe versmelting van geopolitieke conflicten, de versnelde adoptie van kunstmatige intelligentie (AI) in aanvalstechnieken en systemische kwetsbaarheden in onze kritieke infrastructuren. De digitale en fysieke wereld zijn onlosmakelijk met elkaar verbonden, en een verstoring in het ene domein heeft directe, voelbare gevolgen voor het andere. Dit rapport analyseert de belangrijkste dreigingsvectoren van dit moment om het management en de beveiligingsteams te voorzien van strategisch inzicht voor effectief risicobeheer. De volgende hoofdstukken behandelen de belangrijkste domeinen van deze nieuwe realiteit, van staatsgesponsorde operaties tot de kwetsbaarheid van onze digitale toeleveringsketens.

---

1. De Geopolitieke Arena: Staatsgesponsorde Cyberoperaties als Machtsinstrument

Het monitoren van staatsgesponsorde cyberactiviteiten is essentieel voor een strategische risicobeoordeling. Deze operaties zijn niet langer uitsluitend gericht op traditionele spionage, maar worden steeds vaker ingezet als instrument voor destabilisatie, economische disruptie en het uitoefenen van directe politieke invloed. De digitale ruimte is een volwaardig geopolitiek strijdtoneel geworden, waar natiestaten hun capaciteiten inzetten om strategische voordelen te behalen en de belangen van tegenstanders te ondermijnen.

1.1. Analyse van Chinese Spionage en Offensieve Capaciteiten

Een recent datalek bij de Chinese cybersecurityfirma Knownsec heeft een zeldzaam inzicht gegeven in de omvang en professionaliteit van China's staatsgesponsorde cyberoperaties. De strategische implicaties van deze onthullingen zijn significant en verhogen het risicoprofiel voor westerse organisaties.

- **Onthulde Capaciteiten:** Uit de meer dan 12.000 gelekte documenten kwam het bestaan van geavanceerde, staatsgesponsorde cyberwapens en een arsenaal aan interne hackingtools aan het licht. Dit bevestigt de hoge mate van technische verfijning en de nauwe samenwerking tussen de firma en diverse Chinese overheidsinstanties.
- **Mondiale Doelwitten:** Het lek onthulde een lijst van 80 reeds gecompromitteerde buitenlandse doelwitten. Concrete voorbeelden omvatten de diefstal van Indiase immigratiedossiers, telefoongesprekken van de Zuid-Koreaanse telecomprovider LG U Plus en planningsinformatie uit Taiwan.
- **Strategische Conclusie:** Deze onthullingen tonen aan dat Chinese cyberoperaties niet alleen gericht zijn op spionage, maar ook op het verzamelen van data die ingezet kunnen worden voor politieke en economische druk. Voor westerse organisaties en overheden betekent dit een verhoogd risico op diepgaande en langdurige compromitteringen die verder gaan dan directe financiële schade.

1.2. Evaluatie van Russische Hybride Oorlogsvoering in Europa

Rusland en aan Rusland gelieerde groeperingen blijven een actieve en verstorende rol spelen in Europa door middel van een hybride aanpak, waarbij digitale aanvallen worden gecombineerd met sabotage en desinformatie. Recente incidenten in België illustreren deze tactieken. Uit een rapport van Microsoft blijkt dat maar liefst 5% van alle wereldwijde cyberaanvallen die aan Rusland worden toegeschreven, gericht was op België. Dit omvatte een golf van DDoS-aanvallen op vitale infrastructuur, waaronder telecomprovider Proximus en het UZ Gent, met als doel de economie te verstoren en politieke boodschappen over te brengen.

Een zorgwekkende ontwikkeling is de inzet van zogenaamde 'disposable agents'. Via tussenpersonen en criminele netwerken op platforms als Telegram rekruteert Rusland kleine criminelen voor specifieke sabotageacties, zoals de recente drone-incidenten in België. Deze agenten zijn zich vaak niet bewust van de uiteindelijke opdrachtgever. Het doel is niet alleen spionage, maar ook het zaaien van angst en het beïnvloeden van de politieke besluitvorming in Europa. Parallel hieraan blijft politieke inmenging een prioriteit, zoals blijkt uit de maatregelen die de EU treft tegen Russische desinformatie en de pogingen tot beïnvloeding van verkiezingen, waaronder de presidentsverkiezingen in Roemenië die werden geannuleerd vanwege Russische inmenging.

1.3. De Opkomst van Hacktivistische Allianties

De dreiging van politiek gemotiveerde hacktivistische groepen neemt toe in schaal en coördinatie. Collectieven zoals HEZI RASH en NoName hebben recentelijk diverse DDoS-campagnes uitgevoerd tegen Belgische en andere Europese infrastructuren. Doelwitten in België waren onder meer waterbedrijven, energieleverancier ENGIE Electrabel, de Brusselse

vervoersmaatschappij STIB-MIVB en de website van de stad Antwerpen. Deze aanvallen, gericht op het verstoren van openbare diensten, onderstrepen de kwetsbaarheid van onze digitale samenleving. De dreiging wordt verder versterkt door de vorming van nieuwe allianties; de recente aankondiging van een samenwerking tussen NoName en PalachPro vergroot de capaciteit voor gecoördineerde, politiek gemotiveerde digitale verstoringen aanzienlijk.

Naast deze staatstactieken en allianties verandert ook de technologie zelf, met name AI, de aard van de dreiging fundamenteel.

---

2. De Opkomst van AI in Cyberaanvallen: Een Nieuw Paradigma van Dreiging

Kunstmatige intelligentie heeft de dynamiek van cybersecurity fundamenteel veranderd. AI is niet louter een nieuw instrument, maar een 'force multiplier' die zowel aanvallers als verdedigers ongekende mogelijkheden biedt. Voor aanvallers automatiseert en versnelt het de aanvalscyclus, terwijl het voor verdedigers nieuwe, complexe kwetsbaarheden introduceert in de AI-systemen zelf. Deze verschuiving vereist een herziening van traditionele beveiligingsstrategieën.

2.1. Offensief Gebruik van AI: Automatisering en Personalisatie

Aanvallers zetten AI in om de effectiviteit, snelheid en schaal van hun operaties drastisch te verhogen, wat leidt tot een strategisch nadeel voor verdedigende partijen.

1. **Versnelde Exploitatie:** Recente industriële rapporten tonen aan dat 50% tot 61% van de nieuw ontdekte kwetsbaarheden binnen 48 uur wordt misbruikt door aanvallers. Zij gebruiken AI en geautomatiseerde scripts om razendsnel exploitcode te ontwikkelen en te verspreiden. Dit creëert een gevaarlijke "gap" tussen de snelheid van geautomatiseerde aanvallen en de reactietijd van beveiligingsteams die vaak afhankelijk zijn van handmatige patchcycli.
2. **Gepersonaliseerde Social Engineering:** AI wordt ingezet om phishingmails te verbeteren, waardoor ze overtuigender en moeilijker te onderscheiden zijn van legitieme communicatie. Dit verhoogt de effectiviteit van social engineering-aanvallen aanzienlijk.
3. **AI-Gegenereerde Malware:** Het afgelopen jaar is er een stijging van 156% waargenomen in AI-gedreven supply chain-aanvallen. AI-gegenereerde malware is vaak polymorfisch (constant van vorm veranderend) en contextbewust, waardoor het traditionele, op handtekeningen gebaseerde detectiemethoden effectief kan omzeilen.

2.2. De Kwetsbaarheid van AI-Systemen Zelf

De toenemende implementatie van AI-technologie creëert tegelijkertijd een volledig nieuw aanvalsoppervlak. De systemen die bedoeld zijn om ons te helpen, worden zelf een doelwit met unieke kwetsbaarheden.

- **Afluisteren van AI-Gesprekken:** De 'Whisper Leak' zij-kanaalaanval, waarover Microsoft details publiceerde, toont aan dat het mogelijk is om onderwerpen uit versleutelde AI-chats af te leiden met een nauwkeurigheid van 98%. Door patronen in de pakketgrootte van het netwerkverkeer te analyseren, kunnen aanvallers bepalen of een gesprek over gevoelige onderwerpen gaat, zelfs zonder de inhoud te ontsleutelen.
- **Manipulatie van AI-Modellen:** Een recent ontdekte kwetsbaarheid in OpenAI's videomodel Sora 2 maakt het mogelijk om verborgen systeeminstellingen te extraheren via audiotranscripties. Dit type aanval, bekend als 'prompt leaking', legt de interne werking van AI-modellen bloot en kan worden misbruikt voor het genereren van ongewenste content.
- **Fundamentele Kwetsbaarheden:** Het 'ShadowMQ'-probleem heeft een reeks kritieke kwetsbaarheden blootgelegd in de AI-inferentie-engines van grote technologiebedrijven als Meta, Nvidia en Microsoft. Onveilige implementaties van communicatiebibliotheken (ZeroMQ) en deserialisatiemethoden (Python's pickle) maakten remote code execution (RCE) mogelijk, wat aanvallers volledige controle over de AI-systemen kon geven.

Deze geavanceerde, AI-gedreven aanvallen en de inherente kwetsbaarheden van AI-systemen vormen een verhoogd risico voor de meest cruciale digitale en fysieke systemen van onze samenleving.

---

3. Kwetsbaarheid van Kritieke Infrastructuren en Digitale Toeleveringsketens

De strategische afhankelijkheid van organisaties van zowel fysieke vitale infrastructuur als de digitale toeleveringsketen is groter dan ooit. De grens tussen deze twee domeinen vervaagt in toenemende mate; een verstoring in de digitale wereld heeft direct catastrofale gevolgen voor de fysieke wereld, en vice versa. Recente incidenten tonen aan dat zowel directe aanvallen als systemische kwetsbaarheden een acuut risico vormen voor de operationele continuïteit.

3.1. Directe Aanvallen op Vitale Sectoren

De kwetsbaarheid van vitale sectoren wordt pijnlijk duidelijk door een reeks recente, impactvolle cyberaanvallen.

Sector/Doelwit	Analyse van de Impact
Transport & Logistiek	Havens worden geconfronteerd met een gecombineerde dreiging van fysieke (drones) en digitale (cyberaanvallen) sabotage. Als reactie hierop heeft North Sea Port Gent een nieuw strategisch beveiligingsplan geïntroduceerd dat zich richt op het versterken van de weerbaarheid tegen beide dreigingsvectoren.
Productie-industrie	De cyberaanval op Jaguar Land Rover veroorzaakte een productiestop van vijf weken. Dit leidde niet alleen tot directe schade voor het bedrijf, maar had ook een kettingreactie in de toeleveringsketen, met een geschat economisch verlies van €2,2 miljard.
Telecommunicatie	Een mogelijk datalek bij Eurofiber, een sleutelspeler in de nationale digitale infrastructuur, benadrukt het systemische risico. Een dergelijke inbreuk kan de continuïteit van netwerkdiensten voor talloze organisaties in gevaar brengen.
Regionale Media	De ransomware-aanval op RTV Noord illustreert hoe een willekeurige 'spray-aanval' de operationele continuïteit van essentiële regionale diensten kan verstoren, zelfs als de organisatie geen specifiek doelwit was.

3.2. Systemische Risico's door Wijdverbreide Softwarekwetsbaarheden

De ruggengraat van de moderne IT-infrastructuur wordt gevormd door een beperkt aantal softwareproducten en -technologieën. Een kwetsbaarheid in een van deze wijdverbreide componenten creëert een systemisch risico voor duizenden organisaties tegelijk.

- **Netwerkbeveiliging (Firewalls):** Er worden actief misbruikte, kritieke kwetsbaarheden gerapporteerd in WatchGuard Firebox en Cisco Secure Firewall, die aanvallers in staat stellen om kwaadaardige code uit te voeren. Daarnaast zorgt een DoS-kwetsbaarheid in Palo Alto PAN-OS ervoor dat aanvallers firewalls op afstand kunnen herstarten.
- **Cloud & Containertechnologie:** Kritieke kwetsbaarheden in `runC`, de container-runtime die de basis vormt voor Docker en Kubernetes, maken 'container escapes' mogelijk. Dit stelt een aanvaller in staat om uit een geïsoleerde container te breken en toegang te krijgen tot het onderliggende host-besturingssysteem.
- **Bedrijfssoftware:** Essentiële bedrijfsapplicaties blijven een primair doelwit. Recente kritieke kwetsbaarheden zijn gemeld in SAP en Remote Monitoring and Management (RMM) software zoals N-able N-Central. Een kwetsbaarheid in Oracle E-Business Suite werd misbruikt in een campagne die meer dan honderd organisaties trof, waaronder de Amerikaanse krant The Washington Post.

- **Authenticatie-infrastructuur:** Active Directory (AD) blijft een topdoelwit voor aanvallers. Een recent ontdekte "authentication coercion"-aanval op Windows-systemen toont aan hoe aanvallers legitieme protocollen kunnen misbruiken om inloggegevens te bemachtigen zonder dat dit door traditionele beveiligingssystemen wordt opgemerkt.

3.3. De Gecompromitteerde Digitale Toeleveringsketen

De afhankelijkheid van externe softwarebibliotheken en ontwikkeltools creëert een kwetsbare toeleveringsketen. Een compromittering in één component kan zich als een virus verspreiden naar alle applicaties die ervan afhankelijk zijn.

- De toevoeging van **'Software Supply Chain Failures' aan de OWASP Top 10 van 2025** is een duidelijke indicator van het strategische belang en de toenemende risico's in dit domein.
- Concrete voorbeelden illustreren de dreiging: de **GlassWorm-malware** die zich verspreidt via malafide VSCode-extensies, een kritieke kwetsbaarheid in de populaire `expr-eval` JavaScript-bibliotheek met meer dan 800.000 wekelijkse downloads, en een grootschalige spamcampagne die de **npm-registry overspoelde met meer dan 67.000 neppakketten**.

Naast deze systemische en staatgesponsorde dreigingen, evolueert ook de meer 'traditionele' cybercriminaliteit in schaal en professionaliteit.

---

4. Evolutie van Cybercriminaliteit: Professionalisering en Diversificatie

Naast de geopolitieke en technologische verschuivingen wordt de cybercriminele economie steeds volwassener en professioneler. We zien duidelijke trends van specialisatie, zoals Ransomware-as-a-Service (RaaS) en Initial Access Brokers (IAB), een diversificatie van aanvalsvectoren en een continu stijgende financiële impact. Deze professionaliseringsslag maakt geavanceerde aanvalsmethoden toegankelijk voor een bredere groep criminelen.

4.1. Het Ransomware Ecosysteem: Fragmentatie en Nieuwe Tactieken

De ransomware-dreiging blijft onverminderd groot, maar het landschap verandert continu. Het is niet langer een markt die wordt gedomineerd door enkele grote spelers.

- **Marktontwikkeling:** De markt is sterk gefragmenteerd met momenteel **85 actieve groepen**. De Qilin-groep is uitgegroeid tot de meest actieve speler, waarbij de productiesector en zakelijke diensten de zwaarst getroffen sectoren zijn.
- **Operationele Modellen:** Het **Ransomware-as-a-Service (RaaS)** model maakt geavanceerde ransomware toegankelijk voor criminelen zonder diepgaande technische kennis. De recent ontdekte VanHelsing ransomware is hier een goed voorbeeld van; deze RaaS-kit ondersteunt aanvallen op meerdere besturingssystemen, waaronder Windows, Linux en VMWare ESXi, wat de schaalbaarheid van operaties enorm vergroot.
- **Concrete Incidenten:** Grote, multinationale organisaties blijven een primair doelwit. De recente aanval van de **Everest-groep op de Belgische multinational AGFA** is een actueel voorbeeld van de aanhoudende dreiging voor het bedrijfsleven.

4.2. De Schaal van Phishing en Informatiediefstal

Phishing- en infostealer-campagnes worden steeds verfijnder en opereren op een schaal die voorheen ondenkbaar was. Aanvallers misbruiken legitieme infrastructuren om detectie te omzeilen en het vertrouwen van slachtoffers te winnen.

- **Gericht op Bedrijfsaccounts:** Een grootschalige phishingaanval richtte zich via twee verschillende vectoren op gebruikers van Meta's zakelijke tools. Eén vector misbruikte de legitieme uitnodigingsfunctie van de Meta Business Suite, terwijl een andere campagne officiële `@facebookmail.com` e-mailadressen gebruikte. Beide methoden leidden slachtoffers naar overtuigende nep-inlogpagina's, waardoor de inloggegevens van duizenden bedrijven werden gestolen.
- **Grootschalige Infrastructuur:** Het recent ontdekte **'Quantum Route Redirect'** platform maakt gebruik van meer dan 1.000 domeinen om op grote schaal Microsoft 365-inloggegevens te stelen. De infrastructuur is ontworpen om beveiligingsscanners te misleiden en slachtoffers naar overtuigende nep-inlogpagina's te leiden.
- **Terugkerende Malware:** De terugkeer van de **Danabot banking trojan**, kort na de ontmanteling door de internationale handhavingsactie Operatie Endgame, toont de veerkracht van deze criminele netwerken aan. De malware is terug met een geüpdatete versie en een robuustere command-and-control-infrastructuur.

4.3. De Explosieve Groei van Financiële Fraude

De dreiging van directe financiële oplichting, met name via cryptocurrency, is in 2025 explosief gegroeid. Criminelen maken handig gebruik van sociale media en psychologische manipulatie om slachtoffers te overtuigen grote sommen geld te investeren.

- Tot begin november 2025 werd er in Nederland al **€29 miljoen** buitgemaakt door cryptofraude, een significante stijging ten opzichte van voorgaande jaren.
- De gebruikte methoden zijn divers en verfijnd, variërend van misbruik van sociale media tot de beruchte **'pig butchering'** oplichtingstruc, waarbij slachtoffers via datingsites worden benaderd en langzaam worden verleid tot het doen van frauduleuze investeringen.

Deze bevindingen tonen een dreigingslandschap dat complexer, sneller en meer geïntegreerd is dan ooit tevoren, wat een herziene strategische visie op cyberweerbaarheid noodzakelijk maakt.

---

5. Conclusie en Strategische Overwegingen

Het dreigingslandschap van november 2025 wordt gekenmerkt door fundamentele verschuivingen die een proactieve en strategische herijking van het risicobeheer vereisen. Traditionele, reactieve beveiligingsmodellen zijn niet langer toereikend om de snelheid, schaal en complexiteit van de huidige dreigingen het hoofd te bieden.

5.1. Synthese van het Dreigingslandschap

Drie strategische verschuivingen domineren het huidige dreigingslandschap en vormen de kern van de risico's voor organisaties:

1. **Digitalisering van Geopolitiek Conflict:** Cyberaanvallen zijn een integraal en alledaags instrument geworden in de internationale machtspolitiek. Dit resulteert in een toename van disruptie- en sabotageacties die niet primair financieel, maar politiek of strategisch gemotiveerd zijn en zich richten op de vitale infrastructuren van westerse landen.
2. **AI als Brandversneller:** Kunstmatige intelligentie versnelt de aanvalscyclus drastisch, van de ontdekking van kwetsbaarheden tot de exploitatie ervan. Tegelijkertijd creëert AI geheel nieuwe aanvalsvectoren door de kwetsbaarheid van de AI-modellen zelf. Dit stelt de traditionele, op detectie gebaseerde verdedigingsmechanismen zwaar op de proef.
3. **De Toeleveringsketen als Primair Slagveld:** De aanval op de digitale toeleveringsketen is geëvolueerd van een niche-risico naar een primair strijdtoneel. De integriteit van softwarebibliotheken, ontwikkeltools en IT-dienstverleners is een kritieke kwetsbaarheid geworden, waarbij een enkele zwakke schakel kan leiden tot een grootschalige, systemische compromittering.

5.2. Strategische Aanbevelingen voor Risicobeheer

Op basis van deze analyse worden de volgende strategische, niet-technische aanbevelingen gedaan om de weerbaarheid van de organisatie te verhogen:

- **Integreer Geopolitieke Risicoanalyse:** De scheiding tussen cyberdreigingen en geopolitiek is verdwenen. Het is cruciaal om de analyse van cyberdreigingsinformatie (CTI) te verrijken met geopolitieke analyses. Door internationale spanningen en de motieven van natiestaten te monitoren, kan de organisatie beter anticiperen op potentieel disruptieve aanvallen die voortkomen uit conflicten en politieke agenda's.
- **Verhoog de Focus op Weerbaarheid tegen Disruptie:** Gezien de toename van aanvallen die gericht zijn op verstoring (zoals DDoS en ransomware op vitale systemen), is preventie alleen niet meer voldoende. De strategische focus moet verschuiven van enkel het voorkomen van een inbreuk naar het waarborgen van operationele continuïteit en snel herstel. Investeer in robuuste business continuity- en disaster recovery-plannen en test deze regelmatig tegen realistische disruptiescenario's.
- **Implementeer een Robuust Supply Chain Risicobeleid:** De digitale toeleveringsketen is een integraal onderdeel van het aanvalsoppervlak geworden. Het is noodzakelijk om de beveiligingseisen voor softwareleveranciers en IT-partners significant aan te scherpen. Implementeer een actief beleid voor het beheer van afhankelijkheden in software en diensten, conform de lessen uit de OWASP Top 10. Eis transparantie van leveranciers en voer periodieke audits uit om de integriteit van de keten te waarborgen.