Week 45-2025

Strategisch Overzicht Cyberdreigingen: Weekanalyse

Inleiding

Dit strategisch overzicht biedt een beknopte analyse van de meest significante cyberincidenten, dreigingsactoren en opkomende aanvalspatronen die in de afgelopen week zijn waargenomen. De analyse is uitsluitend gebaseerd op de verstrekte brongegevens en heeft als doel om beveiligingsprofessionals en management te ondersteunen bij strategische besluitvorming. De analyse van deze week onthult een duidelijke escalatie in gecoördineerde DDoS-aanvallen tegen West-Europese vitale infrastructuur, de snelle operationalisering van AI in social engineering, en aanhoudende statelijke spionage die misbruik maakt van een alarmerend aantal ongepatchte, internetgerichte systemen. Door inzicht te bieden in de tactieken en doelwitten van aanvallers, helpt dit document bij het prioriteren van defensieve maatregelen en het verhogen van de digitale weerbaarheid.

---

1. Ransomware en Data Extortion: Analyse van Hoog-Impact Incidenten

Het risico van ransomware en data-afpersing blijft een constante en evoluerende dreiging voor organisaties van elke omvang. De tactieken van aanvallers worden steeds geraffineerder, waarbij de focus niet alleen ligt op het versleutelen van data, maar ook op het stelen en publiekelijk lekken ervan om de druk op te voeren. Het is van strategisch belang om de werkwijze van deze groepen te begrijpen, met name vanwege hun impact op vitale sectoren en de kwetsbaarheid van de gehele toeleveringsketen.

- **1.1. Analyse van de Clop-aanval op Ansell** De ransomware-aanval door de Clop-groep op Ansell, een wereldwijde producent van beschermingsoplossingen zoals beschermende handschoenen, veiligheidskleding en condooms, illustreert de kwetsbaarheid van vitale sectoren. Als cruciale leverancier voor de gezondheidszorg en de industrie, resulteerde de aanval in een wereldwijde verstoring van de bedrijfsactiviteiten. De claim van de Clop-groep impliceert de diefstal van gevoelige gegevens van medewerkers en externe partners, wat de risico’s van identiteitsdiefstal en verdere misdrijven aanzienlijk vergroot. Dit incident benadrukt hoe een aanval op één organisatie direct de operationele continuïteit binnen kritieke sectoren kan ondermijnen.

- **1.2. De Omrin-zaak: Datalek en Gevolgen voor Publieke Gegevens** Een eerdere ransomware-aanval op afvalverwerker Omrin heeft geleid tot een significant datalek met directe gevolgen voor burgers. Persoonsgegevens van inwoners van de gemeente Schiermonnikoog, waaronder namen, adressen en BSN-nummers, zijn gestolen en op het darkweb gelekt. Dit incident legt twee kritieke risico's bloot:
    1. **Toeleveringsketenrisico:** Omrin functioneerde als een schakel in de dienstverlening van de gemeente. De aanval toont aan dat de zwakste schakel in de keten de veiligheid van alle betrokkenen bepaalt.
    2. **Geactualiseerd latent risico:** De gemeente had in 2024 ten onrechte een bestand met BSN-nummers gedeeld met Omrin, wat de principes van dataminimalisatie schendt. Deze onjuiste dataverwerking creëerde een latent risico dat door de ransomware-aanval in 2025 werd geactualiseerd, met het lekken van BSN-nummers als gevolg. Dit onderstreept de noodzaak van strikte datagovernance, aangezien een cyberaanval reeds bestaande interne controlezwaktes genadeloos blootlegt.
- **1.3. Opkomst van Georganiseerde Afpersingscollectieven** De vorming van het collectief 'Scattered LAPSUS Hunters' uit de bekende groepen Scattered Spider, LAPSUS en ShinyHunters markeert een professionaliseringsslag in de cybercrime-industrie. Deze groep profileert zich met een 'extortion as a service'-model, waarbij ze hun merkbekendheid en infrastructuur (zoals Telegram-kanalen) inzetten om publieke druk uit te oefenen en betalingen af te dwingen. Hun tactieken omvatten geavanceerde social engineering, zoals spear phishing en vishing. Deze consolidatie van expertise en middelen vergroot de dreiging van geavanceerde en zeer gerichte afpersingscampagnes; een tactiek die vaak wordt vergemakkelijkt door het misbruik van de in sectie 4 besproken, niet-gepatchte kwetsbaarheden in publiek toegankelijke applicaties, die als initiële toegangspoort dienen.

---

2. Verstorende Aanvallen: DDoS-Campagnes en Destructieve Malware

Digitale beschikbaarheid is een strategische pijler voor zowel de publieke als de commerciële sector. Recente incidenten tonen aan dat dreigingsactoren Distributed Denial-of-Service (DDoS) aanvallen en destructieve data-wiping malware inzetten als primaire tactieken om dienstverlening te ontregelen en geopolitieke druk uit te oefenen. Deze aanvallen zijn niet gericht op financieel gewin, maar op het ondermijnen van het vertrouwen in digitale infrastructuren.

- **2.1. Gecoördineerde DDoS-campagnes tegen Belgische Doelwitten** De afgelopen week is België getroffen door een golf van DDoS-aanvallen, opgeëist door verschillende pro-Russische hacktivistengroepen. De doelwitselectie, die zich uitstrekt over de overheid, defensie, energie en telecom, demonstreert een gecoördineerde en

strategische campagne die ontworpen is om maximale maatschappelijke onrust te veroorzaken, in plaats van een reeks onsamenhangende opportunistische aanvallen. De aanval op de militaire inlichtingendienst ADIV werd door NoName057 expliciet gerechtvaardigd met een verwijzing naar uitspraken van de Belgische minister van Defensie over Rusland, wat de geopolitieke motivatie onderstreept.

Aanvallende Groep	Geclaimde Doelwitten	Sector
NoName / NoName057(16)	Parlement van Wallonië, citydev.brussels, VIVAQUA, Proximus, Scarlet, UZ Gent, ENGIE Electrabel, Elia Group, Haven van Antwerpen-Brugge, ADIV (militaire inlichtingendienst), diverse provincies en gemeenten (o.a. Antwerpen, Linkebeek)	Overheid, Telecom, Gezondheidszorg, Energie, Vitale Infrastructuur, Defensie
Server Killers	FPS Economy, VOO, edpnet, Banque CPH, Europabank, Haven van Zeebrugge	Overheid, Telecom, Financiën, Vitale Infrastructuur
TwoNet	Gemeentelijke websites (Beveren, Berlaar, Lochristi)	Lokale Overheid
HEZI RASH	Office national de Sécurité sociale (onss.be)	Overheid

- **2.2. Strategische Escalatie door Allianties** De dreiging van DDoS-aanvallen wordt verder versterkt door de vorming van strategische allianties. De NoName-groep kondigde samenwerkingen aan met 'Perun Swaroga' en 'Heaven of the Slavs'. Het bundelen van middelen zoals botnets, tooling en propagandakanalen vergroot de slagkracht van deze groepen significant. Dit kan leiden tot een intensivering van zowel volumetrische als geavanceerde applicatielaag-aanvallen, waardoor de digitale weerbaarheid van organisaties zwaarder op de proef wordt gesteld.
- **2.3. Inzet van Data Wipers door Statelijke Actoren** Naast verstoring van beschikbaarheid wordt ook destructieve malware ingezet voor strategische doeleinden. De Russische militaire hackergroep Sandworm gebruikte data-wiping malware tegen organisaties in de Oekraïense graansector. De strategische doelstelling is duidelijk: het permanent vernietigen van cruciale data om de oorlogseconomie van Oekraïne te verzwakken en de wereldwijde graanhandel te beïnvloeden. Dit toont hoe cyberaanvallen worden geïntegreerd in bredere geopolitieke en militaire campagnes.

Deze directe, verstorende aanvallen vormen een onmiddellijke dreiging, terwijl tegelijkertijd nieuwe tactieken en technologieën opkomen die het toekomstige dreigingslandschap zullen vormgeven.

---

3. Opkomende Dreigingsvectoren en Tactieken

Voor een effectieve defensieve strategie is het cruciaal om niet alleen te reageren op huidige aanvallen, maar ook te anticiperen op toekomstige dreigingen. Het dreigingslandschap evolueert snel, gedreven door technologische innovaties en de professionalisering van cybercriminelen. Deze sectie analyseert de meest significante opkomende tactieken, waaronder het gebruik van AI in aanvallen, geavanceerde social engineering en de groeiende kwetsbaarheid van mobiele en IoT-ecosystemen.

- **3.1. De Dubbele Rol van Kunstmatige Intelligentie (AI)** Kunstmatige intelligentie (AI) manifesteert zich als een krachtig instrument voor zowel aanvallers als verdedigers, maar brengt ook nieuwe veiligheidsrisico's met zich mee.
    1. **AI als Aanvalswapen:** Criminelen operationaliseren AI voor digitale manipulatie. Voorbeelden zijn het gebruik van deepfakes door de Noord-Koreaanse groep 'Famous Chollima' in valse sollicitatiegesprekken, de opkomst van AI-gedreven ransomware die aanvallen verfijnt, en AI-malware zoals 'PromptFlux' die zijn gedrag dynamisch aanpast om detectie te omzeilen.
    2. **AI als Social Engineering Tool:** Een opkomend concept is 'Vibe hacking', waarbij AI wordt ingezet om de toon, timing en persoonlijkheid van een aanvaller te perfectioneren. Dit maakt misleiding via tekst, stemdeepfakes en andere communicatievormen aanzienlijk overtuigender en moeilijker te herkennen.
    3. **Governance en Beveiligingsrisico's:** De snelle ontwikkeling van AI creëert zorgen over veiligheid en governance. De oprichting van een safety panel bij OpenAI om onveilige releases te stoppen, de constatering dat vrijwel alle AI-benchmarks tekortkomingen hebben, en het verbod op AI-tools zoals Copilot bij Avans Hogeschool vanwege datalekrisico's, illustreren de complexiteit van het beheersen van deze technologie.
- **3.2. Geavanceerde Social Engineering en Fraude** Aanvallers blijven investeren in de verfijning van fraude- en phishingcampagnes, waarbij ze vaak gebruikmaken van legitieme clouddiensten om vertrouwen te wekken en detectie te omzeilen.
    - De **TruffleNet BEC-campagne** misbruikt gestolen AWS-credentials om via de Amazon Simple Email Service (SES) op grote schaal valse facturen te versturen.
    - Een andere campagne maakt misbruik van **Cloudflare Pages en ZenDesk** om overtuigende phishingpagina's te hosten en inloggegevens te stelen.
    - Daarnaast blijft de dreiging van traditionelere methoden zoals **bankhelpdeskfraude** en **nepmails van de politie** onverminderd groot, waarbij criminelen direct inspelen op de onzekerheid van slachtoffers.
- **3.3. Toenemende Risico's voor Mobiele en IoT/OT-Ecosystemen** Het Zscaler ThreatLabz-rapport signaleert een alarmerende toename van aanvallen op mobiele, IoT- (Internet of Things) en OT- (Operational Technology) systemen. De publieke

sector is een belangrijk doelwit, met een gerapporteerde stijging van **370% in IoT-aanvallen op overheidsystemen**. Mobiele malware, met name gericht op Android, is sterk in opkomst, met families als:

- **Landfall:** Spyware die via een kwetsbaarheid in Samsung-telefoons wordt geïnstalleerd.
- **Fantasy Hub:** Malware gericht op het onderscheppen van SMS-berichten en bankinformatie.
- **BankBot-YNRK:** Een banktrojan die financiële gegevens steelt.

De effectiviteit van deze opkomende tactieken hangt vaak af van onderliggende technische kwetsbaarheden in de systemen die organisaties en individuen dagelijks gebruiken.

---

4. Kwetsbaarheden in Kritieke Systemen en Applicaties

Het fundament van een robuuste cyberdefensie is effectief patchmanagement. Veel succesvolle aanvallen zijn niet het gevolg van geavanceerde zero-day exploits, maar van het misbruik van bekende, maar niet-gepatchte, kwetsbaarheden in wijdverbreide software en systemen. De afgelopen week zijn diverse kritieke zwakheden aan het licht gekomen die onmiddellijke aandacht vereisen.

- **4.1. Overzicht van Kritieke Kwetsbaarheden** De onderstaande tabel geeft een overzicht van de meest urgente kwetsbaarheden die recent zijn geïdentificeerd.
- **Tabel 1: Overzicht van recente kritieke kwetsbaarheden** | **Systeem/Software** | **CVE-ID / Identifier** | **Beschrijving van de Impact** | **Status/Aanbeveling** | | :---------- | :---------- | :---------- | :---------- | | **Cisco ASA / FTD Firewalls** | CVE-2025-20333, CVE-2025-20362 | Remote toegang en code-uitvoering zonder authenticatie. | **Actief misbruikt.** Onmiddellijk patchen. | | **CentOS Web Panel** | CVE-2025-48703 | Remote code-uitvoering na het vinden van een geldige gebruikersnaam. | **Actief misbruikt.** Onmiddellijk patchen naar versie 0.9.8.1205. | | **QNAP NAS** | Meerdere (zero-days) | Diverse kwetsbaarheden die toegang tot systemen mogelijk maken. | Patches beschikbaar. Dringend advies om systemen bij te werken. | | **BIND 9 DNS Software** | CVE-2025-40778, CVE-2025-40780 | Kwetsbaarheden kunnen leiden tot DNS-cache poisoning. | Patches beschikbaar. Veel servers zijn nog kwetsbaar. | | **Django Web Framework** | CVE-2025-64459 | Kritieke SQL-injectie die kan leiden tot database-overname. | Upgraden naar de nieuwste versies. | | **WordPress (Post SMTP Plugin)** | CVE-2025-11833 | Ongeauthenticeerde aanvallers kunnen beheerdersaccounts overnemen. | **Actief misbruikt.** Onmiddellijk updaten. | | **WordPress (JobMonster Theme)** | CVE-2025-5397 | Authenticatie-bypass die overname van beheerdersaccounts mogelijk maakt. |

Update naar versie 4.8.2. | | **Microsoft Windows GDI** | CVE-2025-30388, e.a. | Kritieke kwetsbaarheden die remote code-uitvoering mogelijk maken. | Patches beschikbaar via Microsoft updates. | | **Microsoft Teams** | N.v.t. (ontwerpfouten) | Manipulatie van berichten en vervalsing van afzenders. | Clients actualiseren en medewerkers trainen. |

- **4.2. Analyse van Ongepatchte Systemen in Nederland en België** Concrete cijfers illustreren de omvang van het probleem met ongepatchte systemen in de regio:
    - **Cisco Firewalls:** 591 kwetsbare apparaten in Nederland en 86 in België zijn blootgesteld aan actieve aanvallen.
    - **BIND 9 DNS-servers:** 74 kwetsbare servers in Nederland en 18 in België missen een cruciale update, waardoor ze risico lopen op DNS-cache poisoning.
- De aanwezigheid van honderden ongepatchte, kritieke systemen in Nederland en België vormt geen theoretisch, maar een direct en geactualiseerd risico, dat een laagdrempelig aanvalsoppervlak biedt voor zowel opportunistische criminelen als statelijke actoren.

Deze technische zwakheden worden vaak doelbewust geëxploiteerd door statelijke actoren in het kader van bredere geopolitieke conflicten.

---

5. Geopolitieke Context en Statelijke Dreigingen

Geopolitieke spanningen vertalen zich steeds vaker en directer naar het digitale domein. Statelijke actoren en aan hen gelieerde groepen zetten cyberoperaties in als een instrument voor spionage, economische sabotage en het uitoefenen van politieke invloed. De waargenomen activiteiten van de afgelopen week onderstrepen deze trend.

- **5.1. Activiteiten van Belangrijke Statelijke Actoren**
    - **Rusland:** Pro-Russische hacktivistengroepen, met name **NoName** en varianten, voeren gecoördineerde DDoS-campagnes uit tegen landen die Oekraïne steunen, zoals België. Tegelijkertijd zetten militaire hackergroepen zoals **Sandworm** destructieve malware in tegen de Oekraïense economie, en gebruiken groepen als **Curly COMrades** geavanceerde technieken (zoals malware verbergen in Hyper-V VM's) voor spionage.
    - **China:** De geopolitieke spanningen rond de halfgeleiderindustrie komen tot uiting in de zaak rond **Nexperia**, waarbij Nederland wordt beschuldigd van het verstoren van de productieketen. Tegelijkertijd blijven China-geassocieerde hackers oude, bekende kwetsbaarheden (zoals Log4j, vergelijkbaar met de kritieke zwakheden in Django en WordPress die in dit rapport worden geanalyseerd) misbruiken voor langdurige spionageoperaties tegen westerse doelwitten.

  - **Noord-Korea:** Dit land zet cyberoperaties in voor zowel spionage als financieel gewin. De groep **Famous Chollima** gebruikt AI-gegenereerde deepfakes om bedrijven te infiltreren, terwijl de **Kimsuky**-groep de EndClient RAT verspreidt voor spionage tegen mensenrechtenactivisten. De opbrengsten uit deze en andere cybercriminele activiteiten worden witgewassen door Noord-Koreaanse bankiers, wat heeft geleid tot internationale sancties.
- **5.2. Risico's in de Toeleveringsketen (Supply Chain)** Een expliciete waarschuwing is dat de kwetsbaarheid van Nederlandse bedrijven met name bij hun externe toeleveranciers ligt. Statelijke actoren maken bewust gebruik van deze zwakke schakels om via kleinere, minder beveiligde bedrijven toegang te krijgen tot grotere, strategische doelwitten. De Nexperia-zaak is een treffend voorbeeld van hoe geopolitieke druk via de toeleveringsketen kan worden uitgeoefend, met potentieel verstrekkende economische gevolgen voor sectoren zoals de auto-industrie.

De analyse van deze dreigingen en patronen leidt tot een reeks strategische conclusies en aanbevelingen om de weerbaarheid te verhogen.

---

6. Conclusies en Strategische Aanbevelingen

De analyse van de afgelopen week toont een dreigingslandschap dat wordt gekenmerkt door diverse en steeds geavanceerdere aanvalsmethoden. De belangrijkste trends zijn een duidelijke toename van verstorende aanvallen (met name DDoS), de snelle operationalisering van AI in cybercriminaliteit, en de aanhoudende risico's die voortvloeien uit onvoldoende patchmanagement en kwetsbaarheden in de toeleveringsketen. Statelijke actoren blijven een dominante factor, waarbij geopolitieke conflicten direct worden uitgevochten in cyberspace.

Op basis van deze bevindingen worden de volgende strategische aanbevelingen gedaan:

1. **Verhoogde Weerbaarheid tegen Verstorende Aanvallen:** De gecoördineerde en aanhoudende DDoS-campagnes tegen Belgische vitale infrastructuur en overheidsinstellingen tonen de noodzaak om DDoS-mitigatiestrategieën te herzien en te versterken. Organisaties moeten investeren in robuuste beschermingsmaatregelen en continuïteitsplannen ontwikkelen voor het geval van langdurige verstoringen.
2. **Prioritering van Patchmanagement:** De actieve exploitatie van bekende kwetsbaarheden in systemen zoals Cisco-firewalls, CentOS Web Panel en WordPress-plugins onderstreept de urgentie van een gedisciplineerd patchbeleid. Er moet onmiddellijk actie worden ondernomen om de geïdentificeerde kritieke kwetsbaarheden te dichten, met specifieke aandacht voor internet-georiënteerde systemen.

3. **Versterking van de 'Human Firewall':** Medewerkers blijven een cruciaal doelwit. Het is essentieel om trainingen te intensiveren, gericht op het herkennen van geavanceerde social engineering, phishing via legitieme clouddiensten (zoals AWS en Cloudflare) en AI-gegenereerde misleiding (deepfakes, 'vibe hacking'). Bewustwording is de eerste verdedigingslinie tegen deze verfijnde tactieken.
4. **Audit van de Toeleveringsketen (Supply Chain):** De expliciete waarschuwingen en de casus van Omrin tonen aan dat het eigen beveiligingsniveau waardeloos is als toeleveranciers een zwakke schakel vormen. Het is aan te bevelen om de beveiligingsmaatregelen van kritieke externe leveranciers en partners periodiek en kritisch te beoordelen en contractuele eisen te stellen aan hun cyberweerbaarheid.
5. **Beveiliging van Mobiele Ecosystemen:** De gerapporteerde sterke toename van mobiele malware en aanvallen op IoT-systemen vereist een aangescherpt beleid. Beperk de installatie van applicaties uit onbekende bronnen, dwing het gebruik van Mobile Device Management (MDM) af en implementeer een zero trust-architectuur om de risico's van een groeiend aantal verbonden apparaten te beheersen.