Week 44-2025

Strategisch Dreigingsrapport: Analyse van het Cyberlandschap voor Nederland en België

1.0 Inleiding: Het Evoluerende Dreigingslandschap

Nederlandse en Belgische organisaties opereren in een steeds complexer en vijandiger digitaal domein. Het cyberdreigingslandschap wordt gekenmerkt door een toenemende diversiteit aan dreigingsactoren, variërend van financieel gemotiveerde cybercriminelen tot staatsgesponsorde spionagegroepen. De geavanceerdheid en frequentie van aanvallen nemen toe, waardoor de digitale weerbaarheid van zowel publieke als private sectoren continu op de proef wordt gesteld. Dit rapport biedt een strategisch overzicht van de meest relevante dreigingen, gebaseerd op een analyse van recente incidenten en opkomende tactieken. Het doel is om besluitvormers te wapenen met de benodigde inzichten om risico's adequaat in te schatten en de verdediging van hun organisaties proactief te versterken. De analyse begint met een van de meest directe en ontwrichtende bedreigingen voor de bedrijfscontinuïteit: ransomware.

2.0 Analyse van Ransomware-aanvallen: Een Directe Bedreiging voor de Bedrijfscontinuïteit

Ransomware is geëvolueerd van een eenvoudige versleutelingsdreiging naar een geavanceerde afpersingseconomie. Het strategisch belang van het begrijpen van deze evolutie kan niet worden onderschat. Moderne ransomwaregroepen hanteren vaak een tactiek van 'dubbele afpersing', waarbij zij niet alleen data versleutelen, maar deze eerst stelen en dreigen met publicatie op het darkweb. Dit verhoogt de druk op slachtoffers om losgeld te betalen aanzienlijk. De opkomst van het Ransomware-as-a-Service (RaaS) model heeft de drempel voor criminelen verlaagd, waardoor zelfs actoren met beperkte technische kennis toegang hebben tot geavanceerde aanvalstools en infrastructuur. De selectie van doelwitten, variërend van zorginstellingen (VZW Avalon) tot vitale diensten zoals afvalverwerking (Omrin), toont aan dat geen enkele sector immuun is en dat aanvallers zich specifiek richten op organisaties waar operationele verstoring de druk om te betalen maximaliseert.

Recente Ransomware-incidenten in Nederland en België

- **Doelwit:** VZW Avalon (België)

- **Aanvaller:** Incransom
- **Impact:** De zorginstelling werd geconfronteerd met de versleuteling van meer dan 31 gigabyte aan data, verdeeld over bijna 39.000 bestanden. Gevoelige gegevens van kwetsbare bewoners zijn hierdoor mogelijk blootgesteld.

- **Doelwit:** Omrin (Nederland)
  - **Aanvaller:** Qilin
  - **Impact:** De Friese afvalverwerker zag gestolen data, waaronder persoonlijke gegevens van medewerkers (woonadressen, salarisinformatie, ID-kopieën) en bedrijfsinformatie, gepubliceerd worden op het darkweb. Dit leidde tot operationele verstoringen, zoals de tijdelijke sluiting van kringloopwinkels.
- **Doelwit:** Spijkermat (Nederland)
  - **Aanvaller:** Radiant
  - **Impact:** De distributeur van acupressuurmatten werd slachtoffer van een aanval die resulteerde in een datalek, waarbij bedrijfsgegevens mogelijk openbaar zijn gemaakt door de aanvallers.
- **Doelwit:** Bagnoles.nl (Nederland)
  - **Aanvaller:** Qilin
  - **Impact:** Deze autoleverancier werd getroffen door een aanval die vermoedelijk heeft geleid tot toegang tot gevoelige bedrijfs- en klantinformatie.

De tactieken die door deze en andere groepen worden gebruikt, worden steeds geraffineerder. Ze richten zich niet alleen op technische kwetsbaarheden, maar maken ook gebruik van legitieme tools om detectie te omzeilen en exploiteren de menselijke factor binnen organisaties.

Ransomwaregroep	Kenmerkende Tactiek of Aanvalsvector

Qilin	Gebruikt ingebouwde en legitieme Windows-tools zoals mspaint.exe en notepad.exe om handmatig naar waardevolle bestanden te zoeken.
Play	Hanteert een onconventionele tactiek door medewerkers van doelwitbedrijven direct aan te sporen om toegang tot het netwerk te verkopen.
Warlock	Maakte misbruik van een kritieke zero-day kwetsbaarheid in Microsoft SharePoint (CVE-2024-53770) voor de verspreiding van de ransomware.

Terwijl financieel gewin de drijfveer is achter de ontwrichtende ransomware-economie, vormt de strategische dreiging van statelijke actoren, opererend met geopolitieke motieven, een fundamenteel ander en potentieel existentiëler risico.

3.0 Geopolitieke Dreigingen: Staatsgesponsorde Spionage en Hacktivisme

Staatsgesponsorde cyberoperaties vormen een strategische dreiging met verstrekkende gevolgen. Deze campagnes zijn niet alleen gericht op traditionele spionage, zoals het stelen van intellectueel eigendom of staatsgeheimen, maar ook op het destabiliseren van geopolitieke verhoudingen en het aanvallen van vitale infrastructuren. Nederlandse en Belgische organisaties, met name die in de overheid, defensie en hoogtechnologische sectoren, zijn prominente doelwitten in dit speelveld.

Spionagecampagnes in Europa

Recente campagnes tonen een duidelijke focus op Europese entiteiten:

- **Chinese spionage gericht op diplomaten (UNC6384 / Mustang Panda):** Deze Chinese Advanced Persistent Threat (APT)-groep voerde een gerichte spionagecampagne uit tegen Europese diplomaten, onder meer in België en Hongarije. De aanvallers maakten gebruik van een zero-day kwetsbaarheid in Windows (CVE-2024-9491) en verspreidden via spearphishing-e-mails een Remote Access Trojan (RAT) genaamd PlugX. Deze operatie is een duidelijk voorbeeld van cyber-spionage gericht op het verkrijgen van gevoelige diplomatieke informatie.
- **Noord-Koreaanse spionage gericht op de drone-industrie (Lazarus):** De beruchte Lazarus-groep heeft zich gericht op Europese bedrijven die drone-

technologie ontwikkelen. Het doel van deze aanvallen is het stelen van technische ontwerpen en gegevens, vermoedelijk om de eigen Noord-Koreaanse droneproductie te ondersteunen.

De Opkomst van Gecoördineerd Hacktivisme

Naast staatspionage is hacktivisme een groeiend fenomeen. Ideologisch gedreven groepen voeren aanvallen uit om politieke boodschappen te verspreiden of operaties van als vijandig beschouwde staten en organisaties te verstoren. Recentelijk is een trend van toenemende coördinatie zichtbaar:

- **Russische Allianties:** De vorming van allianties tussen Russische hacktivistische groepen, zoals **OverFlame** met **M.O.L.O.T.** en **TwoNet** met **NoName057(16)**, vergroot hun aanvalscapaciteit en bereik. Deze consolidatie in het hacktivistische landschap duidt op een professionaliseringsslag, waarbij losse, ideologisch gedreven groepen evolueren naar meer persistente en capabele dreigingsactoren met het potentieel voor gecoördineerde, systemische verstoringen.
- **Strategische Waarschuwing:** De recente cyberaanvallen op **Canadese vitale infrastructuren**, waaronder olie-, gas- en waterbedrijven, dienen als een strategische waarschuwing. Hacktivisten manipuleerden industriële controlesystemen, wat leidde tot aanpassingen in waterdruk en temperatuur. Dit illustreert de kwetsbaarheid van vergelijkbare vitale sectoren in Nederland en België voor dergelijke ontwrichtende acties.

Deze aanvallen, of ze nu door staten of hacktivisten worden uitgevoerd, zijn afhankelijk van onderliggende technische zwakheden. De volgende sectie analyseert de kernkwetsbaarheden en aanvalsvectoren die deze operaties mogelijk maken.

4.0 Kernkwetsbaarheden en Aanvalsvectoren

Een analyse van succesvolle inbraken toont een ongemakkelijke waarheid: geavanceerde dreigingsactoren bouwen hun campagnes vaak op een fundament van basale, vermijdbare beveiligingsfouten bij hun doelwitten. Zelfs staatsgesponsorde groepen scannen actief naar en exploiteren veelgebruikte, niet-gepatchte zwakheden voor initiële toegang. Het tijdig identificeren en mitigeren van deze kwetsbaarheden is cruciaal om de deur voor aanvallers gesloten te houden. Een analyse van recente incidenten onthult een aantal kritieke zwakke plekken en opkomende aanvalsmethoden die de aandacht van besluitvormers vereisen.

4.1 Kritieke Softwarekwetsbaarheden

1. **Windows Server Update Services (WSUS):** De kwetsbaarheid CVE-2024-59287 stelt aanvallers in staat om niet-gepatchte WSUS-servers op afstand over te nemen, wat hen volledige controle over een bedrijfsnetwerk kan geven. Recent onderzoek identificeerde **81 kwetsbare servers in Nederland en 10 in België** die direct vanaf het internet toegankelijk zijn.
2. **Linux Kernel:** Een ernstige privilege-escalatiekwetsbaarheid (CVE-2024-1086) in de Linux-kernel wordt actief misbruikt door ransomwaregroepen. Aanvallers die reeds beperkte toegang hebben, kunnen hiermee hun rechten verhogen tot root-niveau, wat leidt tot een volledige systeemovername.
3. **Microsoft SharePoint:** Een zero-day kwetsbaarheid (CVE-2024-53770) werd misbruikt door de Warlock-ransomwaregroep als een belangrijke vector voor het binnendringen van bedrijfsnetwerken en het verspreiden van hun malware.
4. **WordPress Plugins:** De enorme populariteit van WordPress maakt zijn ecosysteem een aantrekkelijk doelwit. Recente voorbeelden zijn een kwetsbaarheid in de **Freeio**-plugin (CVE-2024-11533) die ongeautoriseerde toegang met beheerdersrechten mogelijk maakte, en een Cross-Site Scripting (XSS) kwetsbaarheid in de veelgebruikte **LiteSpeed Cache**-plugin.

4.2 Opkomende Malware en Evasieve Tactieken

Aanvallers ontwikkelen continu nieuwe methoden om detectie door beveiligingssystemen te omzeilen. Deze tactieken maken het moeilijker om kwaadaardige activiteit te herkennen en erop te reageren.

- **Malware-as-a-Service (MaaS):** Platformen zoals **Atroposia** en **Herodotus** verlagen de drempel voor cybercriminelen. Ze bieden kant-en-klare malware (zoals Remote Access Trojans) aan via een abonnementsmodel, compleet met controlepanelen en ondersteuning.
- **Geavanceerde Evasie:** Om detectie te voorkomen, worden steeds slimmere technieken ingezet:
    - **Nabootsen van menselijk gedrag:** De Herodotus-malware implementeert willekeurige vertragingen tussen toetsaanslagen om geautomatiseerde detectiesystemen te misleiden.

- **Steganografie:** De Caminho-malware loader verbergt zijn kwaadaardige code in de pixels van ogenschijnlijk onschuldige afbeeldingsbestanden, een techniek bekend als Least Significant Bit (LSB) steganografie.
- **Misbruik van legitieme tools:** De 'ClickFix'-techniek verleidt gebruikers om via social engineering schadelijke opdrachten uit te voeren die de legitieme remote-beheertool NetSupport RAT installeren voor kwaadaardige doeleinden.

4.3 Social Engineering en Fraude

Naast technische exploits blijft de menselijke factor een primair doelwit. Fraudecampagnes richten zich op zowel burgers als werknemers met steeds overtuigendere methoden.

- De grootschalige **'Smishing Triad'-operatie** maakt gebruik van meer dan 194.000 kwaadaardige domeinen voor wereldwijde fraude via sms-berichten, gericht op bankdiensten en pakketleveringen.
- In **België** is een duidelijke toename gemeld van fraude via de remote-desktopsoftware **AnyDesk**, waarbij oplichters slachtoffers overtuigen om hen toegang tot hun systemen te verlenen.
- In **Nederland** blijft **bankhelpdeskfraude** een aanhoudend probleem, waarbij criminelen zich telefonisch voordoen als bankmedewerkers om slachtoffers te overtuigen geld over te maken.

Deze technische kwetsbaarheden en aanvalsvectoren vertalen zich direct naar overkoepelende strategische risico's die een holistische benadering van beveiliging vereisen.

5.0 Strategische Conclusies en Imperatieven voor Besluitvormers

De geanalyseerde dreigingen en kwetsbaarheden vormen geen geïsoleerde incidenten, maar zijn manifestaties van bredere strategische risico's. Het is de taak van besluitvormers om deze analyse te vertalen naar concrete acties en proactief leiderschap te tonen in het versterken van de digitale weerbaarheid. De complexiteit van het huidige dreigingslandschap vereist een adaptieve en gelaagde verdedigingsstrategie.

Risico's door Vervaagde Organisatorische Grenzen

De traditionele perimeter van de organisatie is vervaagd. Dreigingen komen niet langer alleen van buitenaf, maar ook van binnenuit en via de toeleveringsketen.

- ***Insider Threats:*** Het risico van kwaadwillende of nalatige medewerkers wordt steeds concreter en strategischer. De **Play-ransomwaregroep** speelt hier actief op in door medewerkers aan te sporen om bedrijfstoegang te verkopen. Dit risico escaleert echter tot op staatsniveau, zoals blijkt uit de aanklacht tegen de voormalige directeur van **L3Harris' cyberdivisie Trenchant**. Hij wordt beschuldigd van het stelen van bedrijfsgeheimen met de intentie deze aan een Russische koper te verkopen. Dit verschuift de dreiging van opportunistische fraude naar doelgerichte bedrijfsspionage en onderstreept de noodzaak voor robuuste interne controles.
- ***Supply Chain Risico's:*** Organisaties zijn kwetsbaar via de software en diensten die zij gebruiken. De **PhantomRaven**-campagne, die kwaadaardige **npm-pakketten** gebruikte om de omgevingen van softwareontwikkelaars te infiltreren, toont aan hoe de toeleveringsketen van software een kritiek aanvalsoppervlak is geworden.

Kwetsbaarheid van Vitale Infrastructuur en Cloud-afhankelijkheid

De digitalisering van vitale sectoren en de massale adoptie van clouddiensten creëren nieuwe, geconcentreerde risico's.

- **Vitale Infrastructuren onder Vuur:** De waarschuwingen van de **NAVO** en de incidenten in **Canada** waarbij industriële controlesystemen werden gemanipuleerd, zijn geen abstracte scenario's. De ontdekking van kritieke kwetsbaarheden in systemen zoals de **Veeder-Root** brandstofmonitoringsystemen bevestigt dat de operationele technologie (OT) die onze vitale infrastructuur aanstuurt, een direct doelwit is.
- **Afhankelijkheid van de Cloud:** De storingen bij **Microsoft Azure** en **Amazon Web Services (AWS)**, die diensten zoals de reisplanner van de **NS** platlegden, illustreren de operationele risico's van een afhankelijkheid van een klein aantal dominante cloudproviders. Deze machtsconcentratie creëert niet alleen single points of failure, maar ook een strategische kwetsbaarheid. Zoals het hoofd van de versleutelde berichtendienst Signal opmerkte, hebben veel

organisaties "geen andere keuze" dan gebruik te maken van diensten als AWS, wat een systemisch risico voor de gehele digitale economie vormt.

Conclusie: De Noodzaak van een Adaptieve Verdediging

Het dreigingslandschap voor Nederlandse en Belgische organisaties is dynamisch, veelzijdig en onvergeeflijk. De aanvallen variëren van opportunistische fraude tot strategisch geplande staatspionage. Een passieve of reactieve houding is niet langer voldoende. De strategische noodzaak is duidelijk: organisaties moeten een robuuste en adaptieve verdediging opbouwen die is geworteld in proactief risicobeheer. Dit dwingt tot een onmiddellijke en ononderhandelbare focus op cyberhygiëne, te beginnen met agressief en consistent patchbeheer om bekende kwetsbaarheden te dichten. Tegelijkertijd moet het beveiligingsbewustzijn van medewerkers continu worden verhoogd om weerstand te bieden tegen social engineering en insider threats. Ten slotte is de implementatie van zero-trust architecturen – waarbij niets en niemand standaard wordt vertrouwd – essentieel om de weerbaarheid te verhogen tegen de geavanceerde en persistente dreigingen die in dit rapport zijn geanalyseerd.