Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

27-11-2025:

Minister: verboden om producten met verborgen kill-switch aan te bieden

De demissionair minister van Justitie en Veiligheid, Van Oosten, heeft bevestigd dat het op de Europese markt verboden is om producten aan te bieden met verborgen 'kill-switches'. Deze beslissing volgt op een motie die in juni door de Tweede Kamer werd aangenomen, waarin werd gepleit voor wetgeving tegen de integratie van deze technologie in consumentenapparatuur zoals zonnepanelen, omvormers, laadpalen en warmtepompen. De motie, ingediend door de Kamerleden Six Dijkstra en Postma, waarschuwde voor de risico's die verbonden zijn aan het gebruik van apparaten die op afstand kunnen worden uitgeschakeld via verborgen functionaliteiten.

Volgens de minister is het verboden om producten te verkopen die niet volledig transparant zijn over hun technische specificaties, met name als het gaat om software- of hardwarecomponenten die de mogelijkheid bieden om apparaten op afstand aan of uit te zetten. Dit geldt niet alleen voor producten die binnen de Europese Unie worden geproduceerd, maar ook voor producten afkomstig van fabrikanten buiten de EU, zodra ze op de Europese markt worden geïntroduceerd.

Deze wetgeving is een reactie op de bezorgdheid dat veel zonnepanelen en omvormers in Europa zijn uitgerust met dergelijke functionaliteiten die centraal kunnen worden aangestuurd, vaak vanuit leveranciers in landen als China. De Kamerleden benadrukten de potentiële gevaren voor de energievoorziening in Nederland en andere Europese landen, waar een "hack of politiek decreet" ernstige verstoringen zou kunnen veroorzaken. De minister ziet echter geen noodzaak voor aanvullende wetgeving tegen kill-switches, aangezien de bestaande Europese regels deze praktijken al verbieden.

Noord-Koreaanse hackers ontwijken VN-sancties door gebruik te maken van cybercapaciteiten, IT-werknemers en cryptovaluta-activiteiten

Noord-Korea heeft zijn wereldwijde cyberoperaties geïntensiveerd en schendt systematisch de resoluties van de Veiligheidsraad van de Verenigde Naties door grootschalige cyberaanvallen, diefstal van cryptovaluta en grensoverschrijdende witwaspraktijken. Volgens een recent rapport van het Multilaterale Sancties Monitoring Team (MSMT) hebben Noord-Koreaanse hackers in 2024 ten minste 1,19 miljard dollar aan cryptovaluta gestolen, en in de eerste negen maanden van 2025

kwam daar nog eens 1,65 miljard dollar bij. Dit brengt het totaal op ongeveer 2,8 miljard dollar.

De cybercapaciteiten van Noord-Korea hebben bijna het niveau van supermachten bereikt, met verschillende Advanced Persistent Threat (APT)-groepen die gecoördineerde aanvallen uitvoeren binnen de cryptovaluta-industrie. Deze operaties dienen om het regime van financiering te voorzien voor massavernietigingswapens en ballistische raketprogramma's. De inbraak van februari 2025 bij de in Dubai gevestigde Bybit-exchange, waarbij bijna 1,5 miljard dollar werd gestolen, geldt als de grootste cryptodiefstal in de geschiedenis.

Andere belangrijke slachtoffers zijn onder meer de Japanse DMM Bitcoin en het Indiase WazirX. Beveiligingsanalisten van SlowMist hebben vastgesteld dat Noord-Koreaanse dreigingsactoren geavanceerde malware inzetten via social engineering-campagnes die zich voordoen als sollicitatiegesprekken. De "Contagious Interview"-campagne richt zich specifiek op softwareontwikkelaars door hen uit te nodigen voor online sollicitaties, waarna hen wordt gevraagd om kwaadaardige softwarepakketten te downloaden.

Bij uitvoering verzamelt de BeaverTail-malware de gegevens van cryptowallets en creditcardinformatie die in browsers zijn opgeslagen, terwijl de InvisibleFerret-backdoor stiekem wordt geïnstalleerd voor persistente toegang op afstand. Deze aanvalstechnieken tonen de geavanceerde technische bekwaamheid van de aanvallers, die zich door middel van valse sollicitatiewebsites toegang verschaffen tot doelwitsystemen. Zodra slachtoffers de nepwebsites bezoeken, worden ze misleid om kwaadaardige stuurprogramma's te downloaden die hun systemen compromitteren.

Noord-Koreaanse IT-werknemers ondersteunen deze cyberoperaties door infiltratie van bedrijven wereldwijd via freelanceplatforms zoals Upwork, Freelancer en Fiverr. Deze werknemers maken gebruik van door AI gegenereerde valse gezichten en vervalste documenten om identiteitsverificatie te omzeilen. Ze verdienen maandelijks gemiddeld 10.000 dollar, waarvan een groot deel naar het regime wordt doorgestuurd. Het MSMT-rapport bevestigt de inzet van Noord-Koreaanse IT-werknemers in landen als China, Rusland, Laos en verschillende Afrikaanse landen.

Het witwassen van gestolen cryptovaluta volgt een meervoudig proces, waarbij token-swaps worden uitgevoerd via gedecentraliseerde beurzen, mengdiensten zoals Tornado Cash en Wasabi Wallet, en blockchain-bruggen, voordat de valuta uiteindelijk in fiatgeld wordt omgezet via over-the-counter-brokers. Dit systematische

proces van sanctie-omzeiling vormt een toenemende bedreiging voor het wereldwijde financiële ecosysteem, waarvoor een gecoördineerde internationale reactie noodzakelijk is.

Asus waarschuwt voor kritieke AiCloud-kwetsbaarheid in routers

Asus heeft een waarschuwing uitgegeven voor een kritieke kwetsbaarheid in de AiCloud-dienst van zijn routers, die het mogelijk maakt voor aanvallers om op afstand toegang te krijgen tot de routers. De kwetsbaarheid, aangeduid als CVE-2025-59366, stelt aanvallers in staat om de authenticatie van de router te omzeilen, waardoor ze de controle over de apparaten kunnen overnemen. Dit beveiligingslek heeft een zeer hoge risico-inschatting van 9.2 op een schaal van 1 tot 10.

De kwetsbaarheid is ontdekt in de AiCloud-service, waarmee gebruikers via het internet toegang krijgen tot lokale bestanden op apparaten die met de Asus-router zijn verbonden. Asus heeft firmware-updates vrijgegeven voor de getroffen modellen om het probleem te verhelpen. Routers die niet langer worden ondersteund en die aan het einde van hun levensduur zijn, kunnen het best de AiCloud-service uitschakelen om het risico te minimaliseren.

Op dit moment heeft Asus niet precies aangegeven welke routermodellen kwetsbaar zijn. Vorige week werd echter gemeld dat duizenden oudere, niet-ondersteunde routers zijn gecompromitteerd door aanvallers die gebruik maakten van eerdere kwetsbaarheden in dezelfde AiCloud-service.

Firewalls en vpn's blijven aantrekkelijke doelwitten voor aanvallers in Nederland

Firewalls, routers en vpn's van Nederlandse bedrijven blijven een belangrijk doelwit voor zowel statelijke als criminele actoren. Dit blijkt uit het recent gepubliceerde Cybersecuritybeeld Nederland 2025 (CSBN), waarin de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) aangeeft dat vooral edge devices, zoals firewalls en vpn's aan de rand van netwerken, vaak het doelwit zijn van aanvallen. De NCTV benadrukt dat deze apparaten, die vaak als toegangspoort fungeren tot grotere netwerken, steeds vaker worden aangevallen om toegang te verkrijgen tot andere systemen binnen de organisatie.

Een voorbeeld van deze aanvallen is het incident bij het Openbaar Ministerie (OM), waar aanvallers erin slaagden om Citrix-systemen te compromitteren. Dit incident benadrukt de voortdurende dreiging van aanvallen op edge devices. De NCTV meldt dat vooral Chinese actoren, die vaak gebruik maken van gesofisticeerde aanvalsinfrastructuren en malware, verantwoordelijk zijn voor veel van deze aanvallen. Deze aanvallers zijn volgens de NCTV succesvol in het infiltreren van westerse overheden en bedrijven.

Bovendien wijst het CSBN 2025 op de snelle exploitatie van kwetsbaarheden in edge devices. Zodra kwetsbaarheden bekend worden, kunnen aanvallers binnen enkele uren of dagen misbruik maken van deze zwakheden. Dit geeft organisaties maar weinig tijd om beveiligingsupdates of patches te installeren, waardoor het risico op een succesvolle aanval aanzienlijk toeneemt.

Het rapport van de NCTV legt ook de nadruk op het belang van goede digitale basishygiëne. Het niet tijdig installeren van beveiligingsupdates blijft een van de belangrijkste oorzaken van digitale incidenten. Aangezien de dreigingen steeds diverser en complexer worden, blijft het essentieel dat organisaties hun digitale basisbeveiliging op orde houden om zich te wapenen tegen dergelijke aanvallen.

NCTV waarschuwt voor tekortschietende cybersecurity binnen de Rijksoverheid

De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) heeft in het Cybersecuritybeeld Nederland 2025 ernstige zorgen geuit over de huidige staat van cybersecurity binnen de Rijksoverheid. Volgens de NCTV biedt de bestaande beveiliging onvoldoende bescherming en creëert het een vals gevoel van veiligheid. Dit wordt versterkt door het feit dat overheidsorganisaties vaak niet in staat zijn om cyberaanvallen zelfstandig te detecteren of te mitigeren, ondanks diverse projecten en initiatieven die zijn opgezet om de beveiliging te verbeteren.

Het rapport benadrukt dat het onmogelijk is om met zekerheid te stellen dat er momenteel geen incidenten zijn waarbij overheidsinstanties zijn gecompromitteerd. Er wordt aangegeven dat veel overheidsorganisaties niet voldoen aan de informatiebeveiligingsrichtlijnen die de Rijksoverheid zelf heeft vastgesteld. De mate van digitale weerbaarheid verschilt sterk tussen organisaties en sectoren, maar het is duidelijk dat er nog aanzienlijke stappen moeten worden gezet.

Daarnaast wordt gewezen op de risico's die ontstaan door de afhankelijkheid van externe digitale dienstverleners, waarbij de afwegingen rondom deze risico's onvoldoende zijn. Het is dan ook noodzakelijk dat de Rijksoverheid niet alleen de bescherming van digitale infrastructuren verbetert, maar ook zorg draagt voor effectieve terugvalopties in geval van storingen of uitval van digitale processen.

De NCTV concludeert dat er aanzienlijke verbeteringen nodig zijn om de digitale veiligheid van de Rijksoverheid te waarborgen en om de risico’s van cyberdreigingen effectief te beheren.

RomCom gebruikt SocGholish-aanvallen om Mythic Agent-malware te verspreiden

De dreigingsactoren achter de malwarefamilie RomCom hebben onlangs een Amerikaanse ingenieursfirma aangevallen via een JavaScript-loader, SocGholish, waarmee ze de Mythic Agent-malware verspreidden. Dit markeert de eerste keer dat een RomCom-payload via SocGholish werd gedistribueerd, volgens een rapport van Arctic Wolf Labs. De aanval werd toegeschreven aan een Russische militaire eenheid, Unit 29155 van de GRU, die eerder al betrokken was bij cyberaanvallen tegen Oekraïense en NAVO-gerelateerde organisaties.

De aanval werd uitgevoerd via een nep-updatemelding voor webbrowserupdates van Google Chrome of Mozilla Firefox, die op legitieme maar gecompromitteerde websites werd getoond. Gebruikers werden verleid om schadelijke JavaScript-bestanden te downloaden, die vervolgens een malwareloader installeerden. Deze loader haalt aanvullende malware binnen, waaronder de Mythic Agent, een krachtige tool die wordt gebruikt voor afstandsbediening van geïnfecteerde systemen.

De RomCom-groep maakt gebruik van verschillende aanvalsmethoden, waaronder spear-phishing en zero-day exploits, om systemen te infiltreren en de remote access trojan (RAT) op doelwitsystemen te installeren. In dit specifieke geval wisten de aanvallers na infectie de controle over het systeem te krijgen door middel van een reverse shell, waarmee ze commando’s konden uitvoeren en verdere backdoors konden installeren, waaronder een Python-backdoor genaamd VIPERTUNNEL.

Hoewel de aanval werd gestopt voordat verdere schade kon worden aangericht, benadrukt deze gebeurtenis de voortdurende dreiging van RomCom, vooral gericht op Oekraïne en gerelateerde entiteiten. De snelheid waarmee de aanval van toegang tot infectie verloopt, maakt SocGholish tot een bijzonder gevaarlijke techniek die

wereldwijd organisaties blootstelt aan risico's. De aanval werd gedetecteerd en gestopt binnen minder dan dertig minuten, nadat het doelwit was bevestigd via Active Directory.

NTLM misbruik in cyberaanvallen blijft toenemen in 2025

NTLM (New Technology LAN Manager) is een verouderd authenticatieprotocol dat nog steeds veelvuldig wordt gebruikt in Windows-omgevingen, ondanks de goed gedocumenteerde kwetsbaarheden en Microsofts plannen om het protocol uit te faseren. In 2025 wordt NTLM actief misbruikt in cyberaanvallen, met name door middel van technieken zoals NTLM-relay, credential forwarding en man-in-the-middle-aanvallen. Ondanks de bekendheid van deze kwetsbaarheden blijft NTLM in veel bedrijfsnetwerken aanwezig, vaak door compatibiliteitseisen of verouderde applicaties die nog afhankelijk zijn van dit protocol.

In de afgelopen jaren zijn er steeds nieuwe kwetsbaarheden ontdekt die aanvallers de mogelijkheid geven om NTLM op verschillende manieren te misbruiken. Een belangrijke techniek is hash-lekage, waarbij NTLM-hashes per ongeluk worden blootgesteld via phishing-aanvallen of slecht geconfigureerde netwerkinstellingen. Deze hashes kunnen vervolgens worden gebruikt in pass-the-hash-aanvallen, waarbij aanvallers zich kunnen voordoen als een geverifieerde gebruiker zonder het wachtwoord daadwerkelijk te kennen.

Daarnaast zijn er aanvallen waarbij de aanvaller een slachtoffer dwingt om zich aan te melden bij een server die door de aanvaller wordt beheerd, een techniek die bekend staat als coercion-based attacks. Dit maakt het mogelijk om NTLM-hashes af te vangen en later te gebruiken om toegang te krijgen tot andere systemen binnen het netwerk. In veel gevallen wordt dit gecombineerd met man-in-the-middle-aanvallen, waarbij de aanvaller de communicatie tussen de client en de server onderschept en manipuleert om toegang te verkrijgen tot gevoelige systemen.

In 2025 zijn er meerdere kwetsbaarheden gerapporteerd die direct verband houden met NTLM, waaronder CVE-2024-43451 en CVE-2025-24054. Deze kwetsbaarheden stellen aanvallers in staat om NTLM-hashes te lekken zonder dat er veel interactie van de gebruiker vereist is. In sommige gevallen wordt de kwetsbaarheid actief misbruikt in aanvallen die gericht zijn op specifieke regio's, zoals Latijns-Amerika en Rusland, waar cybercriminelen gebruikmaken van sociale engineering en andere technieken om hun malware te verspreiden.

De afhankelijkheid van NTLM blijft een belangrijke zorg voor cybersecurity-experts, omdat het protocol nog steeds wijdverspreid wordt gebruikt in veel bedrijfsomgevingen. De afwezigheid van moderne beveiligingsmechanismen zoals kanaalbinding en wederzijdse authenticatie maakt NTLM bijzonder kwetsbaar voor misbruik. De recente incidenten laten zien dat cybercriminelen nieuwe manieren blijven vinden om dit verouderde protocol te exploiteren, waardoor de veiligheid van netwerken in gevaar komt.

Microsoft heeft plannen om NTLM in de komende jaren uit te faseren, maar tot dat moment blijven organisaties kwetsbaar voor aanvallen die gebruikmaken van dit protocol. Het wordt sterk aanbevolen om NTLM te deactiveren of ten minste te beperken tot de meest kritieke systemen, en om te investeren in modernere en veiligere authenticatieprotocollen, zoals Kerberos.

Water Gamayun APT-klasse aanval blootgelegd door Zscaler

Zscaler Threat Hunting heeft recent een complexe meerfasige aanval van de Water Gamayun APT-groep (Advanced Persistent Threat) geanalyseerd, die gebruikmaakte van een exploit in de Microsoft Management Console (MMC). Deze aanval werd uitgevoerd met behulp van een opzet die ogenschijnlijk onschadelijke zoekopdrachten en documenten gebruikte, maar uiteindelijk verborgen PowerShell-aanvallen en malware-virussen bracht. Water Gamayun, die vaak in verband wordt gebracht met Russische operaties, richt zich op bedrijven en overheidsnetwerken, waarbij ze steelt en inlichtingen verzamelt via langdurige en stealth-aanvallen.

De aanval begon met een ogenschijnlijk normale zoekopdracht via Bing naar een legitieme website. Dit leidde naar een vervalste domeinnaam die de gebruiker omleidde naar een kwaadaardige RAR-archief met een dubbele bestandsextensie. Dit archief werd gepresenteerd als een PDF-document, maar het bevatte een bestand dat uiteindelijk een exploit uitvoerde op de MSC EvilTwin-vulnerabiliteit (CVE-2025-26633) binnen de MMC. Het kwaadwillige bestand injecteerde code in het legitieme proces van mmc.exe en zette een reeks PowerShell-scripts in werking om de aanval voort te zetten.

In de eerste fase van de aanval werd een geïnfecteerd bestand gedownload dat een code injecteerde via de taskpad-functionaliteit in MMC. Dit leidde tot de uitvoering van PowerShell-scripts die verder verborgen bestanden binnenhaalden, waaronder een RAR-bestand dat een wachtwoord beschermde. Deze scripts zorgden ervoor dat

de malware werd uitgevoerd zonder detectie door de gebruiker. Het tweede stadium van de aanval bracht een script dat C# gebruikte om consolevensters te verbergen, terwijl een schijnbaar onschuldige PDF werd getoond om de gebruiker te misleiden.

In de laatste fase van de aanval werd een backdoor geïnstalleerd, vermoedelijk gerelateerd aan bekende Water Gamayun-malware zoals EncryptHub of SilentPrism. Het exacte type malware kon niet worden bevestigd, omdat de communicatie met de command-and-control-infrastructuur werd verstoord. De Zscaler Threat Hunting-team voerde een grondige reconstructie van de aanval uit en koppelde het gebruik van specifieke PowerShell-obfuscatie, het ongewone gebruik van MSC EvilTwin en de infrastructuurpatronen aan de Water Gamayun-groep.

Water Gamayun is een APT-groep die bekend staat om hun verfijnde technieken, waaronder het misbruiken van zero-day kwetsbaarheden, het uitvoeren van proxy-executies via vertrouwde binaries, en het toepassen van geavanceerde obfuscatie om beveiligingsmaatregelen te omzeilen. Hun operaties zijn vaak gericht op strategische inlichtingenverzameling en het verkrijgen van gevoelige gegevens, waarbij ze lange tijd verborgen blijven in systemen.

Deze campagne illustreert opnieuw de geavanceerde tactieken van Water Gamayun, waarbij ze zowel nieuwe als gevestigde kwetsbaarheden exploiteren om door te dringen in netwerken en hun aanwezigheid te verbergen. De Zscaler Threat Hunting heeft hun analyses gebruikt om nieuwe detectiemethoden te ontwikkelen die organisaties kunnen helpen deze geavanceerde dreigingen te identificeren en tegen te gaan.

Vervalsing van Prettier-extensie op VSCode Marketplace levert Anivia Stealer malware af

Een recente aanval via de Visual Studio Code Marketplace heeft duizenden ontwikkelaars wereldwijd getroffen, waaronder in Nederland en België. De kwaadaardige extensie, "prettier-vscode-plus," werd ontdekt op 21 november 2025 en was ontworpen om ontwikkelaars te misleiden door zich voor te doen als de legitieme Prettier-codeformatter. Deze vervalsing, een vorm van merkbedrog, maakte gebruik van de populariteit van Prettier om gebruikers te lokken die op zoek waren naar opmaaktools voor hun code.

De kwaadaardige extensie werd snel geïdentificeerd door de beveiligingsonderzoekers van Checkmarx en binnen vier uur na publicatie van de

Marketplace verwijderd. Toch had de extensie al zes keer gedownload en drie keer geïnstalleerd voordat deze actie werd ondernomen.

De malware die werd verspreid via de vervalste extensie, de Anivia Stealer, richtte zich specifiek op het stelen van inloggegevens en andere gevoelige informatie van Windows-gebruikers. De malware was gericht op het verkrijgen van login-gegevens en privécommunicatie, waaronder WhatsApp-berichten. Het is een voorbeeld van hoe cybercriminelen steeds meer gebruik maken van social engineering en merkbedrog om ontwikkelaars te targeten en waardevolle data te stelen.

Beveiligingsonderzoekers onthulden dat de malware een multi-stage-aanval uitvoerde, waarbij de eerste fase een geavanceerde techniek gebruikte om de payload te verbergen. Deze techniek maakte gebruik van PowerShell-opdrachten om de kwaadaardige code zonder sporen op de computer van het slachtoffer uit te voeren. Dit soort aanvallen maakt gebruik van geavanceerde technieken om beveiligingssystemen te omzeilen en minimaliseert de kans op detectie.

Deze aanval benadrukt de noodzaak voor ontwikkelaars en cybersecurityprofessionals in Nederland en België om alert te blijven op dergelijke bedreigingen, aangezien de aanvallers steeds geavanceerder en doelgerichter te werk gaan. De dreiging van malware zoals de Anivia Stealer is een duidelijk signaal dat iedereen in de techgemeenschap waakzaam moet blijven bij het installeren van extensies en tools, zelfs als ze lijken te komen van vertrouwde bronnen.

Microsoft beschrijft beveiligingsrisico’s van nieuwe agentic AI-functie

Microsoft heeft de beveiligingsrisico’s gepresenteerd van een nieuwe agentic AI-functie, die momenteel wordt getest binnen Copilot Labs. Deze geavanceerde technologie maakt het mogelijk om alledaagse taken, zoals het organiseren van bestanden, het plannen van afspraken en interactie met applicaties, automatisch te laten uitvoeren door digitale agenten. Deze ontwikkeling biedt aanzienlijke productiviteitsvoordelen, maar roept ook belangrijke zorgen op op het gebied van gegevensbeveiliging.

De agentic AI-functie werkt met op de achtergrond actieve digitale agenten die toegang hebben tot gebruikersbestanden en mappen, zoals documenten, downloads en bureaubladbestanden. Microsoft stelt dat deze agenten in een geïsoleerde werkomgeving opereren, wat aanvankelijk een veiligheidsverbetering lijkt. Echter, de betrokkenheid van deze agenten bij meerdere taken vergroot de aanvalsvectoren

voor kwaadwillende actoren. Hackers zouden bijvoorbeeld via kwaadaardige documenten of app-interfaces cross-prompt injectie kunnen toepassen. Dit houdt in dat ze schadelijke opdrachten kunnen versteken aan de agenten, zoals het onbedoeld stelen van gegevens of installeren van malware, zonder dat de gebruiker hier direct van op de hoogte is.

De methode van cross-prompt injectie zorgt ervoor dat malafide inhoud in documenten of app-interfaces kan worden verwerkt als legitieme opdrachten door de agenten. Dit zou kunnen resulteren in ongewilde acties, zoals het wissen van belangrijke bestanden. Microsoft benadrukt dat deze vorm van aanval afwijkt van traditionele malware-aanvallen, aangezien de agenten taken automatisch uitvoeren op basis van ingevoerde instructies. De nadruk ligt dan ook op het verbeteren van toezicht en het strikt beperken van de bevoegdheden van deze digitale agenten om dergelijke aanvallen te voorkomen.

Ondanks de beveiligingsmaatregelen die Microsoft heeft genomen, zoals een manipulatieweerstandige auditlog en gedetailleerde gebruikersautorisatie, blijft waakzaamheid noodzakelijk. Het testprogramma van deze technologie is nog in de beginfase, maar bedrijven die deze technologie in de toekomst willen implementeren, moeten zich bewust zijn van de risico's en ervoor zorgen dat de juiste controlemechanismen aanwezig zijn om de veiligheid te waarborgen.

Albert Heijn waarschuwt voor nepmails die klanten misleiden met gratis foodbox

Albert Heijn heeft klanten gewaarschuwd voor een nieuwe phishingcampagne waarbij oplichters zich voordoen als het bedrijf. De nepmails bieden ontvangers een "gratis foodbox" aan in ruil voor het invullen van een korte enquête. Bij het klikken op de links in de e-mail worden slachtoffers echter gevraagd om hun creditcardgegevens in te vullen, waarmee de oplichters proberen toegang te krijgen tot vertrouwelijke financiële informatie.

Het Nederlandse supermarktbedrijf heeft inmiddels een speciale pagina op haar website geplaatst waarop klanten kunnen leren hoe ze dergelijke phishingpogingen kunnen herkennen. Deze waarschuwing komt te midden van een stijgende trend van online oplichting, waarbij fraudeurs steeds creatiever worden in het misleiden van consumenten. Albert Heijn roept klanten op om verdachte e-mails direct te melden en waarschuwt hen niet in te gaan op dergelijke aanbiedingen. De supermarktketen

benadrukt dat zij nooit persoonlijke gegevens via e-mail vraagt en adviseert klanten om altijd zorgvuldig te controleren of e-mails daadwerkelijk van hen afkomstig zijn.

Dit incident benadrukt de voortdurende dreiging van online oplichting in Nederland en de noodzaak voor consumenten om alert te blijven op digitale bedreigingen. Het is belangrijk dat iedereen zich bewust is van de gevaren van phishing en andere vormen van online fraude.

Politie: 'Cybercrime steeds laagdrempeliger'

Het Cybersecuritybeeld Nederland (CSBN) 2025 toont aan dat de digitale dreiging voor Nederland steeds diverser en complexer wordt. De politie signaleert dat naast burgers en bedrijven, ook overheden steeds vaker doelwit zijn van digitale aanvallen, uitgevoerd door statelijke actoren, cybercriminelen en andere kwaadwillenden. Stan Duijf, verantwoordelijk voor de aanpak van cybercrime binnen de politie, merkt op dat cybercrime door de opkomst van kunstmatige intelligentie (AI) en nieuwe dienstenmodellen steeds toegankelijker wordt voor criminelen, wat aanleiding geeft tot grote zorgen.

De politie is actief in de strijd tegen cybercrime, onder andere door deelname aan internationale operaties zoals de Endgame-operatie. Hierbij werden wereldwijd meerdere malware-aanvallen stopgezet en werden daders rechtstreeks aangesproken. Duijf benadrukt ook het risico dat cybercriminelen vaak gebruik maken van bekende kwetsbaarheden in veelgebruikte software, zoals recentelijk bij Citrix en Microsoft. Veel Nederlandse organisaties gebruiken deze producten, wat het belang van regelmatige software-updates vergroot om schade door aanvallen te voorkomen.

Een ander punt van zorg is de beperkte mogelijkheid van de politie om slachtoffers in het buitenland tijdig te waarschuwen voor cyberaanvallen, door belemmeringen in internationale wetgeving. De politie hoopt dat de wet- en regelgeving op dit gebied wordt aangepast om zo wereldwijd slachtoffers te kunnen informeren.

Groeiende dreiging van transnationale oplichtingscentra onderstreept op de INTERPOL Algemene Vergadering

Op de Algemene Vergadering van INTERPOL werd onlangs een resolutie aangenomen die de groeiende dreiging van transnationale oplichtingscentra

bespreekt. Deze criminele netwerken, die steeds vaker wereldwijd actief zijn, vormen een grote bedreiging voor zowel bedrijven als individuele burgers in Nederland en België. De oplichtingscentra opereren vaak onder valse voorwendselen, zoals lucratieve banen in het buitenland, en gebruiken slachtoffers voor fraude, zoals voice phishing, romance scams en investeringsfraude, vaak gericht op kwetsbare doelgroepen.

Hoewel niet iedereen die werkt in deze centra slachtoffer is van mensenhandel, worden velen tegen hun wil vastgehouden en gedwongen om in deze illegale praktijken mee te werken. De resolutie, voorgesteld door de Republiek Korea, benadrukt ook het gebruik van geavanceerde technologieën door deze criminele netwerken om hun operaties te verhullen en slachtoffers te misleiden.

Een wereldwijde aanpak wordt noodzakelijk geacht, met meer samenwerking tussen landen, het delen van inlichtingen in real-time, en gezamenlijke operaties die door INTERPOL worden ondersteund. INTERPOL pleit ook voor bewustwordingscampagnes, met name gericht op jongeren en werkzoekenden, die vatbaar kunnen zijn voor deze oplichting.

INTERPOL's recente misdaadanalysetrend toont aan dat slachtoffers uit meer dan 60 landen, waaronder Nederland en België, naar deze oplichtingscentra worden gelokt. De operatie van INTERPOL in 2024, die leidde tot de arrestatie van meer dan 2.500 mensen, is een bewijs van de groeiende ernst van deze dreiging.

Nederland en België moeten alert blijven op deze dreiging, aangezien cybercriminaliteit steeds meer internationale dimensies aanneemt. Verdere samenwerking tussen Europese landen is noodzakelijk om de slachtoffers van deze misdaden te beschermen en de criminele netwerken die hiermee gepaard gaan te ontmantelen.

Havenbediende aangehouden na poging tot hacking door drugsbende in Antwerpen

In Antwerpen is een medewerker van een expeditiebedrijf gearresteerd na een poging om de computersystemen van het bedrijf te hacken. De zaak hangt samen met een grotere drugshandelsoperatie die vanuit de Waaslandhaven werkte. De betrokken bende had 495 kilogram cocaïne vanuit Zuid-Amerika naar België proberen te smokkelen, waarbij de drugs verstopt waren in ladingen met bananen en auto's. De poging om het expeditiebedrijf digitaal te infiltreren was onderdeel van de

poging om de operationele kosten van de bende te verlagen. De federale politie heeft de drugs in Panama in beslag genomen, maar de arrestatie van de havenmedewerker benadrukt de steeds verdergaande samenwerking tussen cybercriminaliteit en traditionele criminele netwerken. De aangehouden medewerker wordt verdacht van betrokkenheid bij de hackpoging en het verlenen van ondersteuning aan de criminele organisatie. De zaak werpt licht op de groeiende rol van digitale systemen in georganiseerde misdaadoperaties.

Europese markten stijgen door vredesverwachtingen in Oekraïne en renteverlagingen in de VS, gevolgen voor cybersecurity

De Europese aandelenmarkten vertoonden op 25 november 2025 een stijging, aangedreven door de hoop op een naderend staakt-het-vuren in Oekraïne en de verwachting van renteverlagingen door de Amerikaanse centrale bank. De pan-Europese STOXX 600 index steeg met 0,91%, met name dankzij stijgingen in de materialen- en financiële sectoren. In de bredere context van geopolitieke spanningen, zoals de langdurige oorlog in Oekraïne, kan de onzekerheid invloed hebben op de digitale veiligheid in Europa, met verhoogde risico's van cyberaanvallen tegen vitale infrastructuren.

De Europese markt reageerde positief op de steun van Oekraïne voor een mogelijk vredesakkoord, wat de hoop deed stijgen op stabilisatie in de regio. Dit zou op zijn beurt de druk op Europese landen kunnen verminderen om meer te investeren in defensie en cyberbeveiliging. Investeringen in defensie, zoals de goedkeuring door het Europees Parlement van een 1,5 miljard euro programma, kunnen ook gevolgen hebben voor de cyberweerbaarheid van landen in de EU, inclusief Nederland en België, die zich voorbereiden op potentiële digitale aanvallen door geopolitieke conflicten.

Ondanks de economische voordelen van dergelijke vredesverwachtingen, moeten bedrijven in Nederland en België waakzaam blijven voor mogelijke verhogingen in cyberdreigingen, vooral wanneer landen hun militaire en defensieve capaciteiten uitbreiden. De stijging van aandelen in de Europese defensiesector, zoals die van bedrijven die verbonden zijn aan luchtverdediging en cybersecurity, kan duiden op een bredere trend van versterkte digitale defensie.

De verwachting van renteverlagingen in de VS, die de markten verder positief beïnvloeden, kan tegelijkertijd de kans vergroten op toenemende cyberrisico's door

veranderende economische omstandigheden wereldwijd. De Federal Reserve blijft waakzaam voor tekenen van economische vertraging, wat zowel de wereldmarkten als de digitale dreigingen kan beïnvloeden.

Logius reageert op overname Solvinity: DigiD blijft Nederlands

Logius, de instantie die verantwoordelijk is voor het beheer van het digitale identificatiesysteem DigiD, heeft gereageerd op de voorgenomen overname van het Nederlandse cloudbedrijf Solvinity door een Amerikaans bedrijf. Deze overname heeft in Nederland geleid tot bezorgdheid, aangezien DigiD op servers draait die door Solvinity worden beheerd. Logius benadrukt echter dat DigiD Nederlands blijft en dat de veiligheid van de gegevens van Nederlandse burgers gewaarborgd blijft, ondanks de wijziging in de eigendom van het bedrijf.

Direct na de aankondiging van de overname is een impactanalyse gestart om te beoordelen of de overname risico's met zich meebrengt voor de dienstverlening, beveiliging en privacy. Logius heeft aangegeven dat als de analyse een onacceptabel risico aan het licht brengt, er onmiddellijk maatregelen getroffen zullen worden. Het demissionaire kabinet heeft ook een onderzoek gestart naar de juridische en operationele gevolgen van de overname en de noodzakelijke goedkeuringen door toezichthouders.

De zorgen over de veiligheid van persoonsgegevens worden versterkt door de mogelijkheid dat, indien de servers van Solvinity onder Amerikaanse wetgeving vallen, de Amerikaanse overheid toegang zou kunnen krijgen tot gegevens die in de Verenigde Staten zijn opgeslagen. Dit roept vragen op over data-soevereiniteit en de bescherming van persoonsgegevens volgens de Europese privacywetgeving.

Logius stelt echter dat het platform strikte eisen blijft stellen aan de veiligheid en continuïteit van DigiD, en dat de overname enkel kan doorgaan nadat alle juridische en contractuele voorwaarden zijn goedgekeurd. Het is nog afwachten of de overname daadwerkelijk doorgaat, en welke gevolgen dit zal hebben voor de digitale veiligheid van Nederlandse en Belgische burgers.

Veel Nederlanders overschatten zichzelf bij het herkennen van online oplichting

Uit recent onderzoek van het ministerie van Justitie en Veiligheid blijkt dat veel Nederlanders zichzelf overschatten als het gaat om het herkennen van online oplichting. Het onderzoek, uitgevoerd onder achttienhonderd mensen, betrof het beoordelen van echte en neppe digitale uitingen. Deelnemers kregen verschillende voorbeelden te zien, waaronder e-mails, webshopberichten, video's, WhatsApp- en sms-berichten. Bijna de helft van de ondervraagden gaf aan dat zij online oplichting goed konden herkennen, maar slechts 10% bleek in staat om alle neppe uitingen correct te identificeren.

Daarnaast was er een opvallend verschil tussen de zelfbeoordeling en de werkelijke uitkomsten. Zo dacht 42% van de deelnemers meer uitingen goed te hebben beoordeeld dan in werkelijkheid het geval was. Het ministerie zal de resultaten van dit onderzoek gebruiken voor de campagne "Laat je niet Interneppen", die gericht is op het verhogen van de bewustwording rondom online fraude. De resultaten benadrukken het belang van continue educatie en waakzaamheid tegen steeds geavanceerdere vormen van digitale misleiding.

Europese lidstaten nemen omstreden wet tegen online kindermisbruik aan

Een meerderheid van de Europese lidstaten heeft recent een wetsvoorstel goedgekeurd dat moet helpen bij de bestrijding van online kindermisbruik. Het doel van de wet is om de verspreiding van beelden van kindermisbruik te stoppen door communicatiediensten te verplichten berichten van gebruikers te scannen. Dit voorstel stuitte echter op veel tegenstand vanwege de bezorgdheid over de inbreuk op de vertrouwelijkheid van communicatie. In plaats van een verplichting, is het scannen van berichten nu optioneel voor app-ontwikkelaars, die zelf kunnen beslissen of ze berichten kunnen lezen als dat noodzakelijk wordt geacht. Deze wijziging in het voorstel heeft de steun van een ruime meerderheid van de lidstaten, hoewel Nederland zich tegen de wet heeft uitgesproken, uit vrees dat dit alsnog kan leiden tot verplichte scantechnologie.

De wet bevat ook de oprichting van een Europees meldpunt voor kindermisbruik, waarmee lidstaten en techbedrijven ondersteund worden in het uitvoeren van de wet. Dit meldpunt biedt ook slachtoffers van kindermisbruik de mogelijkheid om hun gevallen te melden, waarna informatie gedeeld kan worden met nationale politiediensten en Europol. De wet zal pas in werking treden nadat het Europees Parlement nog een stemronde heeft gehouden.

Europarlement steunt voorstellen voor strengere bescherming van minderjarigen op sociale media

Het Europees Parlement heeft onlangs een voorstel goedgekeurd dat voorziet in strengere maatregelen ter bescherming van minderjarigen op sociale media. Het plan beoogt onder andere het vaststellen van een minimumleeftijd van 16 jaar voor het gebruik van sociale mediaplatforms. Voor kinderen tussen de 13 en 16 jaar zou het gebruik van deze platforms alleen mogelijk zijn met expliciete toestemming van hun ouders of verzorgers. Dit voorstel is bedoeld om de digitale veiligheid van minderjarigen te waarborgen en hen te beschermen tegen de gevaren van verslavende appontwerpen en onveilige online omgevingen.

Daarnaast wordt er een oplossing voorgesteld waarbij de leeftijd van gebruikers geverifieerd kan worden via een zogenaamde Europese portemonnee, waarin de digitale identiteit van Europese burgers wordt opgeslagen. Er wordt gewerkt aan een app voor leeftijdsverificatie, hoewel de Europarlementariërs er nadrukkelijk op aandringen dat de privacy van minderjarigen gewaarborgd moet blijven. Het parlement vraagt om maatregelen die jonge gebruikers beschermen tegen gerichte advertenties, beïnvloedingscampagnes via influencers en verslavende ontwerptechnieken zoals eindeloos scrollen en automatisch afspelen van video's.

Ondanks de steun voor de voorstellen in het parlement, zijn de voorgestelde maatregelen nog niet definitief. De Europese Commissie en de lidstaten moeten zich nog over de resolutie buigen, en het is niet zeker of alle voorgestelde maatregelen daadwerkelijk in wetgeving zullen worden omgezet.

Hack the Government: Ethische hackers proberen kwetsbaarheden in Belgische overheidssystemen te vinden

In België nemen 71 ethische hackers en studenten deel aan een twee weken durende uitdaging om de veiligheid van de systemen van de Belgische overheid te testen. Dit initiatief, genaamd "Hack the Government", wordt voor de tweede keer georganiseerd door het Centrum voor Cybersecurity (CCB). Het doel van deze ethische hackathon is om kwetsbaarheden in de digitale infrastructuur van de overheid te identificeren voordat kwaadwillende hackers deze kunnen misbruiken. De deelnemers richten zich op de websites, software en contactformulieren van

verschillende overheidsinstellingen, waaronder de federale politie, defensie en andere overheidsdiensten.

Het CCB heeft het evenement opgezet om de digitale weerbaarheid van de overheid te versterken. Tot nu toe hebben de ethische hackers al 81 veiligheidsrisico's ontdekt. Dit is een belangrijk proces, aangezien de kwetsbaarheden die door de hackers worden gevonden, vervolgens snel worden opgelost om mogelijke schade te voorkomen. Het initiatief benadrukt de waarde van ethisch hacken, dat sinds februari 2023 legaal is in België. Ethische hackers mogen nu, zonder voorafgaande toestemming van organisaties, de systemen testen en moeten kwetsbaarheden binnen 72 uur melden.

De hackathon bestaat uit 32 professionele ethische hackers en 39 studenten, die de kans krijgen om in te breken op systemen die normaal gesproken voor hen niet toegankelijk zijn. Dit biedt hen niet alleen unieke ervaring, maar draagt ook bij aan het verbeteren van de beveiliging van overheidsystemen. Vorig jaar werden er 84 kwetsbaarheden ontdekt, waaronder een 'zero-day' kwetsbaarheid, die een wereldwijd effect had op de veiligheid van de betrokken producten. De resultaten van dit jaar worden naar verwachting nog meer kwetsbaarheden aan het licht brengen, wat de noodzaak onderstreept om constant te blijven werken aan de digitale beveiliging van kritieke systemen.

Dit soort initiatieven speelt een cruciale rol in het versterken van de digitale weerbaarheid tegen de steeds toenemende dreigingen in cyberspace, met name van geavanceerde hackersgroepen zoals die uit Rusland, die ook gericht zijn op Belgische doelwitten. Het CCB blijft zich inzetten voor de bevordering van ethisch hacken om de nationale digitale infrastructuur te beschermen tegen cyberaanvallen.

EU-lidstaten stemmen in met voorstel voor vrijwillige chatcontrole en leeftijdsverificatie

Op 26 november 2025 hebben de EU-lidstaten een akkoord bereikt over een voorstel van de Deense EU-voorzitter dat bedrijven de mogelijkheid biedt om vrijwillig chatcontrole door te voeren. Dit voorstel bevat een reviewclausule, waarmee het in de toekomst verplicht kan worden gesteld. Daarnaast verplicht het voorstel platforms om online leeftijdsverificatie te implementeren en voorziet het in de oprichting van een nieuw Europees centrum ter ondersteuning van de regelgeving. Nationale toezichthouders zullen ook worden aangesteld om de naleving van deze regels te

controleren. Zij hebben de bevoegdheid om verdere maatregelen van techbedrijven te eisen om de verspreiding van misbruikmateriaal tegen te gaan.

Dit voorstel volgt op eerdere pogingen van Denemarken om verplichte chatcontrole door te voeren, maar na tegenstand besloot het land een compromisvoorstel te doen, waarbij chatcontrole in eerste instantie vrijwillig is. Dit betreft een uitzondering op de ePrivacy Verordening die begin volgend jaar afloopt. De Europese Commissie heeft langere tijd gepleit voor verplichte chatcontrole voor techbedrijven om de inhoud van berichten te monitoren, vooral om misbruik zoals kinderporno tegen te gaan. De lidstaten hebben nu een positie ingenomen, waardoor de onderhandelingen met het Europees Parlement kunnen beginnen. Het Europees Parlement had in 2023 al een positie ingenomen over het voorstel.

De goedkeuring van het voorstel heeft geleid tot felle kritiek van privacyvoorvechters. Voormalig Europarlementariër Patrick Breyer uitte zijn bezorgdheid over de manier waarop het voorstel zonder voldoende discussie werd aangenomen, en benadrukte dat het risico van grootschalige surveillance en de aantasting van anonimiteit te groot is. Nederland had zich aanvankelijk van stemming willen onthouden, maar de Tweede Kamer vroeg de regering om tegen het voorstel te stemmen, wat demissionair minister Van Oosten heeft bevestigd.

Scattered Lapsus$ Hunters: een hacker-groep die wereldwijd voor opschudding zorgt

De hacker-groep Scattered Lapsus$ Hunters (SLSH) heeft wereldwijd voor opschudding gezorgd door haar datalekken en afpersingscampagnes tegen grote bedrijven. De groep, die uit een combinatie van de hackinggroepen Scattered Spider, LAPSUS$ en ShinyHunters zou bestaan, heeft bedrijven over de hele wereld aangevallen, met als doel gevoelige gegevens te stelen en te extorteren.

In mei 2025 lanceerde de groep een sociale-engineeringcampagne waarbij ze gebruik maakten van voice phishing om toegang te verkrijgen tot de Salesforce-accounts van meerdere bedrijven. Later werd een datalekportal opgezet, die dreigde met het publiceren van gestolen gegevens van bedrijven zoals Toyota, FedEx, Disney en UPS. Deze aanvallen geven aan hoe SLSH gebruik maakt van geavanceerde aanvalstechnieken om hun slachtoffers onder druk te zetten.

Afgelopen week werd bekend dat de groep nu ook hun eigen ransomware-as-a-service-aanbod heeft gelanceerd, genaamd ShinySp1d3r. Dit geeft aan dat SLSH

niet alleen gebruik maakt van bestaande malware, maar ook haar eigen kwaadaardige software ontwikkelt. Dit type dienstverlening stelt andere cybercriminelen in staat om ransomware-aanvallen uit te voeren met minimale technische kennis, wat de dreiging van ransomware verder vergroot.

De beheerder van de groep, bekend onder de naam Rey, is inmiddels geïdentificeerd en heeft zijn identiteit bevestigd na contact van de journalist Brian Krebs. Rey heeft in het verleden actief deelgenomen aan verschillende cybercriminaliteitsforums, waaronder BreachForums, waar gestolen data werd verhandeld. Ondanks zijn betrokkenheid bij de groep, heeft Rey aangegeven te willen stoppen met cybercriminaliteit en zelfs samen te werken met wetshandhavers. De komende tijd zal blijken of deze belofte werkelijkheid wordt.

De opkomst van groepen zoals Scattered Lapsus$ Hunters benadrukt de toenemende dreiging van gesofisticeerde cybercriminaliteit en de noodzaak voor bedrijven en overheden om waakzaam te blijven tegen deze wereldwijde bedreigingen.