Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

06-11-2025:

Schiermonnikoog deelde per abuis BSN’s; data op gehackt Omrin-systeem

De gemeente Schiermonnikoog heeft in 2024 een bestand met namen, adressen en burgerservicenummers van alle inwoners en eigenaren van recreatiewoningen gedeeld met afvalverwerker Omrin. Het bestand diende voor de introductie van nieuwe containerstags, maar bevatte meer gegevens dan noodzakelijk. Bij de ransomwareaanval op Omrin, gemeld op 13 oktober 2025, kwam het bestand op een gecompromitteerde schijf terecht en is mogelijk door criminelen ingezien. Omrin stelt dat het bestand destijds is aangepast, maar dat een kopie is blijven staan. De burgemeester noemde de situatie “vervelend” en ziet geen datalek; er is geen melding gedaan bij de Autoriteit Persoonsgegevens. Binnen de gemeente onderzoekt een privacyexpert het incident. Tijdens de storing waren kringloopwinkels tijdelijk gesloten, was de klantenservice telefonisch onbereikbaar en gaf de Afvalapp problemen; deze dienstverlening is inmiddels hersteld. De casus roept vragen op over dataminimalisatie, verantwoordingsplicht en meldplicht onder de AVG.

Duitsland versterkt aanpak hybride dreiging met nieuw veiligheidsorgaan

Duitsland heeft een Nationaal Veiligheidsberaad opgericht om de toenemende hybride dreigingen vanuit Rusland beter te coördineren. Het beraad brengt vertegenwoordigers van verschillende ministeries, veiligheidsdiensten en de private sector samen. De nadruk ligt op het ontwikkelen van een gezamenlijk actieplan om cyberaanvallen, desinformatie, sabotage en droneactiviteit rond gevoelige locaties te bestrijden. Aanleiding is de toename van vermoedelijk Russische drones boven Europa en de zorgen over kwetsbaarheden in kritieke infrastructuur. Het parlement heeft eerder al ingestemd met een wetswijziging die politie toestaat drones neer te halen wanneer deze een directe dreiging vormen. Tijdens de eerste bijeenkomst besprak het beraad ook afhankelijkheden van strategische grondstoffen en de noodzaak om de aanvoerketens hiervan te versterken. Daarnaast zal het beraad zich richten op spionage en bescherming van kritieke infrastructuur. Oekraïne heeft Duitsland bedankt voor aanvullende luchtafweersystemen.

NoName richt zich op Belgische websites met DDoS-aanvallen

Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

Op 5 november 2025 meldde de cyberbeveiligingsgroep NoName dat het meerdere websites in België had aangevallen via DDoS-aanvallen. De getroffen organisaties omvatten grote bedrijven en publieke instellingen zoals C.P. Bourg, Scarlet, Telenet, Proximus en de stad Comines-Warneton. De aanvallen verstoren de normale werking van deze websites, waarbij de betrokkenen druk bezig zijn met herstel en mitigatie van de dreiging. NoName heeft eerder soortgelijke aanvallen uitgevoerd en blijft een prominente bedreiging voor de Belgische digitale infrastructuur. De zaak benadrukt de groeiende trend van georganiseerde DDoS-campagnes die gericht zijn op belangrijke sectoren en overheidsinstellingen.

Proximus, Scarlet en UZ Gent getroffen door cyberaanval, beperkte gevolgen

Op woensdag 5 november 2025 voerden de pro-Russische hackers van NoName057 een DDoS-aanval uit op de websites van telecomproviders Proximus en Scarlet, evenals op het Universitair Ziekenhuis Gent (UZ Gent). De aanvallen hadden als doel de websites te overbelasten door massale verzoeken te sturen, waardoor deze tijdelijk onbereikbaar werden. Ondanks de overbelasting van de websites zijn er geen gegevens gestolen en bleven de diensten van Proximus en Scarlet operationeel. Het UZ Gent meldde dat er tussen 10 en 11 uur lichte storingen waren, maar dit had geen invloed op de zorgverlening. DDoS-aanvallen zijn in België relatief vaak, met grotere aanvallen op overheidsinstellingen en publieke diensten, zoals in 2023 en 2024. De hackersgroep richt zich op landen die Oekraïne ondersteunen, zoals blijkt uit een boodschap op sociale media.

SmudgedSerpent' hackers richten zich op beleidsdeskundigen

De onbekende groep cybercriminelen 'SmudgedSerpent' heeft tussen juni en augustus 2025 meerdere cyberaanvallen uitgevoerd op academici en experts in buitenlands beleid, gericht op de situatie tussen Iran en Israël. De aanvallers gebruikten social engineering-technieken, zoals valse e-mails die eruit zagen als communicatie van invloedrijke Amerikaanse beleidsinstellingen. Ze probeerden zo slachtoffers te lokken naar schadelijke links die schadelijke software in de vorm van een MSI-installer verschaften. Deze software leek op Microsoft Teams, maar installeerde in werkelijkheid Remote Monitoring and Management (RMM) software zoals PDQ Connect. De aanvallers verzonden e-mails die zich voordeden als prominente figuren in de buitenlandse beleidswereld en probeerden zo vertrouwelijke

informatie van hun doelwitten te verkrijgen. Het gebruik van gezondheid-gerelateerde domeinen en OnlyOffice wijst op een verbinding met eerdere aanvallen van Iraanse cybergroepen. Dit duidt op een evolutie in de samenwerking tussen Iraanse inlichtingendiensten en cybereenheden.

VS waarschuwt voor actief misbruik van kritiek lek in CentOS Web Panel

Het Amerikaanse cyberagentschap CISA meldt dat een kritiek beveiligingslek in CentOS Web Panel actief wordt misbruikt. Het lek, geregistreerd als CVE-2025-48703, maakt het mogelijk dat een ongeauthenticeerde aanvaller op afstand code uitvoert zodra een geldige non-root gebruikersnaam bekend is. Volgens de onderzoeker waren in mei meer dan tweehonderdduizend installaties via Shodan zichtbaar, wat de potentiële blootstelling aanzienlijk maakt. De kwetsbaarheid heeft een impactscore van 9.0 en is verholpen in versie 0.9.8.1205 die afgelopen juni beschikbaar kwam. CISA bevestigt dat aanvallen plaatsvinden, maar verstrekt geen technische details. In juli meldden gebruikers al misbruik. Amerikaanse overheidsinstellingen die het panel gebruiken moeten uiterlijk 25 november de beveiligingsupdate installeren. Het bericht onderstreept de noodzaak om systemen die internetgericht draaien tijdig te patchen, vooral wanneer er publiek bewijs is van actieve exploitatie.

Waarschuwing: Elastic Cloud Enterprise Privilege Escalation Issue – Patch Onmiddellijk!

Er is een kwetsbaarheid ontdekt in Elastic Cloud Enterprise (ECE) versies 3.8.3 en 4.0.3 die kan leiden tot privilege escalation. De kwetsbaarheid, gemeld onder CVE-2025-37736, stelt een kwaadwillende met leesrechten in staat om API-eindpunten te benaderen die normaal gesproken niet toegankelijk zouden moeten zijn. Dit kan leiden tot ongeautoriseerde acties, zoals het aanmaken of verwijderen van gebruikers, het beheren van authenticatiesleutels en het beheren van serviceaccounts. Er is op dit moment geen bewijs van misbruik, maar het wordt sterk aanbevolen om de kwetsbaarheid te verhelpen door de betreffende updates onmiddellijk te installeren. Systemen moeten ook nauwlettend worden gemonitord om verdachte activiteiten te detecteren en snel te kunnen reageren bij een mogelijke inbreuk.

AI Engine-plugin voor WordPress stelt 100.000 sites bloot aan privilege-escalatie-aanvallen

Een kritieke kwetsbaarheid in de AI Engine-plugin voor WordPress heeft meer dan 100.000 actieve installaties blootgesteld aan privilege-escalatie-aanvallen. De kwetsbaarheid, geregistreerd als CVE-2025-11749, maakt het mogelijk voor onbevoegde aanvallers om bearer-tokens te extraheren en volledige administratieve controle over kwetsbare websites te verkrijgen. Deze zwakte werd ontdekt door beveiligingsonderzoeker Emiliano Versini en verantwoord gerapporteerd via het Wordfence Bug Bounty Programma. De kwetsbaarheid bevindt zich in de 'No-Auth URL'-instelling van de plugin, die tokens openbaar maakt via de /wp-json/ REST API. Door deze blootstelling kunnen aanvallers zich authentiseren en beheerdersrechten verkrijgen, waarmee ze kwaadaardige plugins kunnen uploaden, inhoud kunnen wijzigen of bezoekers naar schadelijke websites kunnen leiden. De ontwikkelaar van de plugin heeft een patch uitgebracht in versie 3.1.4 om de kwetsbaarheid te verhelpen. Gebruikers wordt aangeraden hun tokens onmiddellijk te vernieuwen.

Aantal ransomware-aanvallen op Europese organisaties neemt toe door inzet AI-tools

Ransomware-aanvallen op Europese organisaties nemen sinds 2024 aanzienlijk toe, met 2.100 slachtoffers die tot nu toe zijn geregistreerd, wat een stijging van 13% betekent ten opzichte van het voorgaande jaar. Het VK, Duitsland, Italië, Frankrijk en Spanje worden het zwaarst getroffen, vooral in de sectoren productie, professionele diensten en technologie. Een belangrijke factor in de stijging van deze aanvallen is de integratie van kunstmatige intelligentie (AI) door cybercriminelen. AI wordt ingezet voor het verfijnen van phishing-aanvallen, het genereren van polymorfe code en het uitvoeren van geautomatiseerde verkenning van potentiële doelen. Daarnaast maken aanvallers gebruik van de Europese privacywetgeving om slachtoffers onder druk te zetten tijdens losgeldonderhandelingen. Diefstal van inloggegevens en het gebruik van niet-beheerde systemen zijn veelgebruikte technieken om ransomware te verspreiden. De inzet van AI maakt de aanvallen steeds moeilijker te detecteren en te stoppen.

Badcandy infecties bij Cisco apparaten met 103 in Nederland en 13 in België !

Wereldwijd zijn ruim veertienduizend Cisco routers en switches besmet met de Badcandy backdoor. Uit onderzoek van Shadowserver blijkt dat de infecties voortkomen uit misbruik van CVE-2023-20198, een ernstig lek in de webinterface van IOS XE waarmee ongeauthenticeerde aanvallers een privileged account kunnen aanmaken en controle over het apparaat krijgen. Het lek wordt gebruikt om de backdoor te plaatsen, waarna aanvallers het lek lokaal dichten om verdere exploitatie te voorkomen. De backdoor en de toegepaste patch verdwijnen bij een reboot, maar toegang kan blijven bestaan via gestolen inloggegevens of aanvullende kwetsbaarheden. Het aantal besmette apparaten daalde de afgelopen maanden van achttienduizend naar veertienduizend. In Nederland zijn 103 apparaten geïnfecteerd en in België 13. De grootste aantallen worden waargenomen in Mexico en de Verenigde Staten. De situatie laat zien dat ongepatchte systemen langdurig risico's veroorzaken.

Google waarschuwt voor nieuwe AI-gestuurde malwarefamilies

Google's Threat Intelligence Group (GTIG) heeft een verschuiving in cyberdreigingen geïdentificeerd, waarbij aanvallers kunstmatige intelligentie (AI) gebruiken om nieuwe malwarefamilies te creëren. Deze malware, zoals de "PromptFlux" dropper en de "PromptSteal" miner, maken gebruik van grote taalmodellen (LLM's) zoals Gemini, waarmee ze zich dynamisch kunnen aanpassen tijdens uitvoering. Dit stelt hen in staat om hun gedrag in real-time te wijzigen, wat traditionele malwaretechnieken overtreft. De techniek, genaamd "just-in-time" zelfmodificatie, maakt de malware moeilijk te detecteren en te blokkeren. Google ontdekte ook andere AI-gedreven malware zoals FruitShell en QuietVault, die gebruik maken van AI om commando's uit te voeren en gegevens te stelen. De opkomst van AI-tools op ondergrondse marktplaatsen vergroot de toegang tot geavanceerde cyberaanvallen, wat de dreiging verder verhoogt. Google heeft de toegang tot de gebruikte AI-modellen in sommige gevallen geblokkeerd en veiligheidsmaatregelen aangescherpt.

Gootloader malware keert terug met nieuwe technieken

De Gootloader-malware is terug na een pauze van zeven maanden en heeft zijn strategieën aangepast. Deze malware wordt verspreid via websites die door aanvallers zijn gecompromitteerd of gecontroleerd, en maakt gebruik van zoekmachineoptimalisatie (SEO) om valse websites te promoten die schadelijke

bestanden aanbieden. In eerdere campagnes werden valse fora gebruikt om malafide document sjablonen aan te bevelen, maar nu worden websites gepromoot die zogenaamd gratis juridische documenten aanbieden. Gebruikers die op een "Get Document" knop klikken, worden misleid om een schadelijke ZIP-archief te downloaden dat een JavaScript-bestand bevat. Bij openen van dit bestand worden aanvullende malwarepayloads geïnstalleerd, zoals Cobalt Strike en backdoors, waarmee aanvallers toegang krijgen tot netwerken. De onderzoekers wijzen erop dat deze nieuwe variant technieken gebruikt die het voor automatische analysetools moeilijker maken om de dreiging te detecteren.

Verkoop van EU-creditcards op de zwarte markt

Er wordt melding gemaakt van de vermeende verkoop van EU-creditcards op de zwarte markt. Deze kaarten zouden te koop worden aangeboden door cybercriminelen op diverse darknetmarktplaatsen. De verkoop betreft mogelijk gestolen gegevens van Europese consumenten, wat de kans op fraude verhoogt. Het aanbieden van deze gegevens op het darkweb is een onderdeel van grotere cybercriminaliteitsnetwerken die actief zijn in het uitvoeren van financieel gerelateerde misdaden. Dergelijke activiteiten kunnen leiden tot aanzienlijke financiële schade voor de betrokken slachtoffers. Deze zaak benadrukt de voortdurende dreiging van identiteitsdiefstal en het misbruik van persoonlijke informatie, met een groeiend aantal incidenten die via online marktplaatsen worden verhandeld. Cybersecurity-experts adviseren bedrijven en individuen om waakzaam te zijn en beveiligingsmaatregelen te treffen tegen deze vormen van digitale fraude.

Cloudflare verwijdert Aisuru-botnet van Top Domeinenlijst

Cloudflare heeft onlangs domeinen die zijn gekoppeld aan het Aisuru-botnet, verwijderd uit hun publieke lijst van meest gevraagde websites. Het Aisuru-botnet, dat in 2024 werd ontdekt, maakt gebruik van duizenden gehackte IoT-apparaten, zoals routers en beveiligingscamera’s, en is sinds zijn ontstaan aanzienlijk gegroeid. Aisuru wordt ingezet voor DDoS-aanvallen van recordgrootte. De botnetbeheerders maakten gebruik van Cloudflare’s DNS-service om hun malafide domeinen hoog in de ranking te krijgen, wat bezorgdheid opriep over de betrouwbaarheid van deze lijst. Cloudflare reageerde door de malafide domeinen gedeeltelijk te redacteren en hun systeem aan te passen om dergelijke manipulaties te voorkomen. De meeste DNS-

aanvragen naar deze domeinen kwamen uit de VS, waar Aisuru zijn grootste infrastructuur heeft. Cloudflare werkt nu aan verbeteringen om te voorkomen dat dergelijke schadelijke activiteiten de lijst opnieuw verstoren.

RondoDox-botnet verhoogt dreiging met 650% meer exploits gericht op bedrijven

Het RondoDox-botnet heeft zijn aanvalsmogelijkheden drastisch uitgebreid, met een toename van 650% in exploitatiecapaciteiten. Dit markeert een verschuiving van de oorspronkelijke variant, die zich vooral richtte op DVR-systemen, naar een meer geavanceerde versie (RondoDox v2) die meer dan 75 exploitatievectoren bevat. Deze nieuwe variant richt zich op een breed scala aan kwetsbare apparaten, van legacy routers tot moderne enterprise-toepassingen. De aanvallen, die in oktober 2025 werden gedetecteerd via honeypots, kenmerkten zich door een groot aantal exploits die snel na elkaar werden uitgevoerd. Het botnet maakt gebruik van een geavanceerd infrastructuurdesign dat moeilijk te blokkeren is en voegt malware toe aan systemen om resourcegebruik te monopolizeren en andere schadelijke software te elimineren. Dit vergroot de dreiging voor zowel IoT-infrastructuren als bedrijfsomgevingen.

Tycoon 2FA Phishing Kit richt zich op Microsoft 365 en Gmail-accounts

Het Tycoon 2FA phishing-kit is een geavanceerd platform dat sinds zijn lancering in augustus 2023 actief is en specifiek is ontworpen om bescherming van twee- en meerfactorauthenticatie te omzeilen bij Microsoft 365- en Gmail-accounts. Deze dreiging maakt gebruik van een 'Adversary-in-the-Middle'-aanval, waarbij reverse proxy-servers overtuigende phishingpagina’s hosten die legitieme inloginterfaces repliceren en gebruikersgegevens in realtime onderscheppen. Het Tycoon 2FA-kit is bijzonder gevaarlijk omdat het zelfs de codes voor twee-factorauthenticatie steelt. Dit wordt mogelijk gemaakt door het implementeren van complexe JavaScript-executieketens en het gebruik van meerdere verdedigingsmechanismen die gericht zijn op het omzeilen van detectie door automatische beveiligingstools. Het phishing-aanvalsnetwerk verspreidt zich via schadelijke documenten, e-mailbijlagen en cloudopslagplatforms zoals Amazon S3, Canva en Dropbox, waardoor het moeilijker wordt om de dreiging te identificeren.

Silent Lynx APT voert nieuwe aanvallen uit op overheidswerknemers

De APT-groep Silent Lynx blijft haar spionagecampagne tegen overheidsinstanties in Centraal-Azië voortzetten. De groep is sinds 2024 actief en heeft zich gepositioneerd als een bedreiging door overheidsmedewerkers te targeten via phishingcampagnes, waarbij ze zich voordoen als overheidsfunctionarissen. Het belangrijkste aanvalsmiddel zijn vervalste e-mails met kwaadaardige bijlagen, vaak in verband met valse topontmoetingen. Twee campagnes in 2025 richtten zich op diplomatieke entiteiten in verband met de voorbereiding van een Rusland-Azerbeidzjan top en een tweede, gericht op China-Centraal-Aziatische relaties. De aanvallen maken gebruik van PowerShell-scripts en andere kwaadaardige software om inloggegevens en gevoelige informatie te stelen. Silent Lynx past een geavanceerde infectieketen toe, waarbij een onschadelijke RAR-bestand wordt gebruikt om de schadelijke payload te verspreiden. De infecties zijn zorgvuldig gecoördineerd met geopolitieke belangen als drijfveer, niet financieel gewin.

DragonForce Cartel Onstaat Door Gelekte Broncode van Conti v3 Ransomware

De DragonForce groep, actief sinds 2023, heeft zich gepositioneerd als een ransomware-cartel, voortgekomen uit de openbaar gelekte source code van Conti v3. Oorspronkelijk een ransomwaregroep die de LockBit 3.0 builder gebruikte, schakelde DragonForce in 2025 over naar een eigen Conti v3 code, wat hen strategische voordelen en geavanceerde technische capaciteiten gaf. In plaats van te functioneren als een traditionele groep, opereert DragonForce nu als een netwerk van affiliates, die in ruil voor 80% van de winst gebruik kunnen maken van de infrastructuur van het cartel. Het cartel biedt op maat gemaakte encryptor-tools, geautomatiseerde uitrolsystemen en ondersteuning voor meerdere platforms. Ze werken samen met Scattered Spider, een groep die zich richt op social engineering en MFA-bypassing. DragonForce heeft zich gepositioneerd als een krachtige speler in de ransomware-industrie, met meer dan 200 slachtoffers in sectoren zoals retail en luchtvaart.

Internationale actie tegen wereldwijde creditcardfraude

Tijdens een gecoördineerde internationale politieoperatie zijn achttien verdachten gearresteerd die betrokken zouden zijn bij grootschalige creditcardfraude. Volgens Europol en Eurojust gaat het om drie criminele netwerken die wereldwijd ruim 4,3

miljoen slachtoffers maakten in 193 landen. De fraude, goed voor een totale schade van meer dan 300 miljoen euro, vond plaats tussen 2016 en 2021. De verdachten gebruikten gestolen creditcardgegevens om fictieve abonnementen af te sluiten op websites voor pornografie, dating en streaming. Deze sites waren bewust buiten zoekmachines gehouden en gebruikten vage omschrijvingen bij maandelijkse afschrijvingen van circa vijftig euro per slachtoffer. De bendes zouden bovendien hebben samengewerkt met medewerkers van vier Duitse betalingsverwerkers die hen tegen betaling toegang gaven tot de betaalinfrastructuur. In totaal worden 44 personen verdacht en is 35 miljoen euro aan tegoeden in beslag genomen.

Cyberaanval veroorzaakt forse winstdaling bij Marks and Spencer

Marks and Spencer meldt een sterke daling van de winst over de eerste helft van het jaar nadat een cyberaanval het online verkoopkanaal langdurig stillegde. De winst vóór belastingen daalde met ruim de helft en de online verkoop van mode en woonartikelen zakte aanzienlijk doordat de winkel zes weken lang geen bestellingen kon verwerken. De logistieke systemen raakten eveneens verstoord, wat leidde tot lege schappen. Het bedrijf wijt de aanval aan menselijke fout en schat het verlies in omzet op meer dan driehonderd miljoen pond, waarvan een deel werd gecompenseerd door een verzekeringsuitkering. De aanval had ook gevolgen voor klantgegevens die konden zijn buitgemaakt. Andere Britse winkels zoals Harrods en Co op kregen te maken met vergelijkbare aanvallen. Volgens deskundigen versnelt de inzet van generatieve ai de dreigingsontwikkeling en blijft versterking van digitale weerbaarheid noodzakelijk.

Avans verbiedt AI in Outlook wegens risico op datalekken

Avans Hogeschool heeft het gebruik van de Outlook functies Copilot en Samenvatten verboden voor iedereen met een Avans account en voor externe verwerkers van Avans gegevens. De instelling wijst op het risico dat via deze AI functies persoonsgegevens en bedrijfsgevoelige informatie worden verwerkt en mogelijk lekken. Volgens Avans kunnen de knoppen op dit moment niet centraal worden uitgeschakeld vanwege de manier waarop Microsoft de functies aanbiedt; het uitschakelen zou andere essentiële onderdelen van Outlook kunnen beïnvloeden. Daarom vraagt de hogeschool medewerkers en studenten om de functies niet te gebruiken en zorgvuldig met e mail te blijven omgaan. Avans werkt aan formeel

beleid om de regels vast te leggen en gaat in gesprek met Microsoft om naar een structurele oplossing te zoeken. Totdat hierover duidelijkheid bestaat, blijft het gebruik van de AI functies in Outlook binnen de organisatie niet toegestaan.

Kifid: Revolut hoeft schade door bankhelpdeskfraude niet te vergoeden

Een klant van Revolut die slachtoffer werd van bankhelpdeskfraude krijgt geen vergoeding voor de schade van 12.000 euro. Volgens het financiële klachteninstituut Kifid heeft het slachtoffer grof nalatig gehandeld door beveiligingscodes via WhatsApp te delen en waarschuwingen van de bank te negeren. De oplichters deden zich telefonisch en via berichten voor als bankmedewerkers en overtuigden het slachtoffer om geld “veilig te stellen”. Daarbij werden meerdere betalingen uitgevoerd, waaronder een transactie naar crypto.com. Revolut had enkele pogingen al geblokkeerd vanwege vermoedens van fraude, maar de klant bevestigde zelf dat betalingen doorgang moesten vinden. Het Kifid concludeert dat de bank geen zorgplicht heeft geschonden en binnen het coulancekader mocht besluiten geen compensatie toe te kennen. De klacht van het slachtoffer werd ongegrond verklaard.

Kamervragen over uitsluiten Amerikaanse techbedrijven bij aanbestedingen

In de Tweede Kamer zijn vragen gesteld over de afhankelijkheid van de Nederlandse financiële sector van grote Amerikaanse technologiebedrijven. GroenLinks-PvdA vraagt demissionair ministers Heinen (Financiën) en Karremans (Economische Zaken) of zij bereid zijn deze afhankelijkheid te verminderen door samen te werken met de Autoriteit Financiële Markten en De Nederlandsche Bank. Beide toezichthouders waarschuwden recent voor concentratie- en systeemrisico’s, omdat verstoringen bij één Amerikaanse leverancier grote gevolgen kunnen hebben voor de hele sector. De Kamer wil weten of de regering kan onderzoeken welke structurele risico’s hiermee gepaard gaan, welke obstakels Europese samenwerking voor digitale autonomie hinderen en of Amerikaanse bedrijven onder Amerikaanse surveillancewetgeving kunnen worden uitgesloten bij aanbestedingen. De ministers hebben drie weken de tijd om de vragen te beantwoorden.

Zorgen in VS over gezichtsherkenning in Ring-deurbelcamera’s

In de Verenigde Staten groeit de bezorgdheid over Amazons plan om gezichtsherkenning toe te voegen aan de Ring-deurbelcamera. De nieuwe functie “Familiar Faces” maakt het mogelijk om personen te taggen zodat de camera hen later automatisch herkent. Daarbij worden gezichten van voorbijgangers gescand en kan Amazon de verzamelde biometrische data tot zes maanden bewaren. De burgerrechtenorganisatie EFF waarschuwt dat dit kan leiden tot massasurveillance, datalekken en discriminatie, mede doordat Ring al samenwerkt met politie en opsporingsdiensten. Ook senator Edward Markey uitte zijn zorgen en riep Amazon op het plan te schrappen. Volgens hem vormt de uitbreiding een bedreiging voor de privacy van burgers, omdat mensen gevolgd kunnen worden zonder hun medeweten. Amazon kondigde daarnaast de “search party”-functie aan, bedoeld voor het opsporen van huisdieren, maar volgens critici eenvoudig inzetbaar voor het volgen van personen.

Apache OpenOffice ontkent datalek na claim Akira-groep

De Apache Software Foundation heeft ontkend dat haar OpenOffice-project slachtoffer is geworden van een aanval door de Akira-ransomwaregroep. De criminelen beweerden 23 gigabyte aan bedrijfsdocumenten te hebben gestolen, waaronder personeels- en financiële gegevens. Volgens de stichting is er echter geen enkel bewijs dat er een inbraak of datalek heeft plaatsgevonden. OpenOffice is een open-sourceproject zonder betaalde medewerkers, waardoor de organisatie niet over de genoemde gevoelige informatie beschikt. Er is geen losgeldeis ontvangen en er zijn geen aanwijzingen dat de infrastructuur van Apache of OpenOffice is gecompromitteerd. De foundation benadrukt dat alle ontwikkelingsactiviteiten openbaar verlopen via mailinglijsten, waardoor interne documenten zoals door Akira beschreven niet bestaan. Tot op heden is geen gestolen data gepubliceerd en heeft Apache geen contact gezocht met politie of externe beveiligingsexperts.

SonicWall bevestigt dat staatsgesponsorde hackers achter inbreuk op beveiliging stonden

SonicWall heeft bevestigd dat staatsgesponsorde hackers verantwoordelijk waren voor de beveiligingsinbreuk in september, waarbij de back-upbestanden van de firewallconfiguraties van klanten werden blootgesteld. Het onderzoek, uitgevoerd door Mandiant, toonde aan dat de schadelijke activiteiten geen invloed hadden op

SonicWall-producten, firmware, systemen, tools, broncode of klantennetwerken. De inbreuk werd beperkt tot onbevoegde toegang tot cloud-back-upbestanden in een specifieke cloudomgeving via een API-aanroep. De gedupeerden kregen het advies om hun inloggegevens te resetten en bepaalde wachtwoorden en toegangscodes te vernieuwen. Het incident had geen impact op de producten of de werking van SonicWall, en er is geen verband met eerdere aanvallen van de Akira-ransomwaregroep. Het onderzoek is inmiddels afgerond en de cyberweerbaarheid van SonicWall is versterkt.

China straft pig butchering oplichters met de dood

China heeft recent meerdere leden van criminele families die betrokken zijn bij zogenaamde "pig butchering"-oplichterij, tot de doodstraf veroordeeld. De Bai-maffiafamilie is de laatste in een reeks die verantwoordelijk was voor grootschalige oplichtingen in Zuidoost-Azië, met name in Myanmar. Deze bende opereerde op 41 locaties en genereerde miljarden dollars door het uitvoeren van oplichtingsschema's, zoals frauduleuze casino’s en dwangprostitutie. De leden van de Bai-familie werden aangeklaagd voor moord, ontvoering, afpersing, en andere misdaden. Verschillende leden, waaronder de leiders Bai Suocheng en Bai Yingcang, kregen de doodstraf, terwijl andere levenslange gevangenisstraffen of langere straffen kregen. De Chinese autoriteiten intensiveren hun samenwerking met Myanmar en Thailand om dergelijke misdaden harder aan te pakken, met waarschuwingen dat de daders het uiterste risico lopen.

Nexperia-chips: auto-industrie in crisis door exportblokkade China

De blokkade door China van de export van Nexperia-chips heeft de auto-industrie in Europa in een crisissituatie gebracht. Nexperia, gevestigd in Nijmegen, levert essentiële chips die in talloze auto-onderdelen zitten. Door de stopzetting van de leveringen dreigen autofabrieken stil te vallen, aangezien de voorraden snel opraken. Grote fabrikanten zoals Volkswagen en Nissan melden dat het onzeker is of ze na deze week nog door kunnen produceren. Honda heeft een fabriek in Mexico al stilgelegd door het chiptekort. Nexperia-chips zijn moeilijk te vervangen, omdat andere leveranciers mogelijk niet dezelfde hoeveelheden kunnen leveren en het technisch lastig is om ze te vervangen zonder aanzienlijke aanpassingen. De Europese autobezorgers hopen dat China uitzonderingen kan maken op de

exportblokkade, maar er is nog veel onzekerheid over de voorwaarden en het papierwerk kan weken duren. De situatie blijft kritiek voor de auto-industrie.

Onzekerheid over de nieuwe Cyberbeveiligingswet blijft groot voor bedrijven

Er is veel onduidelijkheid voor bedrijven over de nieuwe Cyberbeveiligingswet, die voortkomt uit de Europese NIS2-richtlijn. Deze wet, die organisaties in cruciale sectoren verplicht om hun cyberbeveiliging op orde te brengen en incidenten te melden, zou oorspronkelijk in oktober 2024 ingaan, maar is nu uitgesteld tot het tweede kwartaal van 2026. Deskundigen geven aan dat de voortdurende vertraging en onduidelijke communicatie van de overheid de urgentie voor bedrijven ondermijnen. Veel bedrijven weten nog steeds niet of zij onder de wet vallen en krijgen geen duidelijke antwoorden van overheidsinstanties zoals het NCSC. De overheid heeft aangekondigd dat er eind november een online campagne zal starten om bedrijven beter te informeren en hen aan te moedigen stappen te zetten richting naleving van de wet.

NCSC: ‘We zijn geen digitale brandweer’

Matthijs van Amelsfort, directeur van het Nationaal Cyber Security Centrum (NCSC), benadrukt dat het NCSC niet optreedt als de ‘digitale brandweer’ van Nederland. De invoering van de Cyberbeveiligingswet (Cbw) zal leiden tot een stijging van het aantal organisaties dat het centrum ondersteunt van 300 naar naar verwachting 8.000 tot 10.000. Deze wet, die voortkomt uit de Europese NIS2-richtlijn, verplicht bedrijven in cruciale sectoren zoals energie en zorg om hun cyberbeveiliging op orde te hebben. De wet introduceert meld- en registratieplichten, en bedrijven zullen bestuurlijk aansprakelijk zijn voor nalatigheid. Het NCSC blijft zich richten op het adviseren, duiden en onderzoeken van cyberincidenten, maar bedrijven moeten zelf de verantwoordelijkheid nemen voor het oplossen van incidenten. De wet zou in 2026 in werking moeten treden, nadat eerdere deadlines zijn gemist.

Norton Crack Midnight Ransomware en publiceert gratis decryptor

Norton’s onderzoeksafdeling heeft een kwetsbaarheid ontdekt in de Midnight-ransomware, die is opgebouwd uit de Babuk ransomware-code. Deze kwetsbaarheid, die oorspronkelijk bedoeld was om de versleuteling te versnellen en

te versterken, leidde echter tot een verslechtering van de beveiliging. Het gebruik van RSA-sleutels in combinatie met ChaCha20-versleuteling maakte het mogelijk voor Norton om een gratis decryptor te ontwikkelen die slachtoffers in staat stelt hun bestanden zonder losgeld te herstellen. Midnight, die vergelijkbaar is met Babuk, versleutelt delen van bestanden in plaats van de gehele bestanden, waardoor de versleuteling sneller wordt uitgevoerd. De decryptor van Norton is nu beschikbaar voor Windows-gebruikers in zowel 32-bits als 64-bits versies en biedt een veilige manier om gegevens te herstellen. Norton raadt aan een back-up te maken voordat het herstelproces wordt gestart om verlies van gegevens te voorkomen.

FIN7 hackers gebruiken Windows SSH backdoor voor stealthy toegang en persistentie

De beruchte cybercriminelen van de FIN7 groep, ook wel bekend als Savage Ladybug, blijven een aanzienlijke bedreiging vormen voor bedrijfsomgevingen door een verfijnde Windows SSH backdoor te gebruiken. Deze malware, die sinds 2022 actief is, stelt aanvallers in staat om persistente toegang te verkrijgen en data te stelen, terwijl traditionele detectiemechanismen worden omzeild. De groep maakt gebruik van legitieme OpenSSH-tools en batchscripts om een verborgen communicatielijn te creëren tussen gecompromitteerde systemen en de infrastructuur van de aanvallers. Dit maakt het moeilijk om de aanvallen op te merken, aangezien het verkeer lijkt op reguliere administratieve verbindingen. De backdoor biedt verschillende manieren voor de aanvallers om data te extraheren en zich lateraal door netwerken te bewegen, terwijl de veranderingen minimaal zijn om detectie te voorkomen. Organisaties wordt aangeraden strikte SSH-toegangscontrole in te stellen en op afwijkende verbindingen te letten om deze dreiging effectief te bestrijden.

Curly COMrades Hacker Groep Gebruikt Nieuwe Tools om Verborgen Remote Toegang te Creëren op Gecompromitteerde Windows 10-systemen

De Curly COMrades hacker groep heeft een geavanceerde aanvalsmethode geïntroduceerd die gebruik maakt van Hyper-V virtualisatietechnologie op gecompromitteerde Windows 10-machines. De groep activeert de Hyper-V rol en gebruikt een minimalistische Alpine Linux-gebaseerde virtuele machine (VM) om malware, zoals de reverse shell CurlyShell en de reverse proxy CurlCat, te draaien.

Deze virtuele omgeving is moeilijk te detecteren door traditionele beveiligingsmaatregelen, omdat het verkeer via het netwerk van de host verloopt. Het gebruik van proxy- en tunnelingtools versterkt de flexibiliteit van de toegang tot de getroffen systemen. Deze aanval markeert een verfijnde stap in de tactieken van de groep, die zich eerder in augustus 2025 richtte op geopolitieke doelen. De operatie benadrukt de technologische vaardigheid en zorgvuldige planning van de aanvallers.