Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

29-11-2025:

Zuid-Korea vermoedt betrokkenheid van Noord-Korea bij hack van Upbit crypto-exchange

Zuid-Korea onderzoekt de recente hack van de cryptocurrency-exchange Upbit, waarbij 44,5 miljard won (ongeveer 30,4 miljoen dollar) werd gestolen. De Zuid-Koreaanse autoriteiten vermoeden dat een hackersteam, verbonden aan de Noord-Koreaanse spionagedienst, de Lazarus-groep, verantwoordelijk is voor de inbraak. De aanval werd gekarakteriseerd als een "abnormale opname" van cryptocurrencies.

Upbit, de grootste cryptocurrency-exchange van Zuid-Korea, heeft bevestigd dat er een aanzienlijke hoeveelheid geld is gestolen en heeft aangegeven dat het de oorzaak en de omvang van de vermissing onderzoekt. De aanval vond plaats vlak voor de aankondiging van de overname van Upbit door internetgigant Naver. De Lazarus-groep, die al eerder werd gelinkt aan andere crypto-diefstallen, staat bekend om zijn geavanceerde cyberaanvallen. De Amerikaanse FBI heeft Noord-Korea's cyberoperaties aangemerkt als een van de meest geavanceerde en blijvende dreigingen.

Zuid-Koreaanse wetshandhavers zijn momenteel bezig met een onderzoek, maar hebben verder geen details vrijgegeven. Er wordt verwacht dat de situatie verdere gevolgen kan hebben voor de beveiliging van cryptocurrency-exchanges wereldwijd.

Noord-Korea en Rusland versterken cyberdreigingen door nauwe samenwerking

Noord-Korea heeft recent aangekondigd dat de Russische taal vanaf het vierde leerjaar verplicht wordt in de scholen van het land, een stap die deel uitmaakt van een bredere versterking van de banden tussen Noord-Korea en Rusland. Deze ontwikkeling heeft niet alleen geopolitieke implicaties, maar vergroot ook de risico's op cyberaanvallen voor landen in Europa, waaronder Nederland en België.

De samenwerking tussen Noord-Korea en Rusland is in de afgelopen jaren versterkt, vooral op het gebied van cybercriminaliteit. Twee van de meest actieve door staten ondersteunde cybercrimegroepen, Rusland’s Gamaredon en Noord-Korea’s Lazarus, hebben hun middelen en tactieken gedeeld, wat wijst op een ongekende samenwerking tussen de twee landen op het gebied van geavanceerde cyberaanvallen. Dit kan de digitale veiligheid van Europese landen, waaronder

Nederland en België, bedreigen, vooral als het gaat om langdurige en gecoördineerde cyberaanvallen die door staatsactoren worden uitgevoerd.

Deze ontwikkelingen komen op een moment dat Rusland en Noord-Korea al hun samenwerking in andere domeinen, zoals militaire en economische zaken, hebben verdiept. Dit zou kunnen betekenen dat de gezamenlijke digitale dreigingen van deze landen steeds sterker zullen worden, met mogelijk verregaande gevolgen voor de wereldwijde cyberveiligheid en de beveiliging van kritieke infrastructuren in Europa.

De intensivering van deze samenwerking, vooral in de digitale ruimte, benadrukt de noodzaak voor Europese landen om alert te blijven op de groeiende risico's van staatsgeoriënteerde cyberdreigingen. De gevolgen van deze versterkte samenwerking voor Nederland en België kunnen aanzienlijk zijn, vooral als de cybercriminelen gebruik maken van nieuwe middelen en tactieken die door Rusland en Noord-Korea worden gedeeld.

Gelekte gesprekken tussen Witkoff en Kremlin-adviseurs trekken internationale aandacht

Onlangs zijn er gelekte telefoongesprekken gepubliceerd tussen Steve Witkoff, de Amerikaanse speciale gezant voor Oekraïne, en Yuri Ushakov, de Russische buitenlandadviseur. De gesprekken werden vrijgegeven zonder specifieke informatie over de bron, wat heeft geleid tot een stroom van speculaties over wie achter de lekken zit. Russische president Vladimir Putin heeft gereageerd op de controverse door te suggereren dat de gesprekken mogelijk vervalst zijn, en verweerde zich tegen de beschuldigingen dat Witkoff te veel sympathie voor Rusland zou hebben.

De oorsprong van de gelekte gesprekken is onzeker. Diverse inlichtingendiensten hebben hun vermoedens gedeeld over de bron van het lek, met sommige bronnen die suggereren dat een buitenlandse inlichtingendienst toegang had tot een onveilige mobiele lijn van Ushakov, terwijl andere denken dat de lekken mogelijk uit de VS afkomstig zijn. Dit incident werpt een schijnwerper op de kwetsbaarheid van vertrouwelijke communicatie en de risico's van digitale spionage in geopolitieke onderhandelingen.

Het lek komt op een moment van verhoogde spanningen in de wereldpolitiek, vooral in het kader van de Oekraïense oorlog, en benadrukt de rol van digitale spionage en cyberdreigingen in geopolitieke processen. Dit is een belangrijk voorbeeld van hoe digitale informatiebeveiliging en inlichtingendiensten invloed hebben op internationale

relaties, en het benadrukt de noodzaak van robuuste beveiliging tegen digitale dreigingen, een thema dat ook in Nederland en België van groot belang is.

Geopolitieke spanningen beïnvloeden chipproductie in Nederland: risico's voor cybersecurity

De recente spanningen tussen Nederland en China, veroorzaakt door het conflict rondom chipmaker Nexperia, werpen een schaduw over de wereldwijde toeleveringsketen van halfgeleiders. Nexperia heeft het Chinese moederbedrijf gevraagd om de leveringsproblemen op te lossen, aangezien de dreiging van productiestops in diverse sectoren steeds groter wordt. Deze situatie kan niet alleen de productie in de auto-industrie verstoren, maar ook gevolgen hebben voor de cybersecurity van bedrijven die afhankelijk zijn van deze kritieke technologieën.

Geopolitieke geschillen zoals deze kunnen de wereldwijde supply chains voor digitale producten kwetsbaar maken, wat leidt tot verhoogde risico’s voor cyberaanvallen die gericht zijn op onderbreking van de productie of diefstal van intellectueel eigendom. Aangezien Nederland zich steeds meer positioneert als een technologisch knooppunt in Europa, is het essentieel dat bedrijven zich bewust zijn van de impact van deze geopolitieke ontwikkelingen op hun digitale infrastructuren en de beveiliging daarvan.

Handala Hacker Groep richt zich op high-tech en lucht- en ruimtevaartprofessionals

De Handala hacker groep heeft recent een gerichte aanval gelanceerd op professionals werkzaam in de Israëlische high-tech en lucht- en ruimtevaartsectoren. Deze aanval is niet alleen zorgwekkend voor Israël, maar heeft bredere implicaties voor Europese landen, waaronder Nederland en België, waar de high-techsector sterk vertegenwoordigd is.

De groep publiceerde een lijst van doelwitten, waarvan zij de persoonlijke en professionele informatie op hun dark web platform deelden. Deze gegevens werden vergezeld van beschrijvingen die de doelwitten ten onrechte als criminelen afschilderden. De publicatie werd gevolgd door een beloningssysteem voor aanvullende informatie over deze doelwitten, wat de dreiging vergroot door crowdsourcing van inlichtingen.

Trustwave-beveiligingsonderzoekers ontdekten de aanval en merkten op dat de gepubliceerde dataset grotendeels is gebaseerd op LinkedIn-profielen. Echter, het bleek dat de gegevens onnauwkeurig waren, met profielen van personen die al jarenlang niet meer werkten bij de genoemde bedrijven en informatie die mogelijk was gemanipuleerd om de lijst te versterken.

Deze praktijken, waarbij publiek toegankelijke gegevens worden verzameld en gemanipuleerd voor vijandige doeleinden, benadrukken de risico's voor bedrijven en professionals in de high-techsector. De dreiging van dergelijke aanvallen kan ook gevolgen hebben voor de privacy, veiligheid en reputatie van werknemers in Europese landen, waar de technologische sector in toenemende mate het doelwit is van geopolitieke aanvallen.

Het is cruciaal voor Nederlandse en Belgische organisaties in deze sectoren om zich bewust te zijn van de risico's die gepaard gaan met dergelijke aanvallen en de gevolgen van het onterecht openbaar maken van persoonlijke gegevens. De Handala hacker groep laat zien hoe ver een dreiging kan gaan, van publieke beschuldigingen tot het verzamelen van inlichtingen voor verder gebruik in cyberaanvallen.

Lazarus Group valt Zuid-Koreaanse cryptobeurs aan en steelt miljoenen

De Lazarus Group, een hackinggroep die wordt gesteund door de Noord-Koreaanse overheid, wordt verdacht van het stelen van 45 miljard won (ongeveer 30 miljoen dollar) aan cryptocurrency van de Zuid-Koreaanse cryptobeurs Upbit. De Zuid-Koreaanse autoriteiten onderzoeken de zaak, waarbij wordt aangenomen dat de groep dezelfde methoden heeft gebruikt als bij een eerdere aanval in 2019, waarbij zo'n 40 miljoen dollar aan Ethereum (ETH) werd gestolen. Deze aanvallen zijn een voorbeeld van de groeiende dreiging van geavanceerde hackinggroepen die cryptocurrency-exchanges wereldwijd aanvallen.

Zeker voor Nederlandse en Belgische gebruikers van cryptoplatforms, is het van belang om bewust te zijn van de risico's die dergelijke aanvallen met zich meebrengen. Lazarus, die bekendstaat om zijn connecties met de Noord-Koreaanse staat, maakt gebruik van gedecentraliseerde netwerken om gestolen crypto-activa anoniem te verplaatsen en wit te wassen, wat het traceren van de gestolen middelen bemoeilijkt. Dit toont de dreiging die cybercriminelen vormen voor zowel de crypto-industrie als voor bedrijven die in digitale valuta handelen.

Het incident onderstreept de noodzaak voor strengere beveiligingsmaatregelen, niet alleen voor cryptoplatforms, maar ook voor hun gebruikers wereldwijd. De aanvallen op platforms zoals Upbit zijn slechts een van de vele voorbeelden van hoe cybersecuritydreigingen de digitale economie beïnvloeden. De Lazarus Group wordt sinds 2017 gelinkt aan de diefstal van meer dan 6 miljard dollar aan crypto-activa, wat de omvang van deze cyberdreiging benadrukt.

Malicious LLMs versterken aanvallen door onervaren hackers met geavanceerde tools

De opkomst van ongecontroleerde grote taalmodellen (LLM's) zoals WormGPT 4 en KawaiiGPT heeft het voor onervaren hackers mogelijk gemaakt om geavanceerde aanvallen uit te voeren, waarbij deze tools helpen bij het genereren van kwaadaardige code en het automatiseren van aanvallen. Deze modellen worden steeds vaker gebruikt door cybercriminelen, die toegang krijgen via betaalde abonnementen of gratis lokale versies van de modellen. Het WormGPT-model, dat oorspronkelijk in 2023 werd geïntroduceerd, heeft zijn weg gevonden naar de cybercrimegemeenschap, en de nieuwste versie, WormGPT 4, biedt nog geavanceerdere functionaliteit, zoals ransomware-encryptie en laterale bewegingen binnen netwerken.

Onderzoekers van Palo Alto Networks Unit 42 hebben de mogelijkheden van WormGPT 4 getest en ontdekten dat het model in staat is om werkende scripts te genereren voor ransomware die alle PDF-bestanden op een Windows-host kan versleutelen. Het gegenereerde script maakt gebruik van het AES-256-algoritme en kan zelfs gegevens via Tor exfiltreren. Het model produceerde ook een overtuigende losgeldbrief die "militair-geclassificeerde encryptie" claimt en een 72-uursdeadline stelt voor de betaling, wat het voor aanvallers gemakkelijker maakt om geloofwaardige phishing- en zakelijke e-mailcompromis (BEC)-aanvallen uit te voeren.

KawaiiGPT, een ander kwaadaardig LLM dat dit jaar is gesignaleerd, kan worden gebruikt om goedgeconfigureerde phishingberichten te genereren en scripts te maken die laterale bewegingen binnen netwerken automatiseren. Dit model maakt het ook mogelijk om bestanden op Windows-systemen te doorzoeken en gecompromitteerde gegevens via e-mail naar de aanvaller te sturen. Hoewel KawaiiGPT geen volledige ransomware-payloads kan genereren zoals WormGPT 4,

kan het wel gebruikt worden om aanvallers te helpen bij het verhogen van hun machtigingen en het uitvoeren van aanvullende kwaadaardige handelingen.

Beide modellen worden gedeeld en besproken op gespecialiseerde Telegram-kanalen, waar leden tips en adviezen uitwisselen. Deze ontwikkeling toont aan dat kwaadaardige LLM's niet langer een theoretische dreiging vormen, maar daadwerkelijk actief worden ingezet door cybercriminelen, die zo aanvallen op grotere schaal kunnen uitvoeren en geavanceerdere technieken kunnen gebruiken zonder diepgaande technische kennis. De potentie van deze tools om de dreiging in cyberspace te versterken, maakt het voor zelfs de minst ervaren hackers mogelijk om zeer geavanceerde cyberaanvallen uit te voeren.

Bloody Wolf breidt Java-gebaseerde NetSupport RAT-aanvallen uit

De cyberaanvalscampagne van de dreigingsactor bekend als Bloody Wolf, die vanaf juni 2025 actief is, heeft zich recentelijk uitgebreid naar Oezbekistan en Kirgizië. Deze groep maakt gebruik van spear-phishing-aanvallen om NetSupport RAT (Remote Access Trojan) te verspreiden, vooral gericht op de overheids-, financiële en IT-sectoren. Dit soort aanvallen kunnen ook relevant zijn voor organisaties in Nederland en België, aangezien de gebruikte technieken wereldwijd kunnen worden toegepast.

De aanvallers maken gebruik van schadelijke e-mailbijlagen, die de ontvanger misleiden door officiële documenten van overheidsinstanties te imiteren. Het doel is om een Java Archive (JAR)-bestand te laten uitvoeren, waarmee de NetSupport RAT wordt gedownload. Deze malware stelt de aanvallers in staat om op afstand toegang te krijgen tot geïnfecteerde systemen, met behulp van verschillende methoden om zichzelf in stand te houden, zoals het aanpassen van systeemtaken en het toevoegen van opstartscripts.

De aanvallen maken ook gebruik van geofencing, waarbij verzoeken van buiten Oezbekistan worden omgeleid naar legitieme overheidswebsites, terwijl gebruikers binnen Oezbekistan daadwerkelijk de schadelijke bestanden downloaden. Dit soort geavanceerde aanvallen benadrukt het groeiende risico voor landen in Europa, waaronder Nederland en België, waar soortgelijke tactieken in de toekomst kunnen worden ingezet.

Het gebruik van eenvoudig verkrijgbare tools en social engineering maakt deze aanvallen relatief goedkoop, maar zeer effectief, en benadrukt de noodzaak voor

organisaties wereldwijd om alert te blijven op deze steeds geavanceerdere dreigingen.

Nieuwe tools en technieken van APT-groep Tomiris onthuld

De Tomiris APT-groep heeft in 2025 nieuwe tools en technieken ontwikkeld voor cyberaanvallen. Deze groep richt zich op buitenlandse ministeries, intergouvernementele organisaties en overheidsinstanties, met als doel toegang te krijgen tot diplomatieke en politieke infrastructuren. De groep maakt gebruik van verschillende kwaadaardige hulpmiddelen, waaronder reverse shells in verschillende programmeertalen, zoals Go, Rust, C/C#, C++, Python en PowerShell. Deze tools communiceren vaak via openbare diensten zoals Discord en Telegram, wat hen helpt om kwaadaardig verkeer te verbergen en zo detectie door beveiligingstools te vermijden.

De aanvallen beginnen vaak met phishing-e-mails die een kwaadaardig archief bevatten, meestal met een wachtwoord in de e-mailtekst. Na het uitvoeren van de kwaadaardige bestand worden systemen geïnfecteerd met verschillende soorten backdoors en implantaten. Een opvallend kenmerk van de Tomiris-aanvallen is het gebruik van open-source C2-frameworks zoals Havoc en AdaptixC2, die de aanvallers in staat stellen om lange tijd toegang tot de systemen te behouden en verdere schade aan te richten.

In sommige gevallen wordt de infectie gevolgd door het downloaden van extra payloads, zoals het AdaptixC2-framework, via methoden zoals bitsadmin, curl, PowerShell en certutil. Deze frameworks kunnen op hun beurt zorgen voor verdere exploitatie en het verkrijgen van systeembeheerdersrechten.

De slachtoffers van deze aanvallen zijn voornamelijk Russische entiteiten en sprekers van andere talen uit Centraal-Azië, zoals Turkmenistan, Kirgizië, Tadzjikistan en Oezbekistan. De gebruikte technieken zijn geavanceerd en zijn gericht op het verkrijgen van langdurige toegang zonder gedetecteerd te worden. De evolutie in de tactieken van Tomiris benadrukt de nadruk die de groep legt op stealth en volharding.

Dit recente onderzoek onderstreept de noodzaak voor geavanceerde detectiestrategieën, zoals gedragsanalyse en netwerkverkeersinspectie, om dergelijke dreigingen effectief te kunnen identificeren en mitigeren.

Risico’s door verlaten iCalendar-sync-domeinen kunnen miljoenen apparaten blootstellen aan aanvallen

Digitale agenda's zijn tegenwoordig onmisbare hulpmiddelen voor het beheren van persoonlijke en professionele schema’s. Veel gebruikers abonneren zich op externe kalenders voor openbare feestdagen, sportevenementen of gemeenschapsactiviteiten om hun agenda’s up-to-date te houden. Hoewel deze abonnementen gemak bieden, creëren ze een blijvende verbinding tussen het apparaat van de gebruiker en een extern serverdomein.

Wanneer het domein dat de kalender host verloopt of wordt verlaten, ontstaat er een aanzienlijke kwetsbaarheid. Cybercriminelen kunnen deze verlopen domeinen opnieuw registreren en daarmee het vertrouwen dat oorspronkelijk door het abonnement was opgebouwd misbruiken. Deze aanvalsmethode is bijzonder gevaarlijk, omdat het geen nieuwe actie van het slachtoffer vereist. Het apparaat van de gebruiker blijft namelijk automatisch synchronisatieverzoeken sturen naar het nu kwaadwillige domein.

Aanvallers kunnen op deze manier verschillende bedreigingen rechtstreeks in de kalenderinterface van de gebruiker injecteren, variërend van scareware die zich voordoet als systeemwaarschuwingen tot phishing-links die zich voordoen als exclusieve aanbiedingen. Dit type aanval is moeilijk te detecteren, omdat het traditionele e-mailfilters omzeilt door gebruik te maken van het impliciete vertrouwen dat gebruikers hebben in hun persoonlijke planningstools.

Een recent onderzoek door Bitsight beveiligingsanalisten onthulde meer dan 390 verlaten domeinen die nog steeds actief synchronisatieverzoeken ontvangen. De analyse wees uit dat deze domeinen dagelijks communiceren met ongeveer vier miljoen unieke IP-adressen, voornamelijk van iOS- en macOS-apparaten. Dit wijst op de enorme schaal waarop een eenvoudig verlopen domein miljoenen gebruikers kan blootstellen aan potentiële aanvallen zonder hun medeweten.

Het onderzoek identificeerde specifieke technische patronen die deze exploitatie mogelijk maken. De HTTP-verzoeken vertonen een duidelijke “User-Agent”-string die het iOS-kalendersysteem identificeert, wat bevestigt dat het verzoek een achtergrondproces betreft en geen door de gebruiker geïnitieerde browserbezoek is. Deze techniek maakt het mogelijk om geavanceerde malware of phishing-aanvallen via kalenders te distribueren, zonder dat de gebruiker hier ooit bewust van is.

Kwetsbaarheid in verouderde Python-pakketten maakt aanvallen via domeincompromis mogelijk

In de Python-gemeenschap is recentelijk een kwetsbaarheid ontdekt die developers in gevaar kan brengen. Het betreft verouderde bootstrap-scripts die in legacy-pakketten van Python zijn achtergelaten. Deze scripts bevatten harde verwijzingen naar externe domeinen die niet langer onder controle staan van de oorspronkelijke beheerders, wat ze vatbaar maakt voor overname door kwaadwillende actoren. Het probleem ontstond door het gebruik van een verouderd domein, python-distribute[.]org, dat sinds 2014 niet meer in gebruik is en inmiddels te koop staat.

Als een aanvaller het domein zou kunnen bemachtigen, kunnen ze kwaadaardige payloads hosten die automatisch gedownload en uitgevoerd worden bij het gebruik van de besmette scripts. Dit biedt een directe route voor supply chain-aanvallen, waarbij de normale beveiligingscontrolemechanismen worden omzeild. De scripts zijn vooral gevaarlijk omdat ze zonder enige validatie of controle code van deze externe bronnen ophalen, waardoor het mogelijk is voor aanvallers om code uit te voeren met volledige privileges van de ontwikkelaar.

De kwetsbaarheid wordt niet geactiveerd tijdens een standaard pip-installatie, maar kan wel tot een probleem leiden als de scripts handmatig worden uitgevoerd of tijdens een build-proces. Onderzoekers hebben de kwetsbaarheid aangetoond door een proof-of-concept-exploit te ontwikkelen die de kwetsbaarheid in verschillende populaire pakketten, zoals slapos.core, aanstak.

De impact van deze kwetsbaarheid ligt vooral in de verwaarlozing van legacy-code die nog steeds in veel repositories aanwezig is, hoewel veel ontwikkelaars inmiddels zijn overgestapt op nieuwere verpakkingsstandaarden. Het probleem wordt versterkt door de manier waarop de scripts afhankelijkheden resolven zonder enige controle op de integriteit van de gedownloade code. De ontdekking van deze kwetsbaarheid benadrukt het belang van het onderhouden en updaten van oude softwarecomponenten in de open-source gemeenschap.

Scattered Lapsus$ Hunters registreren 40+ domeinen die Zendesk-omgevingen nabootsen

Een nieuwe, geavanceerde cyberaanval is geïdentificeerd die wordt uitgevoerd door de groep "Scattered Lapsus$ Hunters". Deze aanvallers hebben hun focus verlegd naar het misbruiken van kwetsbaarheden in de toeleveringsketen. De aanval richt zich op Zendesk, een essentieel platform voor klantenservice, en maakt gebruik van deze vertrouwde zakelijke tool om bedrijfsinformatie te verzamelen en gevoelige gegevens te stelen.

De aanvallers hebben meer dan veertig domeinen geregistreerd die op het eerste gezicht legitiem lijken, maar die in werkelijkheid zijn ontworpen om te profiteren van typfouten in domeinnamen, zoals znedesk[.]com en vpn-zendesk[.]com. Deze domeinen bevatten valse Single Sign-On (SSO) portals die in staat zijn om de inloggegevens van nietsvermoedende gebruikers te onderscheppen.

De infrastructuur van de aanval toont een gecoördineerde poging om detectie te vermijden. De aanvallers maakten gebruik van diensten zoals NiceNic voor domeinregistratie en Cloudflare voor het maskeren van de werkelijke naamservers, wat hun poging om de phishingpagina's langer actief te houden vergemakkelijkte. Dit stelde hen in staat om aanzienlijke hoeveelheden high-privilege inloggegevens te verzamelen voordat tegenmaatregelen werden genomen.

De impact van deze aanval reikt verder dan alleen het stelen van inloggegevens. Beveiligingsanalisten van Reliaquest hebben malware geïdentificeerd die deze campagne verbindt met eerdere aanvallen op Salesforce in augustus 2025. Nadat de aanvallers de initiële authenticatielaag hebben omzeild, kunnen ze verder bewegen binnen de netwerken van bedrijven, wat hen toegang geeft tot gevoelige klantgegevens, zoals facturatie-informatie en overheids-ID's. Dit lijkt sterk op de gegevensdiefstal die plaatsvond bij een aanval op Discord in september 2025.

Een van de gevaarlijkste tactieken van de groep is het gebruik van legitieme ondersteuningsverzoeken om de traditionele beveiligingsmaatregelen van bedrijven te omzeilen. In plaats van phishing-e-mails te gebruiken, dienen de aanvallers valse tickets in via het Zendesk-systeem. Deze tickets, die vaak doen alsof ze dringend systeembeheerverzoeken of wachtwoordresets zijn, bevatten links naar de gevaarlijke domeinen of bevatten schadelijke payloads. Wanneer helpdeskmedewerkers de tickets openen, activeren ze per ongeluk Remote Access Trojans (RAT's), waarmee de aanvallers op afstand toegang krijgen tot de systemen en verdere aanvallen kunnen uitvoeren.

De Scattered Lapsus$ Hunters hebben aangegeven dat zij van plan zijn om deze operaties voort te zetten, met een focus op het verzamelen van klantdatabases

tijdens het vakantieseizoen van 2026. Deze campagne illustreert een aanzienlijke evolutie in hun capaciteiten en toont aan hoe vergevorderde cybercriminelen in staat zijn om onopgemerkt ernstige schade toe te brengen via bekende en vertrouwde platformen.

Hackers registreren 18.000 vakantiedomeinen voor oplichting tijdens feestdagen

In de aanloop naar de feestdagen van 2025 hebben cybercriminelen een massale aanval opgezet door duizenden domeinnamen te registreren die inspelen op populaire zoekwoorden zoals “Kerstmis”, “Black Friday” en “Flash Sale”. Dit is onderdeel van een bredere strategie waarbij valse webshops worden opgezet om onoplettende consumenten in Nederland en België te misleiden en hun persoonlijke gegevens te stelen.

In de afgelopen drie maanden zijn er wereldwijd maar liefst 18.000 vakantiegerelateerde domeinen geregistreerd, die zijn ontworpen om legitieme webwinkels na te doen. Veel van deze sites hebben slechts kleine variaties in hun URL, waardoor ze moeilijk te onderscheiden zijn voor consumenten die snel online winkelen. De sites worden gebruikt voor phishingcampagnes en fraude, waarbij vooral cadeaubonfraude en betaalpagina's worden ingezet om gegevens van consumenten te stelen.

Hoewel veel van de domeinen nog inactief zijn om detectie te vermijden, zijn er al duizenden van deze websites actief, met als doel de consumenten in de feestdagenperiode te misleiden. Cybersecurity-experts wijzen op de rol van geautomatiseerde tools die de schaal van de campagne vergroten en de frauduleuze websites hoog in zoekresultaten plaatsen, waardoor ze naast legitieme sites verschijnen wanneer consumenten op zoek zijn naar aanbiedingen.

De gevolgen van deze aanval worden verder vergroot door een toename van gestolen inloggegevens. Er circuleren momenteel meer dan 1,5 miljoen gestolen accounts van populaire e-commercewebsites op ondergrondse markten, die door cybercriminelen kunnen worden gebruikt om snel toegang te krijgen tot accounts en betalingen te doen.

Daarnaast wordt er specifiek ingegaan op kwetsbaarheden in e-commerceplatforms, zoals de CVE-2025-54236 in Adobe Magento. Deze kwetsbaarheid kan door aanvallers worden gebruikt om zonder authenticatie toegang te krijgen tot

beheerdersaccounts en schadelijke code in te voeren, wat leidt tot diefstal van persoonlijke gegevens en verdere systeemcompromittaties.

Dit bericht is niet alleen relevant voor consumenten in Nederland en België, maar benadrukt ook de noodzaak voor webshops en consumenten om extra waakzaam te zijn in deze drukke winkelperiode.

29 verdachten gearresteerd in operaties tegen mensenhandelnetwerken in Europa

Europol heeft recent twee gezamenlijke operaties ondersteund die gericht waren op het verstoren van grote mensenhandelnetwerken in Europa. Deze criminele netwerken waren actief in de seksuele uitbuiting van kwetsbare personen. De operaties werden uitgevoerd in november en resulteerden in de arrestatie van tientallen verdachten, de bevrijding van slachtoffers en de confiscatie van substantiële criminele opbrengsten. De betrokken landen waren Frankrijk, Spanje, Italië en Roemenië.

In de eerste operatie, die gericht was tegen een Chinees mensenhandelnetwerk, werkten de autoriteiten van Frankrijk en Spanje samen. Het netwerk, dat zich richtte op seksuele uitbuiting via ‘seks toerisme’ in meerdere EU-lidstaten, werd blootgelegd door 15 huiszoekingen op 4 november. Tijdens deze operatie werden 37 slachtoffers gevonden, waaronder 34 in Frankrijk. De verdachten hadden de slachtoffers misleid over de omstandigheden van hun werk in de EU. Van de tien gearresteerde verdachten werden zeven in voorlopige hechtenis geplaatst. Er werd 47.000 euro in contanten en 160.000 euro op bankrekeningen in beslag genomen.

In de tweede operatie, uitgevoerd door Italië en Roemenië, werd een netwerk van een Roemeens familieclan ontmanteld dat al meer dan twintig jaar actief was. Het netwerk dwong jonge meisjes via geweld en manipulatie in de prostitutie in Rome. De actie op 18 november leidde tot 25 huiszoekingen en de arrestatie van 19 verdachten. De autoriteiten ontdekten onroerend goed, luxe voertuigen en andere goederen die verband hielden met criminele activiteiten. Het netwerk genereerde naar schatting 1,7 miljoen euro aan illegale opbrengsten.

Deze operaties benadrukken de blijvende dreiging van georganiseerde criminele netwerken in Europa en de noodzaak voor intensieve internationale samenwerking om mensenhandel en seksuele uitbuiting effectief te bestrijden. Het is van groot

belang dat de Europese samenwerking verder wordt versterkt om dergelijke misdrijven tegen kwetsbare mensen te voorkomen en te bestrijden.

INTERPOL versterkt internationale samenwerking in de strijd tegen cybercriminaliteit

De INTERPOL Algemene Vergadering, gehouden in Marrakesh, Marokko, heeft op 27 november 2025 een belangrijk strategisch kader goedgekeurd voor de periode 2026-2030, gericht op het versterken van de wereldwijde samenwerking bij het bestrijden van georganiseerde misdaad, inclusief cybercriminaliteit. Het nieuwe strategisch kader zal landen, waaronder Nederland en België, helpen om hun samenwerking te intensiveren en beter in te spelen op de opkomende dreigingen op het gebied van cyberfraude, mensenhandel en illegale financiering.

Het strategisch plan richt zich op drie belangrijke pijlers: het creëren van een betrouwbare wereldwijde informatiehub voor wetshandhavers, het bieden van operationele ondersteuning aan landen, en het fungeren als de leidende stem voor wetshandhavingsinstanties wereldwijd. Voor landen als Nederland en België, die actief deelnemen aan de internationale strijd tegen cybercriminaliteit, biedt dit strategisch plan de mogelijkheid om verder te investeren in grensoverschrijdende samenwerking en het delen van cruciale informatie.

Tijdens de vergadering werd ook stilgestaan bij de succesvolle inzet van INTERPOL's Notice-systeem en globale databases voor het ontmantelen van criminele netwerken, waarvan de impact ook merkbaar is in Europa. De vooruitgang van het Silver Notice-project, waarmee criminele activa van meer dan 30 miljard euro zijn opgespoord, toont de kracht van internationale samenwerking bij het bestrijden van georganiseerde misdaad, ook in cybercriminaliteit.

Daarnaast werd gendergelijkheid binnen de wetshandhaving benadrukt, met focus op de inclusie van vrouwen in leiderschapsrollen, wat ook relevant is voor de aanpak van misdaad en de effectiviteit van politiewerk wereldwijd.

De goedkeuring van dit strategisch kader benadrukt hoe landen in Europa, waaronder Nederland en België, kunnen profiteren van een sterker en efficiënter internationaal netwerk van wetshandhavers om cyberdreigingen en andere transnationale misdaden gezamenlijk te bestrijden.

Teenager genoemd als beheerder van Scattered LAPSUS$ Hunters groep, ontkent betrokkenheid

Recent is er een onderzoek gepubliceerd waarin een 15-jarige jongen, bekend als "Rey," wordt genoemd als een van de beheerders van de hackinggroep Scattered LAPSUS$ Hunters (SLSH). De jongen, wiens echte naam volgens rapporten Saif Khader zou zijn, ontkent echter elke betrokkenheid bij de groep. Volgens het onderzoek, dat werd geleid door de cybersecurity-onderzoeker Brian Krebs, zou Khader, die zich online ook Hikki-Chan noemde, een van de drie beheerders van het Telegram-kanaal van SLSH zijn. Dit werd ontdekt nadat Krebs de identiteit van Khader nader had onderzocht, waarbij hij een verbinding legde naar de vader van de tiener, een piloot bij de Royal Jordanian Airlines.

De ontdekking van Khader als mogelijk lid van SLSH kwam aan het licht na een reeks toevallige fouten van Rey, die persoonlijke informatie deelde in online chats en op Telegram. In een van de chats zou Rey per ongeluk zijn eigen wachtwoord hebben gedeeld, en in een andere gesprek noemde hij zijn vader, wat leidde tot de verdere ontdekking van zijn identiteit.

Scattered LAPSUS$ Hunters, een groep die verschillende cybercriminaliteitsgroepen combineert, heeft dit jaar een aantal opvallende aanvallen uitgevoerd. De groep zou onder andere gegevens hebben gestolen van Salesforce-systemen en bedrijven zoals Toyota en FedEx hebben bedreigd met het lekken van deze gegevens. Daarnaast zou de groep ook geprobeerd hebben om medewerkers van bedrijven te rekruteren, wat leidde tot de ontslag van een werknemer bij CrowdStrike, die interne screenshots naar de groep had gestuurd.

In een reactie op het onderzoek van Krebs heeft de SLSH-groep de bevindingen verworpen. Ze beschuldigden Krebs ervan te proberen hun reputatie te beschadigen en beschouwden de onderzoeksresultaten als een "wanhopige poging" om hen in diskrediet te brengen. SLSH verklaarde verder dat het onzin was om aan te nemen dat één persoon verschillende aliassen gebruikte met totaal verschillende technieken. Ze noemden de beschuldigingen zelfs lachwekkend en vroegen Krebs om bewijzen te leveren van de onthullingen.

Saif Khader zelf heeft de beschuldigingen ontkend en beweerde dat hij sinds juni 2025 probeerde afstand te nemen van de groep en samenwerkte met wetshandhavers. Hij gaf aan dat hij geen interesse meer had in de criminele activiteiten van de groep en dat hij zelfs bereid was om de gevolgen van zijn acties te aanvaarden, mocht hij geconfronteerd worden met juridische stappen.

De situatie rondom de identiteit van "Rey" en zijn mogelijke rol in de Scattered LAPSUS$ Hunters-groep blijft dus onduidelijk. Desondanks is het opmerkelijk dat iemand die maanden geleden al publiekelijk werd genoemd, nog steeds actief lijkt te zijn en betrokken is bij enkele van de grootste cyberaanvallen van dit jaar. Het lijkt erop dat de verdenkingen rondom zijn betrokkenheid niet snel zullen verdwijnen, ondanks zijn ontkenning en de reacties van de groep.

EVA-team van de Politie spoort 46 veroordeelden op met een totaaltegoed van 140 jaar celstraf

Het EVA-Team (Executie Vonnissen Afgestraften) van de Politie Eenheid Den Haag heeft in de afgelopen vier maanden 46 veroordeelden aangehouden, die gezamenlijk nog 140 jaar celstraf moeten uitzitten. Deze personen waren veroordeeld voor verschillende ernstige misdrijven, waaronder overtredingen van de Opiumwet, fraude, afpersing, oplichting, mensenhandel en witwassen. Het EVA-Team richt zich specifiek op veroordeelden die zich proberen te onttrekken aan hun opgelegde straf, een probleem dat ook cybercriminelen kan betreffen.

De aangehouden verdachten waren moeilijk op te sporen, maar dankzij de samenwerking met nationale en internationale opsporingsinstanties zijn ze nu in beeld gebracht. In een aantal gevallen betrof het verdachten die zowel in Nederland als België actief waren, zoals de 22-jarige man die betrokken was bij zowel wapenbezit in Nederland als een gewapende overval in België. Hij werd na zijn aanhouding in Nederland overgeleverd aan België om zijn resterende straf uit te zitten.

In een ander geval werd een 34-jarige man aangehouden voor criminele activiteiten in Polen, waaronder deelname aan een criminele organisatie en fraude. Hij werd uitgeleverd aan Polen, waar hij een straf van 75 jaar kan krijgen.

Hoewel het EVA-Team zich niet uitsluitend richt op cybercriminelen, is de inzet van gespecialiseerde eenheden om criminelen op te sporen en aan te houden van cruciaal belang, vooral nu ook digitale misdrijven in toenemende mate onderdeel worden van de criminele wereld. Veroordeelden die bijvoorbeeld digitale misdrijven hebben gepleegd en zich aan hun straf onttrekken, kunnen eveneens rekenen op de inzet van opsporingsdiensten zoals het EVA-Team.

Storing bij CME Group legt wereldwijde handelsfutures stil en roept bezorgdheid op over digitale infrastructuur

Op vrijdag 28 november 2025 ondervond CME Group, de grootste beursoperator ter wereld, een technische storing die de handel in Amerikaanse aandelenfutures, valuta en grondstoffen tijdelijk stillegde. De oorzaak van de storing werd toegeschreven aan een koelingsprobleem in de datacenters van CyrusOne, die door CME Group worden gebruikt. Dit incident had wereldwijd invloed op de handelsactiviteiten, waardoor investeerders zich zonder de gebruikelijke voorafgaande gegevens moesten voorbereiden op de verkorte handelsdag.

De verstoring werd in eerste instantie gemeld op donderdagavond, en de futures van belangrijke indexen zoals de S&P 500, Nasdaq 100 en de Dow Jones Industrial Average stopten kort na de laatste handelsactiviteit. Dit probleem kwam op een kritisch moment voor veel handelaren die portefeuilles moesten herbouwen aan het einde van de maand, wat de impact van de uitval vergrootte.

Hoewel het incident vooral de handel op de Amerikaanse markten betreft, is de storing een herinnering aan de kwetsbaarheid van de digitale infrastructuur waarop wereldwijde financiële markten draaien. Het benadrukt het belang van robuuste back-upsystemen en continuïteitsplannen voor kritieke digitale diensten. In de context van de bredere cyberdreigingen en de opkomst van digitale valuta's en blockchaintechnologie, kunnen incidenten zoals deze invloed hebben op de stabiliteit van markten die afhankelijk zijn van digitale platforms.

Er werd een lichte toename van volatiliteit voorspeld zodra de storing werd opgelost, wat mede te wijten was aan de verminderde liquiditeit van de markten tijdens de verkorte handelsweek, die door de Thanksgiving-vakantie werd beïnvloed. In het geval van een verlengde verstoring kunnen de gevolgen voor de markten ernstiger zijn, vooral gezien de cruciale rol die digitale systemen spelen in de moderne handel.

Retailbedrijven, zoals Walmart en Nike, ondervonden kleinere koersstijgingen, wat in verband kan worden gebracht met de feestdagen en de toegenomen onlineverkoop, maar ook met de onzekerheid die werd veroorzaakt door de marktverstoring.

Franse voetbalbond getroffen door cyberaanval, gegevens gestolen

De Franse voetbalbond (FFF) heeft bevestigd dat het slachtoffer is geworden van een cyberaanval, waarbij gegevens van leden zijn gestolen. De aanval richtte zich op

de software die door clubs wordt gebruikt voor het beheer van hun ledenadministratie. Deze aanval werd uitgevoerd via een gecompromitteerd account, waarna ongeautoriseerde toegang werd verkregen.

De federatie heeft snel gereageerd door het verdachte account uit te schakelen en alle wachtwoorden van gebruikersaccounts opnieuw in te stellen. De gestolen gegevens bevatten persoonlijke informatie zoals namen, geslachten, nationaliteit en contactgegevens. Het incident is gemeld bij de autoriteiten, en de federatie benadrukt dat de aanval werd beperkt tot persoonsgegevens.

Hoewel dit incident zich in Frankrijk heeft voorgedaan, illustreert het de wereldwijde dreiging van cyberaanvallen, waarmee organisaties, ook in Nederland en België, dagelijks te maken kunnen krijgen. Het incident benadrukt het belang van voortdurende versterking van beveiligingsmaatregelen tegen cyberdreigingen die voortdurend evolueren.

De FFF heeft haar toezegging herhaald om de gegevens van haar leden te beschermen en haar beveiligingsmaatregelen verder aan te scherpen om zich te wapenen tegen toekomstige aanvallen.

Meeste jonge cybercriminelen stoppen na het twintigste levensjaar

Onderzoekers in opdracht van het Wetenschappelijk Onderzoek- en Datacentrum (WODC) van het ministerie van Justitie en Veiligheid hebben de maatschappelijke kosten van criminele carrières onder adolescenten onderzocht. Uit het onderzoek blijkt dat de meeste jonge cybercriminelen stoppen met hun criminele activiteiten zodra ze de twintig zijn gepasseerd, wat overeenkomt met het patroon dat bij veel vormen van traditionele criminaliteit zichtbaar is. Het onderzoek toont aan dat de leeftijdsstructuren van cybercriminelen in grote lijnen vergelijkbaar zijn met die van andere criminele groepen.

Cybercriminaliteit vereist specifieke technische vaardigheden, die vaak al in de jeugd worden ontwikkeld. Dit kan bijvoorbeeld het hacken van games omvatten. Hoewel cybercriminelen dus vaak jonge leeftijdsgroepen betreffen, wordt er opgemerkt dat het plegen van deze misdrijven aanzienlijke technische kennis vereist, waardoor de daders zich anders ontwikkelen dan traditionele criminelen. Volgens eerdere studies piekt de criminele activiteit onder cybercriminelen vaak rond het twintigste levensjaar, waarna de frequentie van hun misdaden afneemt.

Er wordt echter een kleine groep cybercriminelen van ongeveer vier procent geïdentificeerd die op latere leeftijd actief blijft. De onderzoekers suggereren dat deze groep blijft doorgaan door hun grotere technologische vaardigheden en de intrinsieke motivatie die vaak voortkomt uit een fascinatie voor technologie en de complexiteit van cybercriminaliteit. Deze bevindingen kunnen waardevolle inzichten bieden voor het opstellen van preventiebeleid.

Minister Van Oosten van Justitie en Veiligheid heeft verklaard dat dit onderzoek aantoonde dat jeugdcriminaliteit niet slechts een probleem is binnen het veiligheidsdomein, maar sterk verweven is met het sociaal domein, onderwijs en werk. Het onderzoeksresultaat zal helpen bij het formuleren van effectiever preventiebeleid door beter inzicht te bieden in de criminele carrières van jongeren en hun maatschappelijke impact.

Britse overheid adviseert mkb passphrases, updates en wachtwoordmanager

De Britse overheid heeft onlangs een oproep gedaan aan het midden- en kleinbedrijf (mkb) om hun digitale beveiliging te verbeteren. Het National Cyber Security Centre (NCSC) benadrukt dat jaarlijks de helft van de mkb-bedrijven in het Verenigd Koninkrijk te maken krijgt met een cyberincident. Ondanks de toenemende dreiging, blijkt uit onderzoek dat veel mkb-bedrijven cybersecurity als te complex, te kostbaar of niet urgent beschouwen. Om deze bedrijven te ondersteunen, heeft het NCSC de "Cyber Action Toolkit" gelanceerd. Deze toolkit biedt eenvoudig toepasbare adviezen om de veiligheid van accounts en systemen te verbeteren.

De toolkit richt zich op enkele basismaatregelen, zoals het gebruik van passphrases in plaats van standaardwachtwoorden, het instellen van tweefactorauthenticatie (2FA), het gebruik van wachtwoordmanagers, het maken van back-ups en het tijdig installeren van beveiligingsupdates. Het NCSC wijst erop dat bij 32% van de cyberaanvallen kwetsbaarheden worden misbruikt waarvoor bedrijven geen updates hebben geïnstalleerd. De overheid benadrukt dat het gebruik van de toolkit geen technische expertise vereist en dat het bedrijven kan beschermen tegen verwoestende aanvallen die het voortbestaan van het bedrijf in gevaar kunnen brengen.

De Cyber Action Toolkit is bedoeld als een laagdrempelige manier voor mkb-bedrijven om hun beveiliging te verbeteren zonder dat er diepgaande technische kennis nodig is. De toolkit biedt een praktisch stappenplan dat bedrijven helpt om

essentiële beveiligingsmaatregelen te nemen en zo hun digitale weerbaarheid te vergroten.

GrapheneOS haalt servers weg uit Frankrijk vanwege privacyzorgen

De ontwikkelaars van GrapheneOS, een open-source besturingssysteem voor smartphones, hebben aangekondigd hun servers uit Frankrijk te verplaatsen. Deze beslissing volgt op zorgen over de veiligheid van open-source projecten in het land. Volgens de makers willen de Franse autoriteiten ongewenste toegang krijgen tot hun systemen, met name door het inbouwen van backdoors in encryptie en apparaten. Ze waarschuwen dat dergelijke ontwikkelingen de privacy en veiligheid van gebruikers zouden ondermijnen.

Deze stap komt na een reeks negatieve berichtgevingen in de Franse media, waaronder Le Parisien en Le Figaro, die GrapheneOS in verband brachten met criminaliteit, zoals drugshandel. De Franse overheid zou volgens de ontwikkelaars een onjuiste berichtgeving verspreiden, die de rol van GrapheneOS in misdaad in een verkeerd daglicht stelt. De makers stellen dat, zelfs als de Franse media objectiever zouden berichten, de beslissing om het land te verlaten niet te voorkomen was door de toenemende druk van de autoriteiten.

De ontwikkelaars van GrapheneOS stellen verder dat de situatie in Frankrijk een bredere trend in Europa weerspiegelt, waarbij overheden steeds meer toegang eisen tot versleutelde gegevens en beveiligde apparaten. Ze vrezen dat open-source software onder druk komt te staan, met als gevolg dat veilige technologieën mogelijk niet meer toegestaan zullen worden. Als reactie op deze situatie willen ze hun servers niet langer in Frankrijk hosten en stellen ze dat er actieve pogingen zijn om de nieuwste versie van GrapheneOS voor Pixel-toestellen te blokkeren. Bovendien zouden de ontwikkelaars zelf doelwit zijn van persoonlijke aanvallen.

Dit incident toont de toenemende bezorgdheid over de privacy en de bescherming van gegevens in Europa, vooral met betrekking tot de invloed van overheidsdiensten op digitale beveiliging en open-source projecten. De situatie roept belangrijke vragen op over de toekomstige bescherming van open-source software en het recht op privacy in de EU, die ook Nederland en België aangaan.

Spaanse luchthavenbeheerder krijgt 10 miljoen euro boete voor gezichtsherkenningstechnologie

De Spaanse privacytoezichthouder AEPD heeft een boete van 10 miljoen euro opgelegd aan de Spaanse luchthavenbeheerder Aena wegens het gebruik van gezichtsherkenningssystemen op luchthavens. Dit gebeurde zonder de vereiste Data Protection Impact Assessment (DPIA), een beoordeling van de risico's van biometrische gegevensverwerking, die volgens de Europese privacywetgeving noodzakelijk is. De AEPD oordeelde dat Aena de privacyrechten van passagiers onvoldoende beschermde en dat er alternatieven waren die minder ingrijpend zouden zijn voor de betrokkenen.

De beslissing heeft bredere implicaties voor de toepassing van gezichtsherkenning in de Europese Unie. Ook in Nederland en België wordt steeds vaker gebruikgemaakt van deze technologie in openbare ruimtes en vervoershubs. Het benadrukt de noodzaak voor bedrijven en overheden om te voldoen aan de privacyregels van de AVG, vooral wanneer het gaat om de verwerking van gevoelige gegevens zoals biometrische informatie. De boete komt op een moment dat de EU-lidstaten onder druk staan om strengere richtlijnen te hanteren voor het gebruik van technologieën die de privacy van burgers kunnen aantasten.

Naast de boete heeft de AEPD Aena opgedragen om de gezichtsherkenningstechnologie tijdelijk te staken totdat een nieuwe DPIA is uitgevoerd. Aena heeft aangegeven in beroep te gaan tegen de boete, maar de uitspraak heeft een bredere boodschap voor andere EU-landen over het belang van transparantie en de bescherming van persoonsgegevens bij het implementeren van nieuwe technologieën.

Onderzoek naar aparte domeinextensie voor overheidssites nog gaande

Het onderzoek naar de invoering van een aparte domeinextensie voor overheidswebsites in Nederland is nog steeds in uitvoering. De voortgangsrapportage van de Nederlandse Cybersecuritystrategie, die demissionair minister Van Oosten van Justitie en Veiligheid naar de Tweede Kamer heeft gestuurd, meldt dat de resultaten van dit onderzoek pas eind 2025 worden verwacht. Het idee om een uniforme domeinnaamextensie te gebruiken, zoals .gov.nl of .overheid.nl, werd oorspronkelijk naar voren gebracht in een eerder onderzoek in opdracht van het ministerie van Binnenlandse Zaken. Dit onderzoek stelde vast dat

het voor burgers moeilijk is om de officiële overheidswebsites te onderscheiden van andere online bronnen, wat kan leiden tot verwarring over de betrouwbaarheid van de informatie.

Volgens de voortgangsrapportage heeft het kabinet, op basis van internationale voorbeelden en overwegingen omtrent de veiligheid, een principebesluit genomen om de extensie '.gov.nl' te hanteren voor overheidswebsites. Op dit moment wordt er echter nog gewerkt aan een impactanalyse die de haalbaarheid en de financiële en organisatorische gevolgen van de invoering van een dergelijke extensie onderzoekt. Het onderzoek wordt uitgevoerd binnen een beperkte scope en moet uiteindelijk inzicht geven in de kosten en uitvoerbaarheid van de realisatie van deze domeinnaamextensie. In afwachting van de afronding van dit onderzoek kunnen burgers via het Register Internetdomeinen Overheid controleren of een website of e-mailadres werkelijk tot een overheidsorganisatie behoort.

Simone Smit nieuwe directeur van AIVD: Impact op cybersecurity

Simone Smit wordt per maart 2026 benoemd tot directeur-generaal van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD). Smit, die sinds begin 2021 plaatsvervangend directeur-generaal was, volgt Erik Akerboom op. De benoeming werd goedgekeurd door de ministerraad op voorstel van demissionair minister Kajsa Ollongren van Binnenlandse Zaken. Smit heeft een lange ervaring binnen de nationale veiligheid, onder andere als directeur van Contraterrorisme bij de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en als programmadirecteur voor de acute aanpak van Covid-19.

In haar nieuwe rol zal Smit verantwoordelijk zijn voor het versterken van zowel de strategische als operationele capaciteiten van de AIVD, met bijzondere aandacht voor de technologische ontwikkeling en digitale veiligheid. Haar inzet op het verbeteren van de infrastructuur en ondersteunende processen zal essentieel zijn in een tijd waarin de dreigingen in cyberspace steeds geavanceerder en complexer worden. Smit zal als directeur ook nauw samenwerken met zowel nationale als internationale veiligheidspartners en andere inlichtingenorganisaties, wat de samenwerking op het gebied van cybersecurity versterkt.

Deze benoeming is van belang voor de cybersecuritygemeenschap, aangezien de AIVD een sleutelrol speelt in het beschermen van Nederland tegen digitale dreigingen en het bestrijden van cybercriminaliteit. Het wordt verwacht dat onder

Smit’s leiding de AIVD zich verder zal inzetten voor het ontwikkelen van geavanceerde technologieën om Nederland’s digitale veiligheid te waarborgen.

Slachtoffers van online Facebook-oplichting spreken in Pano

In de recente aflevering van Pano, uitgezonden op 26 november 2025, werden de persoonlijke verhalen gedeeld van slachtoffers van oplichting via Facebook-advertenties. De documentaire belicht hoe deze slachtoffers aanzienlijke bedragen verloren, variërend van spaargeld tot zelfs hun huis. Het gebruik van bekende Vlamingen en politici in valse advertenties, versterkt door kunstmatige intelligentie, blijkt een terugkerende tactiek te zijn die slachtoffers naar frauduleuze websites lokt.

De modus operandi van deze scam wordt laag voor laag opgebouwd. Van de eerste klik op een advertentie tot de voortdurende telefoontjes van callcenters die de slachtoffers blijven lastigvallen, terwijl de gestolen bedragen uiteindelijk in buitenlandse databanken terechtkomen. In Belgrado werd een ex-werknemer van een callcenter geïnterviewd, die vertelde over de dagelijkse praktijk van het bellen van 240 mensen, terwijl zijn collega's tot wel 70.000 euro per dag binnenhaalden. Het werkklimaat in deze centra werd omschreven als een 'Wolf of Wall Street'-sfeer, waarbij succesvolle scammers vaak werden beloond met cocaïne.

Ondanks duidelijke richtlijnen van Facebook, het moederbedrijf van het platform, lijkt het moeilijk te zijn om deze scams te stoppen. Justitie in België heeft haar zorgen geuit, aangezien de gerechtelijke systemen overbelast raken door het aantal meldingen. De kans om bruikbare sporen te vinden in online oplichtingsdossiers wordt momenteel geschat op slechts 5 procent. De aflevering concludeert dat België niet goed voorbereid is op de steeds grotere dreiging van cybercriminaliteit, waarbij zowel de platformen als de autoriteiten tekortschieten in de bestrijding van deze fraude.

Online afpersing treft steeds meer gezinnen in het VK, maar ook wereldwijd

Uit recent onderzoek blijkt dat bijna één op de tien ouders in het VK aangeeft dat hun kind slachtoffer is geworden van online afpersing, waarbij criminelen dreigen intieme beelden te publiceren of persoonlijke informatie openbaar te maken. De Britse kinderbeschermingsorganisatie NPCC ontdekte dat één op de vijf ouders een kind kent dat dit soort afpersing heeft meegemaakt. Veel ouders geven aan dat ze niet

zeker weten hoe ze het onderwerp met hun kinderen moeten bespreken, uit angst hen te verontrusten.

De afpersers maken vaak gebruik van privéberichten op sociale mediaplatformen, en in sommige gevallen wordt kunstmatige intelligentie ingezet om valse profielen aan te maken, waardoor slachtoffers worden misleid om vertrouwelijke beelden te sturen. Daarna worden de slachtoffers afgeperst voor geld.

Deze problematiek is niet alleen een zorg voor het VK. Het wereldwijd toenemende aantal gevallen van online afpersing wijst op de bredere dreiging van sextortion, die steeds vaker voorkomt. Deskundigen roepen op tot actie van zowel techbedrijven als overheden om de bescherming van kinderen tegen dit soort online dreigingen te verbeteren.

iOS 26 Zero-Click Exploit Te Koop Op Dark Web

Een nieuwe dreiging is opgekomen in de wereld van cyberbeveiliging, waarbij een zero-click exploit voor iOS 26 te koop wordt aangeboden op het dark web. De exploit, geclaimd door de actor "ResearcherX," zou in staat zijn om root-toegang te verkrijgen tot iOS-apparaten en de recente beveiligingsmaatregelen van het besturingssysteem te omzeilen. Dit zou de mogelijkheid bieden om toegang te krijgen tot gevoelige gegevens zoals foto's, berichten, locatie-informatie en Keychain-items zonder dat de gebruiker daar enig actie voor hoeft te ondernemen.

De verkoper beweert dat de exploit volledig functioneel is en geschikt voor verkoop aan andere cybercriminelen. Dit type exploit is bijzonder gevaarlijk omdat het geen interactie van de gebruiker vereist, wat betekent dat een kwetsbaar apparaat op afstand kan worden gecompromitteerd. Ondanks de claims van de verkoper, waarschuwen experts dat de aanbieding mogelijk een oplichtersactie is, aangezien het aanbod nog niet geverifieerd is. De beschrijving van de exploit vertoont echter overeenkomsten met eerdere zero-click exploits die iOS-systemen hebben getroffen.

Dit incident benadrukt de continue dreiging van kwetsbaarheden in populaire besturingssystemen zoals iOS en de grote risico's die het dark web biedt voor de verkoop van geavanceerde aanvallen. De situatie is nog in afwachting van verdere verificatie, maar de gevolgen kunnen groot zijn voor gebruikers van iOS-apparaten, vooral als het blijkt dat deze exploit daadwerkelijk werkt.

Europese zorgen over opslag overheidsdata in Amerikaanse cloudoplossingen

In de recente publicatie van de Zwitserse vereniging van functionarissen voor gegevensbescherming, Privatim, wordt gewaarschuwd voor het gebruik van Amerikaanse clouddiensten voor de opslag van gevoelige overheidsdata. Hoewel de boodschap gericht is op Zwitserland, heeft de resolutie brede implicaties voor overheidsinstellingen in de EU, waaronder Nederland en België, die te maken hebben met vergelijkbare kwesties rondom gegevensbescherming en privacy.

Volgens Privatim brengt het uitbesteden van de opslag van gevoelige gegevens aan buitenlandse cloudproviders risico's met zich mee, vooral wanneer deze bedrijven geen volledige end-to-end encryptie bieden. Dit betekent dat cloudaanbieders mogelijk toegang hebben tot de opgeslagen data, wat de controle over persoonlijke gegevens van burgers bemoeilijkt. De resolutie verwijst specifiek naar de Amerikaanse CLOUD Act, die Amerikaanse bedrijven kan verplichten om klantgegevens te verstrekken, zelfs als deze in Europese datacenters zijn opgeslagen. Dit roept vragen op over de mogelijke schending van fundamentele rechten zoals privacy, een onderwerp dat in Nederland en België al breed wordt besproken, gezien de strengere EU-wetgeving op het gebied van gegevensbescherming, zoals de AVG.

Privatim stelt voor dat overheidsinstellingen, om deze risico's te beperken, alleen Amerikaanse cloudoplossingen gebruiken wanneer de gegevens zelf zijn versleuteld door de betreffende instantie en de cloudprovider geen toegang heeft tot de encryptiesleutel. Deze aanpak biedt een extra laag van bescherming, zodat de cloudprovider geen toegang heeft tot de versleutelde data.

Deze zorgen sluiten aan bij bredere Europese discussies over de veiligheid van cloudoplossingen voor overheidsdata, vooral nu de EU zich steeds sterker richt op digitale soevereiniteit en de controle over persoonlijke gegevens binnen de regio wil behouden. Voor Nederlandse en Belgische overheden kan dit debat belangrijke gevolgen hebben voor de keuze van cloudproviders en de bescherming van burgergegevens.