Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

24-11-2025:

Oekraïne's cybercapaciteiten als strategisch hulpmiddel tegen China's wereldwijde proxy-netwerk

Oekraïne speelt niet alleen een cruciale rol in de verdediging van Europa tegen de Russische agressie, maar heeft zich ook gepositioneerd als een technologisch strategisch instrument tegen China's groeiende invloed wereldwijd. In de huidige geopolitieke context heeft Oekraïne, met zijn snel ontwikkelende militaire technologie, de mogelijkheid om indirect druk uit te oefenen op Chinese proxy-netwerken, wat een belangrijke rol speelt in de bredere mondiale machtsstrijd.
De snelle technologische vooruitgang van Oekraïne heeft het land in staat gesteld om geavanceerde militaire technologieën, zoals drones en elektronische oorlogsvoering, te ontwikkelen en in te zetten. Deze innovaties stellen Oekraïne niet alleen in staat zichzelf te verdedigen, maar ook om digitale en fysieke netwerken te verstoren die de Russische strategie ondersteunen, waaronder die met Chinese connecties.
De inzet van Oekraïne in de 'grijze zone', waar het land zonder directe escalatie strategische aanvallen uitvoert, biedt waardevolle inzichten in de inzet van cybertechnologie in hybride conflicten. Oekraïne heeft bijvoorbeeld cyberoperaties uitgevoerd die gericht zijn op de ondermijning van Chinese logistieke netwerken in Latijns-Amerika en Azië, gebieden die traditioneel moeilijk toegankelijk zijn voor westerse landen.
De strategische inzet van technologie door Oekraïne vormt een belangrijk voorbeeld van hoe cyberoperaties kunnen worden ingezet tegen mondiale dreigingen. Deze acties versterken niet alleen de veiligheid van Oekraïne, maar dragen ook bij aan de bredere cyberveiligheidsagenda van westerse landen, door indirect de invloed van China en Rusland wereldwijd te verminderen.
Oekraïne's benadering biedt een waardevolle les in het gebruik van digitale middelen als een krachtig hulpmiddel in geopolitieke conflicten, wat relevant is voor zowel cyberveiligheidsexperts als beleidsmakers.

Drones gesignaleerd boven vliegbasis Volkel, Defensie zet wapens in tegen luchtbedreiging

Op 21 november 2025 werden meerdere drones gesignaleerd boven de strategisch belangrijke vliegbasis Volkel in Noord-Brabant, een locatie die onder andere F-35-gevechtsvliegtuigen huisvest. De drones, die verboden zijn boven militaire bases, werden tussen 19.00 en 21.00 uur opgemerkt door bewakingspersoneel. Als reactie werd door de Koninklijke Luchtmacht wapens ingezet om de drones uit de lucht te halen.

Dit incident volgt op een reeks soortgelijke gevallen in Europa, waarbij drones vaker worden ingezet bij luchthavens en andere kritieke infrastructuur. Drones kunnen gebruikt worden voor uiteenlopende doeleinden, waaronder spionage, het verstoren van operaties of zelfs cyberaanvallen door middel van het uitlekken van informatie of verstoren van netwerken. De inzet van wapens tegen de drones is een signaal dat dergelijke activiteiten niet worden getolereerd, maar roept ook vragen op over de kwetsbaarheid van onze vitale infrastructuur voor dergelijke technologieën.
Hoewel het onduidelijk is wie er achter de drones zit, wordt het incident onderzocht door de Koninklijke Marechaussee en de politie. De aanwezigheid van kernwapens op Volkel maakt dit voorval extra gevoelig, en de inzet van drones in deze context zou kunnen wijzen op een grotere dreiging voor nationale en internationale veiligheid. Defensie werkt aan nieuwe technologieën, zoals netten en geavanceerde wapens, om drones effectief uit de lucht te halen, waarmee ze zich voorbereiden op de voortdurende toename van drone-gerelateerde risico's.

Ruimte-datacenters: snelgroeiende sector met nieuwe cyberrisico's
De ontwikkeling van datacenters in de ruimte neemt snel toe, en de markt kan tegen 2030 een waarde van 535 miljard euro bereiken, aldus een rapport van het European Space Policy Institute (ESPI). Deze ontwikkelingen brengen aanzienlijke voordelen met zich mee, zoals het gebruik van zonne-energie voor een duurzamere werking, maar ook nieuwe cyberveiligheidsuitdagingen. De Europese Unie wordt aangespoord om snel een strategie te ontwikkelen, anders dreigt Europa achter te blijven op dit gebied.
Commerciële bedrijven, vooral uit de ruimtevaart- en AI-sector, zijn actief bezig met het realiseren van ruimte-datacenters. Deze technologie belooft aanzienlijke energievoordelen, maar tegelijkertijd ontstaan er vraagstukken over de bescherming van gegevens en systemen in de ruimte. Het beheren van zulke gedistribueerde netwerken brengt nieuwe uitdagingen met zich mee op het gebied van privacy en databeveiliging, aangezien de kwetsbaarheden die normaal in aardse datacenters worden aangepakt, nu moeten worden geëxtrapoleerd naar de ruimte.
Daarnaast vormen de stijgende aantallen satellieten en het risico op botsingen in de ruimte een nieuw terrein voor cybersecurity. Een toenemend aantal botsingen kan leiden tot schade aan satellieten, met mogelijke gevolgen voor de integriteit van gegevensstromen en communicatiekanalen. De opkomst van ruimte-datacenters vraagt dus niet alleen om innovatieve technische oplossingen, maar ook om robuuste cybersecuritymaatregelen die in staat zijn om deze nieuwe digitale infrastructuren te beschermen tegen zowel traditionele als opkomende dreigingen.

China-gerelateerde APT31 voert stealthy cyberaanvallen uit op Russische IT via cloudservices

APT31, een geavanceerde persistente dreiging (APT) die vaak wordt gekoppeld aan China, heeft tussen 2024 en 2025 doelgerichte cyberaanvallen uitgevoerd op de Russische IT-sector. Deze aanvallen werden gekarakteriseerd door het gebruik van legitieme cloudservices, waaronder de veelgebruikte Yandex Cloud, als command-and-control (C2)-infrastructuur en voor data-exfiltratie. Het gebruik van deze cloudservices diende om de aanvallen te camoufleren en detectie te vermijden door zich als normaal netwerkverkeer voor te doen.

De aanvallen richtten zich vooral op Russische IT-bedrijven die werkten als contractanten en integratoren voor overheidsinstanties. De cyberaanvallers bleven lange tijd onopgemerkt, met sommige aanvallen die al in 2022 begonnen en later escaleerden. In sommige gevallen werden versleutelde opdrachten en schadelijke payloads via sociale media, zowel binnenlandse als buitenlandse, verspreid. Deze techniek werd ook gebruikt tijdens het weekend en op feestdagen om het risico van ontdekking te minimaliseren.

In een voorbeeld uit december 2024 stuurden de aanvallers een spear-phishing e-mail die een RAR-archief bevatte. Dit archief opende een Windows Shortcut (LNK), die een Cobalt Strike-loader genaamd CloudyLoader activeerde via DLL side-loading. Dit illustreert de verfijning van de gebruikte technieken en de lange tijd dat de aanvallers in de netwerken van hun slachtoffers actief bleven.

APT31 maakt gebruik van zowel openbaar beschikbare als aangepaste tools om toegang te verkrijgen en hun aanwezigheid te handhaven binnen de systemen van de slachtoffers. De groep zet onder andere software zoals Yandex Disk en Google Chrome in voor persistente toegang, en maakt gebruik van een breed scala aan tools om gevoelige informatie te verzamelen, zoals wachtwoorden en interne berichten van de getroffen organisaties.

De groep heeft bovendien geavanceerde tunnelingtechnieken toegepast, zoals het gebruik van Microsoft OneDrive en andere cloudservices voor command-and-control, wat hen in staat stelde om hun infrastructuur efficiënt te beheren en nieuwe payloads naar besmette systemen te sturen. Deze strategieën hebben ertoe bijgedragen dat APT31 in staat is gebleven om gedurende lange periodes onopgemerkt te blijven, terwijl het tegelijkertijd cruciale gegevens exfiltreerde van de getroffen netwerken.

China's spionage in Europa breidt zich uit en wordt geavanceerder

China vergroot zijn spionage-inspanningen in Europa door middel van steeds geavanceerdere en langdurige netwerken die zowel menselijke bronnen als zakelijke

en academische connecties combineren. Dr. Marcin Grabowski, directeur van het Centrum voor Internationale Studies en Ontwikkeling aan de Jagiellonische Universiteit, merkt op dat de Chinese spionage steeds meer gebruik maakt van digitale en fysieke kanalen om toegang te krijgen tot gevoelige informatie binnen Europese instellingen. Deze activiteiten zijn vaak minder zichtbaar dan traditionele cyberaanvallen, maar ze maken gebruik van netwerken in de academische wereld, het bedrijfsleven en diplomatieke kanalen om Europese besluitvormers en technologische capaciteiten te beïnvloeden.
Hoewel cyberespionage vaak de aandacht trekt, blijkt uit recente gevallen dat China zijn focus steeds meer legt op de inzet van menselijke bronnen. Dit gebeurt door middel van subtiele relaties die vaak via onderzoekers, studenten, en zakelijke vertegenwoordigers worden opgebouwd. Deze methoden vormen een subtiele dreiging, waarbij persoonlijke contacten en langdurige netwerken worden ingezet om toegang te krijgen tot strategische kennis en informatie die van belang zijn voor de technologische en geopolitieke machtspositie van China. De recente gevallen in Groot-Brittannië, waarbij nep-headhunters parlementair personeel benaderden, wijzen op de toenemende complexiteit van deze spionagestrategieën.
Hoewel de spionage van China vaak niet hetzelfde politieke stigma heeft als de Russische activiteiten vanwege de oorlog in Oekraïne, is de dreiging evenzeer aanwezig. Grabowski benadrukt dat spionage steeds meer een ingeburgerd onderdeel is van internationale politiek, en dat Europa zich bewust moet worden van de blijvende en uitbreidende aanwezigheid van Chinese inlichtingendiensten.
Deze ontwikkelingen hebben aanzienlijke gevolgen voor de digitale veiligheid in Europa, vooral op het gebied van onderzoeks- en technologische samenwerking. Het is belangrijk dat Europese landen zich voorbereiden op een breder scala aan spionagedreigingen, niet alleen in de vorm van cyberaanvallen, maar ook door fysieke infiltratie en langdurige relaties die toegang geven tot gevoelige informatie.

WhatsApp API-kwetsbaarheid stelt onderzoekers in staat 3,5 miljard accounts te extraheren

Onderzoekers van de Universiteit van Wenen en SBA Research hebben ontdekt dat een kwetsbaarheid in de WhatsApp API hen in staat stelde om 3,5 miljard accounts van het platform te extraheren. Deze kwetsbaarheid zat in de contactdiscoveriefunctie van WhatsApp, die telefoonnummers controleert op de aanwezigheid van een account en de bijbehorende apparaten. Het probleem was het gebrek aan adequate rate limiting op de API, waardoor onderzoekers in staat waren om zonder restricties massale aanvragen naar de servers van WhatsApp te sturen.

De onderzoekers gebruikten een enkele server om meer dan 100 miljoen nummers per uur te controleren, wat resulteerde in een dataset met 3,5 miljard actieve WhatsApp-accounts. Ze ontdekten gegevens van gebruikers wereldwijd, waaronder profielafbeeldingen, "over"-tekst en informatie over de apparaten die aan een nummer waren gekoppeld. Het onderzoek toonde ook aan dat in landen waar WhatsApp geblokkeerd was, zoals China en Iran, het gebruik van de app doorging. Deze ontdekking illustreert een groter probleem met onbeveiligde API's, die gemakkelijk kunnen worden misbruikt voor grootschalige gegevensscraping. Dit type kwetsbaarheid is niet uniek voor WhatsApp; ook andere platforms, zoals Facebook en Twitter, zijn in het verleden slachtoffer geworden van vergelijkbare aanvallen. WhatsApp heeft inmiddels maatregelen genomen om de API te beschermen door rate-limiting in te voeren, maar het incident benadrukt de noodzaak voor strengere beveiliging van online platformen tegen misbruik van API's. Het lek van zo'n omvang kan ernstige gevolgen hebben voor de privacy van gebruikers, vooral omdat gegevens zoals telefoonnummers en profielinformatie jarenlang kunnen worden misbruikt voor andere kwaadaardige doeleinden.

VS meldt actief misbruik van kritiek RCE-lek in Oracle Identity Manager

De Verenigde Staten hebben gemeld dat er actief misbruik wordt gemaakt van een ernstige kwetsbaarheid in Oracle Identity Manager, een systeem voor gebruikersbeheer. Het beveiligingslek, aangeduid als CVE-2025-61757, stelt aanvallers in staat om op afstand willekeurige code uit te voeren (Remote Code Execution, RCE) op kwetsbare systemen. De impact van deze kwetsbaarheid wordt beoordeeld met een score van 9.8 op een schaal van 10, wat aangeeft hoe ernstig de risico's zijn.

Volgens het Amerikaanse Cybersecurity and Infrastructure Security Agency (CISA) is het lek al mogelijk misbruikt, hoewel de details van de aanvallen niet openbaar zijn gemaakt. Dit wordt bevestigd door een waarschuwing van het Nationaal Cyber Security Centrum (NCSC), die aangeeft dat er steeds meer scanverkeer wordt waargenomen. Dit wijst erop dat aanvallers actief zoeken naar systemen die kwetsbaar zijn voor deze kwetsbaarheid. De kans op een toename van misbruik is groot, vooral nu er Proof-of-Concept (PoC)-code beschikbaar is.

Het NCSC adviseert organisaties om de beveiligingsupdate, die op 21 oktober werd vrijgegeven, zo snel mogelijk te implementeren om schade te voorkomen. Aangezien de kwetsbaarheid al geruime tijd bekend is, wordt verwacht dat de aanvallen zich zullen intensiveren nu het lek verder verspreid wordt. De Amerikaanse overheid heeft organisaties bovendien opgedragen de noodzakelijke updates voor 12 december te installeren.

Onderzoek naar Qilin ransomware-aanval onthult complex aanvalspad
Op 8 oktober 2025 werd een endpoint binnen een organisatie getroffen door een Qilin ransomware-aanval, die later werd onderzocht door analisten. Dit incident bood beperkte zichtbaarheid, aangezien de antivirussoftware pas na de aanval werd geïnstalleerd en slechts op één endpoint actief was. Hierdoor waren er maar weinig gegevensbronnen beschikbaar voor het onderzoek.
Het onderzoek begon met de meldingen van het beheerde antivirus (MAV), die pas na de installatie van de nieuwe software enkele verdachte activiteiten detecteerden. Door de Windows Event Logs te analyseren, werd ontdekt dat de aanvaller op 8 oktober 2025 toegang had gekregen tot het systeem en een ongeautoriseerde versie van de software voor externe toegang installeerde. Deze installatie leidde naar een extern IP-adres, dat verder werd onderzocht. Ook werd opgemerkt dat eerdere software-installaties, zoals LogMeIn, een rol speelden bij de aanvalspogingen.
Verdere analyse van de aangeleverde gegevens onthulde dat drie bestanden, r.ps1, s.exe en ss.exe, via de kwaadaardige software naar het systeem werden overgebracht. Van deze bestanden bleef r.ps1 op het systeem aanwezig, maar de pogingen om s.exe en ss.exe uit te voeren faalden, wat werd bevestigd door de logbestanden van de Windows Program Compatibility Assistant (PCA).
Tijdens het onderzoek werd tevens vastgesteld dat de aanvaller Windows Defender had uitgeschakeld, waardoor de ransomware kon worden uitgevoerd. Desondanks werd de ransomware uiteindelijk door Windows Defender gedetecteerd, wat suggereert dat de ransomware van een ander systeem in het netwerk werd uitgevoerd en zich via netwerkschijven verspreidde.
Deze analyse van de Qilin-aanval benadrukt het belang van het combineren van verschillende gegevensbronnen om het aanvalspad volledig te begrijpen. Ondanks de beperkte beschikbare gegevens was het mogelijk om het verloop van de aanval te reconstrueren, wat aantoont hoe cruciaal het is om meerdere bronnen te valideren bij het onderzoeken van cyberaanvallen.

Hackers doen zich voor als TechCrunch-journalisten om gevoelige informatie te stelen
Een nieuwe phishingcampagne richt zich op techmedewerkers door hackers die zich voordoen als journalisten van TechCrunch. De aanvallers proberen via e-mail toegang te krijgen tot bedrijfsnetwerken en vertrouwelijke gegevens. Ze maken gebruik van vervalste domeinen, imiteren de schrijfstijl van TechCrunch-rapporters en stellen gerichte vragen die legitiem lijken om hun doelwitten te misleiden. In sommige

gevallen gebruiken de hackers zelfs de identiteit van echte TechCrunch-medewerkers, waarbij ze e-mailextensies gebruiken die lijken op de officiële adressen van de site. TechCrunch waarschuwt dat deze aanvallen een verband vertonen met een "persistent threat actor," die eerder vergelijkbare methoden gebruikte om gegevens te stelen, vooral van bedrijven in de tech-, crypto- en cloudsector. De aanvallers proberen niet alleen toegang te krijgen tot systemen maar ook vertrouwelijke informatie door bijvoorbeeld kwaadwillende planningslinks te versturen. TechCrunch adviseert bedrijven om voorzichtig te zijn met media-invorderingen, en e-mailverzoeken altijd via officiële kanalen te verifiëren. Dit helpt niet alleen de eigen organisatie te beschermen, maar ook het vertrouwen in de journalistiek te behouden. Het bedrijf roept bedrijven op om alert te blijven en phishingaanvallen actief te melden.

Online winkelen op Black Friday: verhoogde risico's op digitale dreigingen
Met de naderende feestdagen en de Black Friday-uitverkoop richten veel consumenten zich op online winkelen, maar dit brengt ook verhoogde digitale risico's met zich mee. Cybercriminelen maken gebruik van de drukte rondom populaire winkeldagen zoals Black Friday en Cyber Monday om online fraude en phishing-aanvallen te verspreiden. Het is belangrijk om waakzaam te zijn voor valse webshops, diefstal van betalingsgegevens en andere vormen van cybercriminaliteit die zich voordoen in de feestdagenperiode.
Aangezien consumentenbestedingen een aanzienlijk deel van de economie vormen, is het van groot belang om te letten op de potentiële cyberdreigingen die hiermee gepaard gaan. Cybercriminelen kunnen profiteren van verhoogde koopactiviteit door zich voor te doen als betrouwbare verkopers. Het is essentieel dat consumenten alert blijven en beveiligingsmaatregelen nemen bij online aankopen.

Misbruikte kwetsbaarheden in Nederland, België en wereldwijd
De afgelopen weken is er een opvallende stijging geweest in het aantal aanvallen gericht op kwetsbaarheden in verschillende software- en hardwareproducten, zowel in Nederland als België, maar ook wereldwijd. Dit overzicht geeft inzicht in de meest geëxploiteerde kwetsbaarheden, met een focus op de urgentie van de patches en beveiligingsmaatregelen die genomen moeten worden.
In Nederland staat Metabase op nummer één met de CVE-2023-38646, een kwetsbaarheid die voorkomt in de open-source business intelligence tool. Deze kwetsbaarheid wordt actief misbruikt, met een opvallend hoog aantal aanvallen in de afgelopen dagen en weken. Andere veelgebruikte kwetsbaarheden zijn te vinden in Cisco RV320/RV325 routers, die sinds 2019 bekend zijn, en in de populaire Apache

Hadoop YARN ResourceManager, die bedrijven helpen bij het verwerken van grote hoeveelheden data. De kwetsbaarheden in deze systemen variëren van misconfiguraties die eenvoudig te exploiteren zijn, tot ernstige beveiligingslacunes die complexere aanvallen mogelijk maken.
In België zien we soortgelijke trends, met kwetsbaarheden in de Dahua DVR/NVR/IPC-apparaten die in beveiligingssystemen worden gebruikt. Deze apparaten zijn in toenemende mate doelwit van aanvallen door de slechte beveiliging van standaardinstellingen. Daarnaast zijn er kwetsbaarheden gedetecteerd in CrushFTP, die een aanzienlijke impact hebben op de veiligheid van bedrijven die afhankelijk zijn van veilige bestandsoverdracht.
De risico's die voortvloeien uit deze kwetsbaarheden kunnen ernstig zijn, variërend van datalekken tot ransomware-aanvallen die gevoelige bedrijfsinformatie compromitteren. Deze kwetsbaarheden kunnen bovendien de deur openen voor langdurige toegang van aanvallers, wat het herstel en de schadebeperkingen bemoeilijkt. Het is van groot belang dat bedrijven en organisaties in Nederland, België en wereldwijd de nodige beveiligingspatches toepassen en ervoor zorgen dat hun systemen up-to-date blijven om dit soort aanvallen te voorkomen.
Dit overzicht toont de noodzaak van continue waakzaamheid in het beheer van netwerk- en softwarebeveiliging. Kwetsbaarheden die lange tijd onopgemerkt blijven, kunnen een aanzienlijk gevaar vormen voor de digitale infrastructuur van bedrijven en overheidsinstellingen wereldwijd.

Top 10 Trending CVE's op Sociale Media: Kritieke Kwetsbaarheden en Hun Risico's
In de afgelopen 24 uur zijn er verschillende kritieke kwetsbaarheden (CVE's) trending op sociale media, wat aangeeft dat deze kwetsbaarheden de aandacht van beveiligingsexperts en cybercriminelen hebben getrokken. Deze zogenaamde 'hype score', variërend van 0 tot 100, reflecteert hoe vaak en op welke wijze de kwetsbaarheden worden besproken, wat de urgentie en potentiële dreiging van elk probleem benadrukt.
CVE-2025-65018 is een heap buffer overflow-kwetsbaarheid in de populaire bibliotheek libpng, die wordt geactiveerd wanneer 16-bit interlaced PNG-afbeeldingen worden verwerkt. Het misbruiken van deze kwetsbaarheid kan leiden tot verlies van gegevens, denial of service, of zelfs de uitvoering van willekeurige code op getroffen systemen. De hype score van 37 geeft de significante zorg aan die dit probleem teweegbrengt, vooral gezien het brede gebruik van libpng in tal van softwareapplicaties.
Een andere veelbesproken kwetsbaarheid is CVE-2025-4123, een cross-site scripting (XSS) kwetsbaarheid in Grafana. Ondanks dat aanvallers deze kwetsbaarheid kunnen

uitbuiten zonder specifieke rechten, kan dit leiden tot ongewenste doorverwijzingen naar kwaadaardige websites en mogelijk verder escaleren tot server-side request forgery (SSRF). De hype score van 20 wijst op een opkomende dreiging, vooral gezien het gebruik van Grafana in veel kritieke infrastructuren.
Daarnaast zijn er verschillende andere kwetsbaarheden die de aandacht trekken, zoals CVE-2025-59287, die een remote code-executie in de Windows Server Update Service (WSUS) mogelijk maakt, en CVE-2025-58034, een OS command injection-kwetsbaarheid in Fortinet FortiWeb, die geauthenticeerde aanvallers in staat stelt ongeautoriseerde code uit te voeren.
Kwetsbaarheden zoals CVE-2025-41115, die gebruikersimpersonatie in Grafana Enterprise en Grafana Cloud mogelijk maakt, en CVE-2025-61757, die het mogelijk maakt voor aanvallers om de Oracle Fusion Middleware Identity Manager te compromitteren, voegen zich bij de lijst van bedreigingen die de komende dagen nauwlettend in de gaten gehouden moeten worden.
Ook zijn er kwetsbaarheden die minder bekend zijn, zoals CVE-2025-64755, die een bypass van het sed-commando in de Claude Code-tool betreft, en CVE-2025-64446, die unauthenticeerde aanvallers toegang geeft tot administratieve functies van Fortinet FortiWeb.
Beveiligingsteams moeten zich bewust zijn van deze kwetsbaarheden en de nodige stappen ondernemen om hun systemen te beschermen tegen mogelijke uitbuiting. Het monitoren van deze trending CVE's biedt een cruciaal inzicht in de potentiële risico's die organisaties kunnen bedreigen.

Minister: AIVD waarschuwt voor risico's bij vrijwillige chatcontrole
Minister Van Oosten van Justitie en Veiligheid heeft de zorgen van de AIVD over het Deense voorstel inzake chatcontrole bevestigd. Volgens de AIVD brengt de mogelijkheid van vrijwillige chatcontrole aanzienlijke risico's voor de digitale weerbaarheid met zich mee. Het voorstel, dat binnenkort als hamerstuk wordt behandeld tijdens de Corepervergadering, zou chatdiensten kunnen verplichten berichten van gebruikers te controleren. Dit wordt gezien als een bedreiging voor zowel de privacy als de beveiliging, vooral door de ondermijning van end-to-end encryptie.
De Europese Commissie heeft een plan gepresenteerd waarbij chatdiensten verplicht zouden worden om berichtinhoud te scannen, wat verdeeldheid veroorzaakt binnen de EU-lidstaten. Nederland heeft aangegeven zich van de stemming te onthouden, maar het voorstel blijft de mogelijkheid van vrijwillige chatcontrole openhouden. Deze controle zou als maatregel tegen de verspreiding van illegaal materiaal zoals seksueel kindermisbruik gebruikt kunnen worden. Minister Van Oosten wees erop

dat er een clausule is toegevoegd aan het voorstel, waarin wordt aangegeven dat over drie jaar wordt beoordeeld of chatcontrole alsnog verplicht wordt. De AIVD heeft echter aangegeven dat de risico's voor de digitale veiligheid door dergelijke maatregelen zeer hoog zijn.
Dit voorstel zal op 26 november verder besproken worden.

CrowdStrike ontslaat medewerker na uitlekken vertrouwelijke informatie
Cybersecuritybedrijf CrowdStrike heeft een medewerker ontslagen nadat werd ontdekt dat deze vertrouwelijke interne screenshots had gedeeld. De beelden, die door de hacker-groep Scattered Lapsus$ Hunters op Telegram werden gepubliceerd, wekten de indruk dat de systemen van CrowdStrike waren gecompromitteerd. De afbeeldingen bevatten onder meer een dashboard van interne systemen. De aanvallers claimden dat ze via een aanval op Gainsight toegang hadden gekregen tot de systemen van CrowdStrike, maar het bedrijf ontkende deze bewering en stelde dat de systemen niet waren gehackt. De screenshots bleken afkomstig te zijn van een werknemer die deze extern had gedeeld. De zaak is overgedragen aan de autoriteiten voor verder onderzoek. Dit incident benadrukt de risico’s van insider threats en de noodzaak voor organisaties om strikte beveiligingsmaatregelen en toezicht te handhaven.

Kabinet onderzoekt mogelijke gevolgen overname cloudbedrijf Solvinity door Kyndryl
Het demissionaire kabinet heeft aangekondigd de overname van het cloudbedrijf Solvinity door het Amerikaanse bedrijf Kyndryl nog niet te blokkeren, maar de implicaties voor de digitale veiligheid van Nederland zorgvuldig te onderzoeken. Solvinity speelt een cruciale rol in het hosten van overheidsdiensten zoals DigiD, MijnOverheid, en het beveiligde communicatiesysteem van het ministerie van Justitie en Veiligheid. De overname heeft tot bezorgdheid geleid, met name over de afhankelijkheid van de overheid van buitenlandse techbedrijven en de mogelijke risico’s voor de cybersecurity van deze vitale diensten.
Minister Frank Rijkaart van Binnenlandse Zaken gaf aan dat het kabinet momenteel onderzoekt of en welke risico's deze overname met zich mee zou kunnen brengen. Diverse partijen in de Tweede Kamer hebben Kamervragen gesteld over de mogelijkheden om de overname te blokkeren, maar Rijkaart benadrukte dat het nog te vroeg is voor dergelijke maatregelen. Hij stelde dat er eerst goed moet worden gekeken naar de werkelijke gevolgen van de overname.
De zorgen over de overname hebben betrekking op de invloed die een buitenlandse partij kan uitoefenen op de digitale infrastructuur van de Nederlandse overheid, die

gevoelig is voor cyberdreigingen. Deze kwestie wordt ook kritisch gevolgd door ICT-experts en politiek Nederland, die vrezen voor een afname van de controle over essentiële digitale diensten. Het kabinet blijft de situatie monitoren en benadrukt de zorgvuldigheid van het proces.

Beperkingen bij Amerikaanse verkiezingsbeveiliging roepen zorgen op voor internationale veiligheid

De Cybersecurity and Infrastructure Security Agency (CISA), verantwoordelijk voor de bescherming van kritieke infrastructuur in de Verenigde Staten, heeft ingrijpende veranderingen ondergaan die gevolgen hebben voor de beveiliging van verkiezingen. Sinds de tweede ambtstermijn van voormalig president Trump heeft de CISA te maken met budgetverlagingen, personeelsverminderingen en verschuivende prioriteiten, waardoor de federale steun voor de beveiliging van verkiezingen in diverse staten afnam. Deze situatie heeft geleid tot bezorgdheid onder verkiezingsfunctionarissen, die zich nu genoodzaakt zien om alternatieve maatregelen te zoeken voor het waarborgen van de verkiezingsbeveiliging.
In verschillende Amerikaanse staten, waaronder Californië en Pennsylvania, was CISA nauwelijks betrokken bij de recente verkiezingen, wat resulteerde in een verhoogde afhankelijkheid van lokale autoriteiten en externe cybersecurity-experts. De situatie benadrukt het groeiende belang van robuuste nationale en internationale samenwerking in de strijd tegen cyberdreigingen die verkiezingen kunnen ondermijnen, iets wat ook relevant is voor Europese landen zoals Nederland en België, waar soortgelijke dreigingen kunnen optreden.
Gezien de wereldwijde toename van hybride aanvallen, waarbij digitale en fysieke dreigingen elkaar versterken, blijft de vraag of CISA in de toekomst nog voldoende capaciteit heeft om verkiezingen adequaat te beschermen. Dit nieuws roept belangrijke vragen op over de rol van overheidsinstanties bij het beschermen van democratische processen tegen cyberaanvallen en beïnvloeding door buitenlandse machten.

Iberia onthult datalek na beveiligingsinbreuk bij leverancier

Iberia, de grootste luchtvaartmaatschappij van Spanje, heeft een datalek onthuld dat veroorzaakt werd door een beveiligingsinbreuk bij een van haar externe leveranciers. Het incident, dat werd gemeld nadat een dreigingsactor op hackerforums beweerde 77 GB aan gegevens van de luchtvaartmaatschappij te hebben gestolen, betreft voornamelijk persoonlijke klantinformatie, zoals namen, e-mailadressen en loyaliteitskaartnummers van Iberia Club.

De luchtvaartmaatschappij benadrukt dat geen toegang werd verkregen tot klantaccountgegevens of betaalinformatie. Iberia heeft onmiddellijk haar beveiligingsmaatregelen aangescherpt en extra bescherming toegevoegd rond klant-e-mailadressen, waarbij nu een verificatiecode vereist is voor wijzigingen aan deze adressen. Daarnaast worden systemen nauwlettend gemonitord op verdachte activiteiten, en zijn relevante autoriteiten geïnformeerd.
Het is nog onduidelijk of het gelekte datamateriaal daadwerkelijk verband houdt met de gegevens die de aanvaller claimde te hebben bemachtigd. De inbreuk benadrukt echter de kwetsbaarheid van externe leveranciers in de supply chain van bedrijven, wat een belangrijk aandachtspunt is voor organisaties die afhankelijk zijn van derde partijen voor het beheren van klantinformatie.

Eerste volledig AI-gegeneerde bioscoopfilm: risico's voor de cybersecuritysector
De opkomst van kunstmatige intelligentie (AI) in de filmindustrie is een teken van de toekomst, maar het roept ook belangrijke vragen op voor de cybersecuritysector. Luma AI, een Amerikaans bedrijf, is bezig met de ontwikkeling van de eerste volledig door AI gegenereerde bioscoopfilm, die al in 2026 op de markt zou kunnen komen. Dit project is deels gefinancierd door het Saoedische bedrijf Humain, dat een prominente rol wil spelen in de wereldwijde AI-markt.
Deze technologische vooruitgang heeft verstrekkende implicaties voor de filmindustrie, maar kan ook nieuwe cyberdreigingen creëren. AI wordt al ingezet voor het maken van hyperrealistische deepfakes en het manipuleren van media, wat risico's met zich meebrengt voor misinformatie en identiteitsfraude. De enorme hoeveelheden data die AI-systemen zoals die van Luma verzamelen, kunnen bovendien leiden tot nieuwe kwetsbaarheden in de beveiliging, vooral wanneer dergelijke technologieën worden ingezet door kwaadwillende actoren.
Met de enorme investering die Luma AI heeft ontvangen, vooral uit Saoedi-Arabië, komt er waarschijnlijk meer focus op AI-gebaseerde toepassingen in andere sectoren, waaronder cybercrime. Het zou niet verrassend zijn als AI in de toekomst een sleutelrol gaat spelen bij het uitvoeren van cyberaanvallen, bijvoorbeeld door geautomatiseerde phishingcampagnes of de inzet van AI voor het ontwikkelen van complexere malware.
Daarnaast opent de opkomst van AI-gegeneerde content de deur voor nieuwe vormen van digitale fraude, waarbij zowel bedrijven als consumenten in gevaar kunnen komen. Het is van cruciaal belang dat de cybersecuritysector zich voorbereidt op de potentiële dreigingen die deze ontwikkelingen met zich meebrengen.