Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

26-11-2025:

Rusland besteedt ongekende €400 miljoen om invloed uit te oefenen op Moldavische verkiezingen via digitale manipulatie

De Moldavische parlementsverkiezingen van september 2025 stonden in het teken van een aanzienlijke buitenlandse inmenging. Igor Grosu, voorzitter van het Moldavische parlement en leider van de pro-Europese Actie en Solidariteitspartij (PAS), verklaarde dat Rusland bijna €400 miljoen had geïnvesteerd om de verkiezingen te beïnvloeden. Dit gebeurde via een combinatie van cyberaanvallen, grootschalige desinformatiecampagnes en andere digitale manipulatiepogingen. Moldavië, dat zich positioneert tussen Rusland en de Europese Unie, werd doelwit van Russische hybride oorlogsvoering. Moskou zou geavanceerde cyberaanvallen hebben uitgevoerd om de verkiezingsinfrastructuur te verstoren, informatie te manipuleren en valse narratives te verspreiden via sociale media. Daarnaast werden er pogingen ondernomen om straatgeweld aan te wakkeren als middel om de politieke situatie te destabiliseren.
Ondanks deze digitale aanvallen en de poging van Rusland om politieke steun te verkrijgen voor pro-Kremlin partijen, behield de pro-Europese PAS een meerderheid van de zetels in het parlement. Het resultaat werd gezien als een overwinning voor de digitale veerkracht van het land en het vermogen om zich tegen cyberdreigingen te verzetten, waarmee Moldavië zijn koers naar de Europese Unie bevestigde.

Drones in Europees luchtruim: Nederland verhoogt maatregelen tegen dreiging

De afgelopen periode is er een toename van drone-incidenten in Europa, wat ernstige zorgen oproept over de beveiliging van luchtruimen en strategische locaties. Recent zijn in Roemenië gevechtsvliegtuigen ingezet om drones nabij de grens met Oekraïne te volgen. Ook in Nederland werden drones gesignaleerd bij de militaire vliegbasis Volkel, wat leidde tot verstoringen in het vliegverkeer rondom Eindhoven Airport. Dergelijke incidenten zijn niet uniek en worden steeds vaker gemeld in landen als België, Frankrijk, Duitsland en Zweden.
Deze ontwikkelingen hebben geleid tot een versterkte inzet van middelen door het ministerie van Defensie. In reactie op de dreiging wordt er tussen de 1,25 en 3 miljard euro geïnvesteerd in de verbetering van de Nederlandse antidronecapaciteit. Dit omvat de aanschaf van geavanceerde technologieën, zoals antidronekanonsystemen en onderscheppingsdrones, evenals investeringen in de bescherming van marineschepen tegen drone-aanvallen. De eerste van deze nieuwe systemen, waaronder de Skyranger 30, wordt pas in 2028 verwacht.

Deze maatregelen zijn noodzakelijk geworden door de moeilijkheden die gepaard gaan met het onderscheppen van drones, die een steeds grotere uitdaging vormen voor de nationale en Europese veiligheid. Het ministerie van Defensie benadrukt dat het effectief inzetten van dronesystemen een 'kat-en-muisspel' is, waarbij snelle innovaties vereist zijn om de dreiging te neutraliseren.
Voor Nederland en België is het van groot belang dat de impact van deze nieuwe dreiging goed begrepen wordt, vooral gezien de mogelijkheid dat drones ook gebruikt kunnen worden voor cyberaanvallen of spionage.

Bedrijfsleven kwetsbaar voor geopolitieke risico's, een halve dag stroomuitval is al problematisch

Het Nederlandse bedrijfsleven is kwetsbaar voor verstoringen van essentiële voorzieningen, zoals stroomuitval, communicatie-uitval of andere ICT-diensten. Volgens het onderzoek van de Amsterdam Business School, gepubliceerd in de Nederlandse Innovatiemonitor, kan een bedrijf al na een halve dag zonder deze vitale voorzieningen niet meer functioneren. Gezien de toename van cyberdreigingen, zoals DDoS-aanvallen en ransomware, is deze afhankelijkheid van ICT-diensten problematisch. Bedrijven die onvoldoende voorbereid zijn op dergelijke verstoringen, kunnen ernstige operationele problemen ondervinden.
De monitor toont aan dat langdurige verstoringen, zoals een week zonder essentiële voorzieningen, het functioneren van bedrijven in Nederland vrijwel onmogelijk maken. Het is opvallend dat minder dan de helft van de ondervraagde bedrijven zich zorgen maakt over de geopolitieke risico's die kunnen leiden tot verstoringen van vitale infrastructuren. Dit gebrek aan bewustzijn onder bedrijven over de impact van geopolitieke conflicten en cyberdreigingen kan de bedrijfscontinuïteit ernstig bedreigen.
Ondanks de kritieke rol die ICT- en communicatiediensten spelen in de bedrijfsvoering, heeft een op de vijf bedrijven geen voorzorgsmaatregelen getroffen voor het geval deze voorzieningen uitvallen. Het onderzoek benadrukt dat bedrijven meer actie moeten ondernemen om zich beter voor te bereiden op cyberincidenten en andere verstoringen van vitale infrastructuren.
Henk Volberda, hoogleraar strategie en innovatie aan de Universiteit van Amsterdam, noemt de bevindingen zorgwekkend. Hij wijst erop dat de overheid weliswaar maatregelen neemt om burgers voor te bereiden op noodsituaties, maar dat bedrijven veel minder aandacht schenken aan hun eigen kwetsbaarheid voor cyberaanvallen en geopolitieke risico's.
Het onderzoek benadrukt verder dat bedrijven in Nederland zich meer moeten richten op hun digitale veerkracht, waaronder het versterken van hun

cyberbeveiliging en het nemen van maatregelen tegen potentiële stroom- en communicatiestoringen die door geopolitieke conflicten kunnen worden veroorzaakt. Bedrijven die zich onvoldoende voorbereiden op dergelijke risico's, kunnen geconfronteerd worden met ernstige gevolgen voor hun operaties.

Russische hackers richten zich op Amerikaans ingenieursbedrijf vanwege Oekraïens zusterstadproject

Deze herfst werd een Amerikaans ingenieursbedrijf het doelwit van een cyberaanval, vermoedelijk uitgevoerd door hackers die werken voor de Russische inlichtingendienst. De aanval werd uitgevoerd omdat het bedrijf betrokken was bij een project voor een Amerikaanse stad die een zusterstad heeft in Oekraïne. Dit incident onderstreept de steeds geavanceerdere tactieken van de Russische cyberoorlog en laat zien dat Rusland zijn aanvallen uitbreidt naar een bredere groep doelwitten, waaronder overheden, organisaties en privébedrijven die, al is het maar indirect, Oekraïne ondersteunen.

De aanval werd geïdentificeerd door het Amerikaanse cybersecuritybedrijf Arctic Wolf, dat in september waarschuwde voor de aanval voordat het de operaties van het ingenieursbedrijf zou kunnen verstoren. Het bedrijf zelf had geen directe betrokkenheid bij de Russische invasie van Oekraïne, maar de hackergroep achter de aanval, bekend als RomCom, richt zich regelmatig op organisaties die Oekraïne ondersteunen, zowel op civiel als defensief vlak.

Volgens Ismael Valenzuela, vicepresident van Arctic Wolf, richt de groep zich doorgaans op organisaties die direct betrokken zijn bij het ondersteunen van Oekraïense instellingen, het leveren van diensten aan Oekraïense gemeenten, of het ondersteunen van civiele, defensieve of overheidsfuncties van Oekraïne. Deze aanval volgt kort na een waarschuwing van de FBI over de activiteiten van hackers die banden met Rusland hebben en die proberen toegang te krijgen tot Amerikaanse netwerken, met als doel belangrijke systemen in gevaar te brengen of kritieke infrastructuur te verstoren.

Het is duidelijk dat de Russische hackers meerdere motieven hebben, variërend van het verstoren van de humanitaire en militaire steun aan Oekraïne tot het bestraffen van bedrijven met banden met Oekraïne of het stelen van militaire of technologische geheimen. Dit incident toont aan hoe de digitale dreiging in de context van geopolitieke conflicten steeds breder en complexer wordt.

Honderden kwetsbare Monsta FTP-clients toegankelijk vanaf internet

Honderden installaties van Monsta FTP, een webgebaseerde FTP-client, vertonen een ernstige kwetsbaarheid die vanaf het internet toegankelijk is. Deze kwetsbaarheid,

aangeduid als CVE-2025-34299, stelt aanvallers in staat om op afstand willekeurige code uit te voeren op getroffen systemen. Via een malafide FTP-server kunnen aanvallers bestanden naar de kwetsbare clients uploaden en deze op door hen opgegeven locaties plaatsen. Het uitvoeren van malware is een van de risico's die hierbij ontstaat.
De kwetsbaarheid werd verholpen in versie 2.11.3 van Monsta FTP, die op 26 augustus werd uitgebracht. Echter, in de release-notes werd geen melding gemaakt van deze kritieke kwetsbaarheid, wat de transparantie van de ontwikkelaars aantast. De ernst van de kwetsbaarheid wordt beoordeeld met een score van 9.3 op de CVSS-schaal, wat wijst op de hoge impact die dit kan hebben op de systemen die niet zijn gepatcht.
Hoewel de beveiligingsupdate al beschikbaar is, blijkt uit onderzoek van The Shadowserver Foundation en het beveiligingsbedrijf watchTowr dat er wereldwijd nog honderden kwetsbare Monsta FTP-clients toegankelijk zijn vanaf het internet. Bij de laatste metingen waren er nog ongeveer achthonderd kwetsbare systemen, waarvan er dertien in Nederland en vier in België werden aangetroffen.
Dit incident benadrukt het belang van regelmatige updates en het tijdig patchen van software om te voorkomen dat systemen kwetsbaar blijven voor exploitatie.

VS waarschuwt WhatsApp- en Signal-gebruikers voor spyware-aanvallen
Het Amerikaanse Cybersecurity and Infrastructure Security Agency (CISA) heeft gebruikers van de populaire chatapplicaties WhatsApp en Signal gewaarschuwd voor recente aanvallen met commerciële spyware. Deze aanvallen richten zich voornamelijk op hooggeplaatste individuen, zoals overheidsfunctionarissen, militairen en politici, maar ook op maatschappelijke organisaties en individuen in Europa, de Verenigde Staten en het Midden-Oosten. De aanvallers maken gebruik van geavanceerde technieken, waaronder phishing, malafide QR-codes en zeroclick-exploits, die geen enkele interactie van het slachtoffer vereisen om toegang te verkrijgen tot de chatapplicaties en de telefoons van de doelwitten.
Signal-gebruikers waren eerder dit jaar al doelwit van dergelijke aanvallen, waarbij apps werden gepromoot die zich voordeden als de originele chatapplicaties. Daarnaast wordt er melding gemaakt van aanvallers die proberen toegang te krijgen via gespoofte applicaties of misbruik maken van kwetsbaarheden in de software van de apps.
Het CISA adviseert gebruikers om veiligheidsmaatregelen te treffen, zoals het inschakelen van specifieke beveiligingsinstellingen op zowel iPhone- als Android-apparaten, en het beperken van de permissies van apps. Ook wordt gebruikers afgeraden om SMS-berichten te gebruiken voor gevoelige communicatie, gezien de

kwetsbaarheid van dit kanaal. De CISA benadrukt verder het belang van het volgen van best practices voor mobiele communicatie om het risico op spyware-aanvallen te verminderen.

Malafide Blender-bestanden verspreiden StealC infostealer malware via 3D-modellen

Een nieuwe campagne verspreidt de StealC V2 infostealer malware via malafide Blender-bestanden, die zijn geüpload naar 3D-model marktplaatsen zoals CGTrader. Deze aanval wordt toegeschreven aan Russische dreigingsactoren en maakt gebruik van Blender's mogelijkheid om Python-scripts uit te voeren voor automatisering van workflows en het laden van aangepaste interfacepanelen. Door de Auto Run-functie in Blender te gebruiken, kunnen kwaadaardige scripts automatisch geladen worden wanneer gebruikers een 3D-model openen.
Onderzoekers van Morphisec hebben bevestigd dat de malafide Blender-bestanden een malware-loader ophalen van een Cloudflare Workers-domein. Dit script laadt vervolgens een PowerShell-script dat twee ZIP-bestanden met de namen ZalypaGyliveraV1 en BLENDERX ophaalt. Deze bestanden worden uitgepakt in de tijdelijke map van de computer en plaatsen opstartbestanden om de malware persistent te maken. De gedropte malware omvat de StealC V2 infostealer, die in staat is om gegevens te stelen van meer dan 23 verschillende browsers, meer dan 100 cryptocurrency wallet-extensies, en berichten- en e-mailclients zoals Telegram en Discord.
Ondanks dat de StealC malware al sinds 2023 bekend is, is het moeilijk te detecteren voor antivirussoftware. Dit benadrukt de noodzaak voor 3D-modellisten en gebruikers van dergelijke marktplaatsen om extra voorzichtig te zijn bij het downloaden van bestanden van onbekende of onbetrouwbare bronnen. Het wordt sterk aangeraden om de Auto Run-functie in Blender uit te schakelen en om alleen bestanden van vertrouwde uitgevers te gebruiken.

Onbeveiligde codeformatters lekken duizenden gevoelige gegevens van organisaties wereldwijd

Onderzoekers hebben vastgesteld dat via de online codeformatters JSONFormatter en CodeBeautify duizenden gevoelige gegevens van organisaties wereldwijd tijdelijk openbaar toegankelijk waren. Het gaat om wachtwoorden, authenticatiesleutels, configuratiebestanden en persoonsgegevens die afkomstig zijn uit sectoren zoals overheid, bankwezen, kritieke infrastructuur, gezondheidszorg, verzekeringen, telecommunicatie, technologie en cybersecurity. Deze gegevens waren toegankelijk

via de recente links functie van de platforms, waar gebruikers opgeslagen JSON bestanden konden delen via directe links.
Bij het opslaan van codefragmenten bieden de platforms een link waarmee de inhoud kan worden geraadpleegd. Deze links bleken zonder enige vorm van beveiliging publiek beschikbaar en volgens de onderzoekers ook gemakkelijk vindbaar via geautomatiseerd zoeken. In totaal werden meer dan 80.000 JSON bestanden verzameld, goed voor ruim 5 gigabyte aan informatie, die in sommige gevallen jaren online beschikbaar was. De inhoud bevatte onder meer inloggegevens voor Active Directory, cloudomgevingen, databases, API tokens, privésleutels en configuratiebestanden van gevoelige systemen. In bepaalde gevallen betrof het bestanden die interne hostnamen, netwerkadressen, scripts voor systeemconfiguratie en registrysleutels bevatten.
Ook bleek dat kwaadwillende scanners actief op dergelijke gegevens jagen. Onderzoekers plaatsten testgegevens op de platforms, die ondanks verwijdering na 24 uur nog steeds werden opgehaald en getest door onbekende partijen. Een deel van de organisaties die werden geïnformeerd over het lek nam maatregelen, maar veel bestanden bleven toegankelijk via de onbeveiligde Recent Links omgeving.

JackFix gebruikt nep Windows-update pop-ups op volwassen websites om meerdere malware-stealers te verspreiden
Cybersecurity-experts hebben onlangs een kwaadaardige campagne ontdekt die gebruik maakt van nep Windows-update pop-ups op volwassen websites, waaronder kloons van xHamster en PornHub, om gebruikers te misleiden. Deze aanvallen maken gebruik van ClickFix-technieken, waarbij de aanvallers een valse "kritieke beveiligingsupdate" presenteren. Wanneer gebruikers hierop klikken, wordt schadelijke code uitgevoerd, die de systemen van slachtoffers infecteert met verschillende soorten malware.
De aanval wordt vermoedelijk verspreid via malvertising en sociale-engineeringtechnieken. Slachtoffers worden naar nep-websites geleid, die lijken op populaire volwassen platforms, en worden vervolgens misleid om een zogenaamd Windows-updateproces te starten. Dit leidt tot de uitvoering van een PowerShell-script, dat kwaadaardige software op het systeem installeert. De malware kan variëren van informatie-steelers zoals Rhadamanthys Stealer en Vidar Stealer tot meer geavanceerde remote access trojans (RATs).
Wat deze aanvallen bijzonder zorgwekkend maakt, is de moeilijkheid om de kwaadaardige code te detecteren. De aanvallers passen verschillende lagen van obfuscatie toe om te voorkomen dat de malware wordt geanalyseerd. Daarnaast

wordt er steganografie gebruikt om schadelijke code in afbeeldingen te verbergen, wat het voor onderzoekers uitdagend maakt om de volledige aanval te doorgronden. Deze aanvalstechnieken benadrukken het groeiende risico van ClickFix-aanvallen, waarbij de gebruiker onbewust zijn eigen systeem infecteert door een vals commando uit te voeren. Het gebruik van een nep Windows-update en de psychologische druk die hiermee gepaard gaat, maakt deze aanvallen bijzonder effectief.
In Nederland en België worden gebruikers steeds vaker het slachtoffer van dit soort social engineering-aanvallen, waarbij malvertising en obfuscatie steeds vaker worden toegepast om beveiligingsmaatregelen te omzeilen. Bedrijven en particulieren moeten zich bewust zijn van deze dreiging en zorgvuldig omgaan met pop-ups die hen aansporen tot het uitvoeren van onbekende of verdachte commando's.

Is jouw Android TV-streamingbox onderdeel van een botnet?
De Superbox-streamingapparaten, die te koop zijn bij grote detailhandelaren zoals BestBuy en Walmart, bieden voor een eenmalige betaling van ongeveer $400 toegang tot duizenden betaalde streamingdiensten zoals Netflix en ESPN. Deze producten lijken op het eerste gezicht een goede deal voor consumenten die op zoek zijn naar betaalbare toegang tot televisie- en filmcontent. Echter, experts wijzen op de risico's die verbonden zijn aan deze apparaten, die vaak beveiligingskwetsbaarheden bevatten die ze vatbaar maken voor misbruik in cybercriminaliteit.
In tegenstelling tot de officiële Android TV-apparaten, gebruiken deze Superbox-apparaten onofficiële software die het mogelijk maakt om content te streamen zonder de vereiste licenties, maar dit brengt ook beveiligingsrisico's met zich mee. De benodigde apps voor het streamen van onbeperkte content leiden de internetverbinding van gebruikers naar een gedistribueerd proxy-netwerk, wat vaak wordt misbruikt voor frauduleuze activiteiten zoals advertentiefraude en accountovername.
Beveiligingsexperts zoals Ashley van Censys hebben vastgesteld dat de Superbox-apparaten verbinding maken met servers van Tencent QQ en de proxyservice Grass IO. Dit soort onveilige verbindingen maken de apparaten kwetsbaar voor het worden opgenomen in botnets, die gebruikt kunnen worden voor allerlei vormen van cybercriminaliteit, van gegevensdiefstal tot het uitvoeren van grootschalige fraude. Hoewel de verkoop van dergelijke apparaten legaal is, moeten gebruikers zich bewust zijn van de risico's die gepaard gaan met het installeren van onofficiële apps. In Nederland en België kan het gebruik van dergelijke software zelfs leiden tot juridische

problemen, aangezien het mogelijk in strijd is met auteursrechtwetten en de digitale veiligheidsregels.
Daarnaast kan het gebruik van deze streamingboxen leiden tot compromittering van thuisnetwerken, waarbij gebruikers onbewust hun internetverbinding delen voor criminele doeleinden. Dit heeft implicaties voor de veiligheid van de gebruiker, die mogelijk hun persoonlijke gegevens en netwerk blootstelt aan externe bedreigingen. Voor Nederlandse en Belgische consumenten is het belangrijk om te begrijpen dat het aanschaffen van dergelijke apparaten niet zonder risico is. Naast de mogelijke juridische gevolgen kunnen de beveiligingsrisico's groot zijn, wat de integriteit van persoonlijke netwerken in gevaar kan brengen. Het gebruik van deze producten kan leiden tot deelname aan grotere netwerken van kwaadaardige bots, met gevolgen die verder gaan dan alleen het verlies van persoonlijke gegevens.

Amazon, Lidl, Costco en IKEA bovenaan de Black Friday scamlijsten in Nederland en België

Cybercriminelen zijn al vroeg begonnen met hun Black Friday phishingcampagnes, waarbij ze zich richten op zowel vroege koopjesjagers als de merken die zij vertrouwd vinden. Dit gebeurt niet alleen in de VS, maar ook in Nederland en België, waar vergelijkbare phishing-aanvallen zijn waargenomen. De eerste pogingen werden al begin november gedetecteerd, maanden voordat de gebruikelijke kortingen van Black Friday van start gingen. Volgens een analyse van KnowBe4 Threat Labs, een platform voor beveiligingsbewustzijnstraining, steeg het aantal Black Friday-gerelateerde phishingmails al op 1 november tot 8% van alle waargenomen e-mails. Deze vroege start van de phishingcampagnes helpt aanvallers om hun technieken te testen, filteringssystemen te omzeilen en consumenten die op zoek zijn naar vroege kortingen te misleiden. Door valse webwinkels op te zetten en frauduleuze aanbiedingen te verspreiden, kunnen criminelen profiteren van de hoge vraag naar kortingen tijdens de periode voor Black Friday.
De phishingpogingen richten zich op de bekende merken Amazon, Lidl, Costco en IKEA, die ook in Nederland en België veel consumenten aanspreken. Deze merken worden vaak geïmiteerd in phishingmails en frauduleuze websites. Deal Watchdogs, een populaire website voor het volgen van aanbiedingen, wordt vaak nagebootst in 84% van de phishingmails. De aanvallers gebruiken deze lokkertjes om consumenten te verleiden hun persoonlijke gegevens of betaalinformatie in te vullen.
Hoewel de piek in aanvallen na 1 november afneemt, blijven de phishingpogingen door de maand november heen consistent aanwezig. De meeste aanvallen richten zich op vroege bargain hunters en gebruiken thema's zoals kortingen op Amazon-apparaten of exclusieve aanbiedingen van populaire merken. In Nederland en België

zijn veel van deze scams gericht op bekende supermarkten zoals Lidl, evenals op internationale ketens zoals IKEA en Costco, waarbij frauduleuze cadeaubonaanbiedingen vaak worden verspreid.
Cybercriminelen maken gebruik van generatieve AI om frauduleuze websites steeds realistischer te maken. Deze websites bootsten aanbiedingen en banners van grote retailers na, en zetten countdown timers en schaarsteberichten in om consumenten te dwingen tot impulsieve aankopen. Ze maken ook gebruik van betaalde advertenties op Google en Meta om slachtoffers te lokken.
De waarschuwing is duidelijk: wees uiterst voorzichtig met aanbiedingen, vooral als ze te goed lijken om waar te zijn. Het is van belang om altijd te controleren of de website veilig is en de aangeboden deal te verifiëren om te voorkomen dat je slachtoffer wordt van een fraude.

Valse FFmpeg-update infecteert Mac-gebruikers met backdoor
Onderzoekers hebben een nieuwe aanval ontdekt waarbij Mac-gebruikers verleid worden om een valse update voor de populaire software FFmpeg te downloaden. Deze zogenaamde update blijkt in werkelijkheid een backdoor te installeren, waarmee aanvallers toegang krijgen tot het slachtoffer's systeem. De aanval begint vaak via een LinkedIn-bericht, waarin slachtoffers worden benaderd door een zogenaamde recruiter. Zij worden gevraagd om te solliciteren naar een functie en hiervoor een video-introductie in te sturen.
Wanneer slachtoffers de link naar de opgegeven website volgen, worden zij eerst gevraagd om een "job assessment" in te vullen. Daarna krijgen zij de opdracht om een video-introductie op te nemen. Als ze proberen toegang te krijgen tot de camera, krijgen ze de melding dat de toegang is geblokkeerd. De aanvallers laten hen vervolgens een "update" voor FFmpeg downloaden om het probleem op te lossen. Om deze update te verkrijgen, moeten slachtoffers een commando in de Terminal uitvoeren. Dit commando downloadt een script dat uiteindelijk de backdoor installeert.
Naast de backdoor wordt er ook een 'decoy' applicatie gedownload die zich voordoet als een waarschuwing van de Chrome-browser, met een verzoek om toegang tot de camera. Vervolgens verschijnt er een venster waarin om het wachtwoord van de gebruiker wordt gevraagd. Wat het slachtoffer invoert, wordt direct naar een Dropbox-account van de aanvallers gestuurd.
Deze aanval benadrukt de risico's van ongevraagde sollicitaties en de gevaren van het uitvoeren van onbekende commando's in de Terminal. Organisaties worden aangemoedigd hun medewerkers bewust te maken van dergelijke dreigingen en waakzaam te blijven voor verdachte sollicitatie-aanvragen.

Verdachte aangehouden na bankhelpdeskfraude in Hilversum
Op 18 juli 2025 werd een vrouw in Hilversum het slachtoffer van een bankhelpdeskfraude, waarbij een bedrag van bijna 10.000 euro werd gestolen. De fraudeur deed zich telefonisch voor als een medewerker van een bank, met het verhaal dat er verdachte transacties op de rekening van het slachtoffer waren aangetroffen. De vrouw werd vervolgens geïnformeerd dat een verzekeringsmedewerker langs zou komen om de situatie verder te onderzoeken.
De persoon die bij het slachtoffer aan de deur verscheen, beweerde een verzekeringsagent te zijn en vroeg haar om een code te verstrekken ter identificatie. Nadat de code werd doorgegeven, vroeg de verdachte om foto's van de sieraden en het contant geld van de vrouw te maken voor de verzekeringsdoeleinden. Toen het slachtoffer even afgeleid was, vluchtte de fraudeur met het contante geld.
De politie deelde beelden van de verdachte via sociale media en het opsporingsprogramma Bureau NH, wat leidde tot de herkenning van de verdachte. Dankzij meldingen uit het publiek werd de man, een minderjarige uit Almere, op 12 november 2025 aangehouden en verhoord.
Deze zaak benadrukt het belang van waakzaamheid en de waarde van meldingen vanuit het publiek bij het oplossen van misdrijven. Dankzij de tips van burgers kon de zaak snel worden opgelost.

EU-lidstaten akkoord met invoering van digitaal reisdocument op smartphone
EU-lidstaten hebben ingestemd met het voorstel van de Europese Commissie voor de invoering van het Digital Travel Credential (DTC), een digitaal reisdocument dat op smartphones kan worden gebruikt. Deze ontwikkeling heeft belangrijke implicaties voor digitale veiligheid, aangezien het reisdocument biometrische gegevens van gebruikers vereist voor grenscontrole. Het voorstel maakt het mogelijk om reisdocumenten via een smartphone-app te genereren, waarbij de chip van een paspoort wordt uitgelezen en gekoppeld aan een selfie voor gezichtsherkenning. De technologie werd getest op Schiphol, waar deelnemers via een speciale poort hun reis konden voortzetten na het uploaden van hun gegevens.
Hoewel de digitale toegangsgemakken kunnen verbeteren, roept de implementatie van biometrische verificatie zorgen op over privacy en gegevensbeveiliging. De bewaartermijn van reisgegevens is in lijn met de AVG en beperkt tot 24 uur na grenspassage, maar er is bezorgdheid over de potentiële risico's van datalekken of misbruik. De voorgestelde technologie zou een aanzienlijke toename van digitale identificatie en gegevensverwerking betekenen, wat nieuwe aanvalsvectoren voor cybercriminelen kan openen.

Nederland heeft zijn steun voor het voorstel uitgesproken, maar de definitieve goedkeuring van het Europees Parlement wordt nog afgewacht. Het is nog onbekend wanneer de onderhandelingen worden afgerond en wat de uiteindelijke impact zal zijn op de digitale privacy van burgers.

Tor Project vervangt encryptie-algoritme om privacy te versterken

Het Tor Project heeft besloten het encryptie-algoritme voor Tor-relays te vervangen door een nieuw systeem, genaamd Counter Galois Onion (CGO). Dit nieuwe algoritme moet gebruikers beter beschermen tegen aanvallen die de anonimiteit van het Tor-netwerk in gevaar kunnen brengen. Tor, dat wereldwijd door miljoenen gebruikers wordt ingezet voor anoniem internetverkeer, maakt gebruik van een netwerk van vrijwillige servers en relays die het verkeer van gebruikers omleiden om hun identiteit te verbergen.

Het vorige encryptie-algoritme bleek kwetsbaar voor aanvallen waarbij data binnen het netwerk gemanipuleerd werd. De nieuwe CGO-versie voorkomt zulke aanvallen door manipulatie van de versleutelde data onherstelbaar te maken, wat de veiligheid van communicatie binnen het netwerk aanzienlijk versterkt. Daarnaast biedt het nieuwe systeem verbeterde forward secrecy, wat betekent dat het ook oude communicatie beschermt, zelfs als de gebruikte sleutels in de toekomst worden gekraakt.

Hoewel de overgang naar het nieuwe systeem stapsgewijs zal plaatsvinden, kan het in de beginfase tot compatibiliteitsproblemen tussen oude en nieuwe relays leiden. Desondanks worden de beveiligingsvoordelen van de nieuwe technologie gezien als een belangrijke stap in het verbeteren van de privacy en veiligheid van Tor-gebruikers wereldwijd.

Signal introduceert end-to-end versleutelde back-ups voor iOS

Signal heeft een belangrijke update aangekondigd door end-to-end versleutelde back-ups nu ook beschikbaar te maken voor iOS-gebruikers. Deze functie was eerder al voor Android-gebruikers toegankelijk. Met deze nieuwe mogelijkheid kunnen gebruikers hun berichten en media, zoals foto’s, video's, en bestanden, veilig opslaan in een versleutelde back-up. De gratis versie biedt 100 MB opslag voor berichten en media van de afgelopen 45 dagen. Voor gebruikers die meer opslag wensen, is er een betaalde versie beschikbaar voor $1,99 per maand, waarmee 100 GB opslag wordt aangeboden en berichten langer dan 45 dagen bewaard kunnen worden.

De back-ups zijn beveiligd met een unieke herstelcode van 64 tekens, die alleen op het apparaat van de gebruiker wordt gegenereerd. Deze code is vereist om toegang

te krijgen tot de versleutelde gegevens, wat een extra beveiligingslaag biedt tegen ongeautoriseerde toegang.
Signal wil deze versleutelde back-upfunctie ook beschikbaar stellen voor de desktop-app, waarmee gebruikers hun versleutelde chatgeschiedenis kunnen synchroniseren tussen Android, iOS en desktop. Deze stap maakt deel uit van Signal's bredere missie om gebruikers volledige controle te geven over hun privé-informatie en om hen te beschermen tegen cyberdreigingen, zoals ongewenste toegang en datalekken.
Dit maakt Signal een nog sterkere keuze voor gebruikers die waarde hechten aan privacy en gegevensbeveiliging in hun dagelijkse communicatie.

Ssd-schijven verliezen data zonder stroom
Voor gebruikers van ssd-schijven is er een belangrijk risico op dataverlies wanneer de schijven gedurende langere tijd geen stroom ontvangen. In tegenstelling tot traditionele harde schijven, die data opslaan via magnetische schijven, gebruiken ssd's NAND-geheugen, waarin data door middel van elektrische ladingen wordt opgeslagen. Dit betekent dat wanneer er geen stroom op de schijf staat, de opgeslagen gegevens langzaam kunnen vervagen.
De snelheid waarmee data verloren gaat, is afhankelijk van het type NAND-geheugen in de ssd. Schijven met QLC (quad-level cell) NAND kunnen data slechts ongeveer één jaar bewaren zonder stroom, terwijl TLC (triple-level cell) NAND dit voor drie jaar volhoudt. MLC (multi-level cell) en SLC (single-level cell) NAND kunnen respectievelijk vijf en tien jaar lang de gegevens bewaren zonder stroom. De meeste consumenten-ssd's gebruiken echter QLC of TLC NAND, wat het risico op dataverlies vergroot voor mensen die deze schijven voor langdurige opslag gebruiken.
Dit probleem heeft gevolgen voor de integriteit van opgeslagen data, vooral voor gebruikers die ssd-schijven gebruiken voor archivering of langetermijnopslag. De afname van de lading in de NAND-cellen kan leiden tot volledig verlies van gegevens of zelfs onbruikbare schijven. Aangeraden wordt om altijd een back-up te maken volgens de '3-2-1' regel, waarbij drie kopieën van de data op twee verschillende opslagmedia worden bewaard, waarvan één op een off-site locatie.
Het is belangrijk dat gebruikers zich bewust zijn van dit risico, vooral gezien de toenemende populariteit van ssd-schijven voor zowel dagelijks gebruik als voor archivering.

Minister Heinen begrijpt acceptatieplicht digitale euro voor winkels
Minister van Financiën, Heinen, heeft aangegeven begrip te hebben voor de mogelijke invoering van een acceptatieplicht voor de digitale euro in winkels en bedrijven. Deze reactie kwam na vragen van de VVD over de onderhandelingen die

momenteel in Europa plaatsvinden. EU-voorzitter Denemarken hoopt dit jaar nog tot een raadsakkoord te komen over de digitale euro.
Heinen benadrukte dat het gebruik van de digitale euro door consumenten vrijwillig blijft, maar de Europese Commissie wil winkels en bedrijven verplichten de digitale euro als wettig betaalmiddel te accepteren. Het kabinet staat positief tegenover deze verplichting, mits er een balans wordt gevonden tussen brede acceptatie en uitvoerbaarheid voor kleine bedrijven. Heinen gaf aan dat er mogelijk uitzonderingen kunnen komen voor bepaalde situaties.
Het kostenmodel van de digitale euro wordt momenteel nog besproken, en volgens de Europese Centrale Bank kunnen de kosten voor de invoering tussen de 4 en 5,77 miljard euro liggen. De minister benadrukte dat basisdiensten voor consumenten gratis moeten blijven, hoewel banken extra kosten kunnen doorberekenen voor aanvullende diensten.
Heinen merkte op dat er enige spanning bestaat tussen het beschermen van winkeliers tegen hoge kosten en het compenseren van betaaldienstverleners voor gemaakte kosten. Het voorgestelde compensatiemodel voorziet in maximumkosten die betaaldienstverleners aan winkeliers mogen doorberekenen.

AIVD waarschuwt voor risico's bij chatcontrole en toegang tot mobiele gegevens
De AIVD heeft recentelijk gewaarschuwd voor de potentiële cybersecurityrisico’s die verbonden zijn aan de infrastructuur die nodig is voor chatcontrole. Dit systeem, dat bedoeld is om misbruikmateriaal zoals CSAM (Child Sexual Abuse Material) te detecteren, kan kwaadwillenden toegang verschaffen tot grote hoeveelheden persoonlijke gegevens op mobiele apparaten. Deze zorgen werden geuit naar aanleiding van een Deens voorstel om chatcontrole permanent te maken, wat de verplichting zou inhouden om berichten van gebruikers te monitoren.
Op dit moment is er een tijdelijke uitzondering op de ePrivacy Verordening die techbedrijven toestaat om communicatie op misbruikmateriaal te controleren. Deze uitzondering verloopt begin volgend jaar, en Denemarken wil deze regeling nu permanent maken. De AIVD benadrukt dat de benodigde technologie voor chatcontrole toegang vereist tot de persoonlijke data op mobiele apparaten. Deze toegang maakt het systeem kwetsbaar voor cyberaanvallen, omdat de combinatie van uitgebreide toegangsrechten en een complexe beheersstructuur een aantrekkelijk doelwit vormt voor kwaadwillende actoren.
Volgens de AIVD vergroot dit systeem het risico op digitale kwetsbaarheden. De inlichtingendienst heeft ernstige zorgen over de mogelijkheid dat hackers misbruik maken van de infrastructuur, wat leidt tot ongewenste toegang tot grote hoeveelheden persoonlijke gegevens. Hoewel het voorstel een belangrijke stap is in

de bestrijding van misbruik, blijven de risico's voor de digitale weerbaarheid hoog. Nederland heeft aangegeven zich van stemming te onthouden over dit voorstel, maar blijft aandacht vragen voor zorgvuldige afwegingen in de implementatie van dergelijke maatregelen.

Stalkers misbruiken technologie voor digitale intimidatie: "Stalking gebeurt nu vanachter een scherm"

In een wereld waar technologie steeds vaker wordt ingezet voor digitale misdrijven, maken stalkers gebruik van geavanceerde technieken zoals spoofing, anonieme oproepen en buitenlandse telefoonnummers om hun slachtoffers lastig te vallen. Dit maakt het voor de autoriteiten steeds moeilijker om daders op te sporen en hen voor de wet te brengen. Christophe Van Bortel, cybercrime-expert bij de federale politie, benadrukt dat deze technieken, die ook bij phishing worden ingezet, het mogelijk maken voor stalkers om onder de radar van de politie te blijven.

Een voorbeeld van de ernst van deze problematiek kwam naar voren in een incident in Stabroek, waarbij een onbekende partij tientallen begrafenisondernemers naar het huis van een levende vrouw stuurde, met de valse mededeling dat haar lichaam moest worden opgehaald. Dit soort gevallen valt onder 'proxystalking', waarbij de dader via anderen het slachtoffer intimideert. Dit fenomeen, dat zich niet beperkt tot persoonlijke stalking maar ook voorkomt in gevallen van politieke intimidatie of online pesterijen, toont de gevaren van technologie wanneer deze in de handen van kwaadwillenden terechtkomt.

Veel slachtoffers van digitale stalking schamen zich om aangifte te doen, wat het een uitdaging maakt om betrouwbare gegevens te verzamelen. Dit wordt bemoeilijkt door de noodzaak voor de politie om via juridische kanalen gegevens op te vragen bij betrokken partijen, zoals bedrijven of personen die door de stalkers worden misleid. Toch zijn er technische oplossingen die slachtoffers kunnen helpen, zoals tools van Google en Samsung die verdachte oproepen blokkeren en de mogelijkheid bieden om persoonlijke gegevens beter te beschermen.

De federale politie maakt gebruik van gespecialiseerde teams, zoals de 'Computer crime unit', die digitale sporen kunnen analyseren om zelfs de meest geavanceerde technieken te doorzien. Dit benadrukt dat ondanks de geavanceerde technieken die stalkers gebruiken, er altijd mogelijkheden blijven om digitale sporen te traceren en daders te identificeren.

Nederland stemt toch tegen Europees voorstel voor chatcontrole

Nederland zal tijdens de Europese bespreking over chatcontrole tegen het meest recente Deense voorstel stemmen. Dit besluit komt nadat een meerderheid in de

Tweede Kamer een motie van GroenLinks PvdA heeft aangenomen. Deze motie stelt dat het voorstel voor de CSAM verordening onvoldoende rekening houdt met de bescherming van privacy, de risico's van massasurveillance en de digitale weerbaarheid van Nederland. Demissionair minister Van Oosten en staatssecretaris Rutte van Justitie en Veiligheid bevestigden dat Nederland bij aanvaarding van de motie tegen zal stemmen.
De Europese Commissie wil chatdiensten verplichten om berichten van gebruikers te controleren op verboden materiaal. Lidstaten zijn hierover verdeeld en een definitief standpunt ontbreekt nog, waardoor onderhandelingen met het Europees Parlement voorlopig niet kunnen doorgaan. Denemarken, voorzitter van de EU, deed eerder een voorstel voor verplichte chatcontrole, maar trok dit in vanwege te weinig steun. Het aangepaste voorstel maakt vrijwillige chatcontrole permanent en biedt later mogelijkheid tot verplichtstelling via een reviewclausule. Deze uitzonderingsregeling geldt nu als tijdelijke afwijking van de ePrivacy verordening, die begin volgend jaar afloopt.
Het Deense voorstel omvat controle op foto's en tekstberichten en bevat daarnaast een verplichting voor online leeftijdsverificatie. Critici wijzen op een ernstige inmenging in persoonlijke communicatie en vrezen dat toegang tot gegevens in berichtenapps de cyberveiligheid ondermijnt. De AIVD waarschuwde eerder dat chatcontrole kwaadwillenden toegang kan geven tot gevoelige data op mobiele apparaten. Volgens de aangenomen motie moet de regering zich in de vervolgfase actief inzetten om verplichtingen die kunnen leiden tot massasurveillance op versleutelde diensten en verhoogde cyberveiligheidsrisico's uit het voorstel te verwijderen.
De motie kreeg steun van verschillende partijen, waaronder SP, 50Plus, GroenLinks PvdA, PvdD, Volt, D66, Denk, BBB, PVV en Forum voor Democratie. Nederland, dat traditioneel tegenstander was van voorstellen met chatcontrole, komt hiermee terug op het eerdere voornemen om zich van stemming te onthouden.

FBI: Cybercriminelen stelen $262 miljoen door bankondersteuning te imiteren
Het FBI heeft gewaarschuwd voor een significante toename van fraude door accountovername (ATO) en meldt dat cybercriminelen die zich voordoen als medewerkers van banken en financiële instellingen sinds januari 2025 meer dan $262 miljoen hebben gestolen. Het Internet Crime Complaint Center (IC3) van het FBI heeft meer dan 5.100 meldingen ontvangen van slachtoffers wereldwijd, waaronder zowel particulieren als bedrijven uit verschillende sectoren.
De criminelen verkrijgen ongeautoriseerde toegang tot online bankrekeningen, salarisadministraties of zorgspaarrekeningen door gebruik te maken van social

engineering of valse websites. Wanneer ze toegang hebben, verplaatsen ze vaak de gestolen fondsen naar cryptowallets, waardoor het moeilijk is om het geld te traceren of terug te vorderen. In veel gevallen veranderen de criminelen ook de wachtwoorden van de accounts, waardoor de legitieme eigenaren geen toegang meer hebben.
De FBI meldt dat de aanvallers zich vaak voordoen als bankmedewerkers via sms, telefoongesprekken of e-mails, waarmee ze slachtoffers manipuleren om hun inloggegevens, inclusief multi-factor authenticatiecodes, te verstrekken. Deze gestolen gegevens worden vervolgens gebruikt om in te loggen op de accounts van de slachtoffers en om het wachtwoord te resetten, zodat de criminelen volledige controle over de accounts krijgen. In sommige gevallen doen criminelen zich ook voor als wetshandhavers om slachtoffers naar phishingwebsites te leiden of hen te dwingen gevoelige informatie te verstrekken.
In Nederland en België moeten slachtoffers van dergelijke aanvallen direct contact opnemen met hun bank of financiële instelling om een terugboeking te vragen en schadevergoeding te verkrijgen. Het wordt aangeraden om altijd gebruik te maken van veilige onlinepraktijken, zoals het inschakelen van multi-factor authenticatie en het gebruiken van bladwijzers om bankwebsites te bezoeken, in plaats van zoekresultaten die mogelijk leiden naar frauduleuze sites.