Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

18-11-2025:

Datalek bij Franse tak Eurofiber blijkt beperkt tot regionale merken in Frankrijk

De Franse dochter van Eurofiber heeft bevestigd dat onbevoegde toegang is verkregen tot interne systemen waarin klantgegevens waren opgeslagen. Cybercrimeinfo ontdekte op 14 november dat er sprake was van een datalek, maar inmiddels blijkt dat de impact uitsluitend de Franse tak betreft en niet de Nederlandse omgeving. Aanvallers maakten misbruik van een kwetsbaarheid in het ticketmanagementplatform van Eurofiber France en in een portaal dat door hosting en outsourcingpartner ATE wordt gebruikt. Daarbij is informatie uit beide systemen gekopieerd, al geeft Eurofiber niet aan om welke gegevens het precies gaat of hoeveel klanten zijn getroffen. De kwetsbaarheid is na ontdekking verholpen.

Eurofiber benadrukt dat alleen klanten van Eurofiber France en de regionale merken Eurafibre, FullSave, Netiwan en Avelia zijn geraakt. Klanten die gebruikmaken van diensten die in Nederland, België of Duitsland worden gehost, waaronder Eurofiber Cloud Infra, zijn volgens de verklaring niet getroffen. Berichten op sociale media suggereren dat de aanval mogelijk verband houdt met een verouderde versie van GLPI en dat gegevens van duizenden klanten kunnen zijn buitgemaakt, maar deze details zijn niet bevestigd. Eurofiber geeft aan dat betrokken klanten inmiddels zijn geïnformeerd en dat melding is gedaan bij de Franse toezichthouder CNIL.

(Zie ook 14 november 2025 | Mogelijk datalek bij Eurofiber met publicatie interne gegevens)

Poolse sabotagezaak gezien als onderdeel van hybride oorlogsvoering

Polen onderzoekt een explosie op de spoorlijn tussen Warschau en Lublin die volgens de regering het gevolg is van doelbewuste sabotage. Premier Donald Tusk bevestigde dat een explosief het spoor op meerdere locaties heeft beschadigd en noemde het een ernstige aantasting van de nationale veiligheid. De autoriteiten zien geen verband met ongevallen en beschouwen coördinatie als aannemelijke mogelijkheid. Er zijn geen gewonden gemeld.

De sabotage wordt door de Poolse regering geplaatst in een patroon van hybride activiteiten dat de afgelopen periode zichtbaar is geworden. Het land rapporteert vaker over droneincidenten, verstoringen aan de grens met Belarus en oplopende cyberaanvallen die volgens Warschau passen binnen een bredere strategie om

Europese lidstaten te destabiliseren. Tusk stelt dat deze combinatie van digitale en fysieke acties de druk op Europese veiligheidsstructuren vergroot. Hij benadrukt dat samenwerking binnen de NAVO en versterking van de Europese defensieve capaciteit noodzakelijk blijven om dergelijke incidenten het hoofd te bieden.

Duitse waarschuwing voor Russische dreiging versterkt aandacht voor hybride oorlogsvoering

De Duitse minister van Defensie Boris Pistorius waarschuwt dat Rusland binnen enkele jaren opnieuw over voldoende militaire slagkracht kan beschikken om de Europese veiligheid te ondermijnen. Volgens militaire en inlichtingenanalyses zou Moskou rond 2028 of 2029 in staat kunnen zijn om rechtstreeks druk uit te oefenen op de oostflank van de NAVO. Deze ontwikkeling wordt geplaatst in een bredere context van hybride strategieën waarin digitale aanvallen, sabotage en desinformatie een centrale rol spelen.

Pistorius benadrukt dat de voortdurende modernisering van de Russische strijdkrachten gepaard gaat met intensivering van activiteiten die ook het civiele domein raken, zoals cyberaanvallen en verstorende operaties in diverse Europese landen. De recente droneincidenten in onder meer Polen, Denemarken en Duitsland worden door verschillende analisten gezien als signalen dat Moskou de grenzen van de Europese defensie en digitale weerbaarheid blijft testen.

Hoewel de NAVO zijn afschrikking volgens Pistorius op peil heeft, vraagt de combinatie van conventionele opbouw en digitale druk om versnelde versterking van zowel fysieke defensie als cybercapaciteit. De Duitse analyse maakt duidelijk dat Europa rekening moet houden met een langere periode van verhoogde hybride dreiging, waarin nieuwe technologieën snel worden ingezet op het slagveld en in het digitale domein.

Overheid benadrukt voorbereiding op langdurige stroomuitval en cyberdreigingen in Nederland

De Nederlandse overheid heeft een informatiecampagne gelanceerd om burgers voor te bereiden op langdurige stroomuitval en andere crisis-situaties. Experts waarschuwen dat het slechts een kwestie van tijd is voordat Nederland te maken krijgt met een scenario waarin de infrastructuur dagenlang ontwricht is. Langdurige

stroomstoringen, mogelijk als gevolg van cyberaanvallen op het elektriciteitsnet, worden als reële dreigingen beschouwd. De campagne 'Denk vooruit' richt zich niet alleen op fysieke noodsituaties, maar benadrukt ook de noodzaak voor zelfredzaamheid in het geval van cyberincidenten, zoals hackaanvallen op kritieke infrastructuur.

Vanaf 25 november ontvangen alle huishoudens een informatieboekje waarin wordt uitgelegd hoe men zich kan voorbereiden op een situatie waarin de overheid tijdelijk niet in staat is hulp te bieden. De boodschap is duidelijk: burgers moeten de eerste 72 uur na een crisis zelf kunnen overleven, door bijvoorbeeld een noodpakket en een communicatieplan op te stellen.

Het onderzoek van Mark Levels, hoogleraar sociologie, benadrukt de veranderende veiligheidssituatie in Nederland en Europa, waarbij de dreiging van cyberaanvallen en hybride oorlogsvoering, waaronder desinformatie en digitale sabotage, steeds groter wordt. Het is belangrijk dat burgers zich niet alleen voorbereiden op fysieke rampen, maar ook op de mogelijkheid van aanvallen op vitale systemen zoals elektriciteit en communicatie.

Met deze campagne wil de overheid de weerbaarheid van de samenleving versterken, zodat men in geval van een crisis niet afhankelijk is van externe hulp. De focus ligt daarbij niet alleen op fysieke noodmaatregelen, maar ook op het versterken van digitale veiligheid en weerbaarheid tegen cyberdreigingen.

Bulkveiling van 800 fullz met 70% geldigheid op darkweb gemeld

Op 16 november 2025 werd er op het darkweb een bulkveiling gemeld van 800 volledige gestolen identiteiten, ook wel "fullz" genoemd. De verkoper claimt dat 70% van de gelekte gegevens geldig is. Fullz bevat vaak gevoelige persoonlijke informatie, zoals naam, adres, geboortedatum, sociaal-zekerheidsnummer en bankgegevens, die door cybercriminelen gebruikt kunnen worden voor identiteitsdiefstal of andere vormen van fraude.

Het verhandelen van dergelijke gegevens op darkweb marktplaatsen is een veelvoorkomend fenomeen waarbij criminelen profiteren van gestolen informatie. De mate van geldigheid van de gelekte gegevens verhoogt de risico's voor individuen wiens gegevens zijn betrokken bij dergelijke aanbiedingen.

Detectie van NotDoor malware in Outlook: geavanceerde technieken beschreven

De NotDoor malware, gelinkt aan de hacker-groep APT28 (Fancy Bear), maakt gebruik van Outlook-macro's om toegang te krijgen tot systemen en gegevens te stelen. Dit soort aanvallen is bijzonder gevaarlijk omdat het misbruik maakt van vertrouwde software, zoals Outlook, om ongemerkt gegevens te exfiltreren. De aanvallers plaatsen schadelijke code in Outlook-bestanden, waardoor ze onopgemerkt toegang krijgen tot het systeem.

De aanvallen beginnen vaak met een techniek genaamd DLL-sideloading, waarbij schadelijke bestanden naast legitieme applicaties worden geplaatst, zoals OneDrive.exe. Dit stelt de aanvallers in staat om ongezien commando's uit te voeren en malware te installeren zonder dat dit direct wordt opgemerkt. De infectie laat verschillende sporen na, zoals gewijzigde bestandsinstellingen en verdachte registerwijzigingen, die belangrijk kunnen zijn voor het opsporen van dergelijke aanvallen.

Beveiligingsexperts, zoals Splunk, hebben deze technieken grondig onderzocht en laten zien hoe de malware op een slinkse manier communiceert via Outlook en PowerShell, en hoe belangrijke detectiepunten kunnen worden gebruikt om dergelijke aanvallen te identificeren. Dit onderzoek biedt waardevolle inzichten voor bedrijven die hun systemen willen beschermen tegen dit soort geavanceerde dreigingen.

EVALUSION-campagne gebruikt ClickFix-techniek om Amatera Stealer en NetSupport RAT te verspreiden

In november 2025 werd een nieuwe malwarecampagne ontdekt die geavanceerde sociale-engineeringtechnieken combineert met krachtige stealer- en RAT-tools. Deze campagne maakt gebruik van de ClickFix-techniek, waarbij aanvallers gebruikers misleiden om specifieke commando's uit te voeren via het Windows Run-venster. Zodra gebruikers deze stappen volgen, wordt hun systeem geïnfecteerd met Amatera Stealer, een geavanceerd stuk malware dat is ontworpen om gevoelige informatie van browsers, wachtwoordbeheerders en crypto-portemonnees te stelen.

Na de initiële infectie wordt NetSupport RAT geïnstalleerd, waarmee de aanvallers volledige toegang krijgen tot het slachtoffer zijn computer. De campagne maakt gebruik van complexe technieken, zoals het versleutelen van communicatie via AES-256-CBC en het omzeilen van traditionele beveiligingsmaatregelen door middel van

obfuscatie en het uitschakelen van de AMSI (Anti-Malware Scan Interface) van Windows. Het gebruik van een .NET-gebaseerde downloader en geavanceerde injectietechnieken maakt de malware moeilijk te detecteren en te analyseren.

De Amatera Stealer, voorheen bekend als ACR Stealer, maakt gebruik van WoW64-syscalls om beveiligingstools zoals antivirussoftware en endpoint-detectiesystemen te omzeilen, wat betekent dat zelfs goed beveiligde systemen kwetsbaar blijven voor deze aanval. Deze campagne is een zorgwekkend voorbeeld van hoe cybercriminelen meerdere geavanceerde technieken combineren voor maximale schade en benadrukt de noodzaak voor robuuste en gelaagde beveiligingsmaatregelen.

Hackers misbruiken Microsoft Entra-uitnodigingen voor TOAD-aanvallen

Een nieuwe phishingcampagne maakt gebruik van Microsoft Entra-gastgebruiker-uitnodigingen om slachtoffers te misleiden en hen telefonisch contact te laten opnemen met aanvallers die zich voordoen als Microsoft-ondersteuning. Deze aanval maakt gebruik van een zwakke plek in de manier waarop Microsoft Entra communiceert met externe gebruikers, waardoor een legitieme samenwerkingstool wordt omgezet in een middel voor geavanceerde social engineering-aanvallen.

De campagne is een evolutie van de TOAD (Telephone Oriented Attack Delivery)-aanvalstechniek, waarbij cloudgebaseerde systemen voor accountbeveiliging worden gecombineerd met traditionele telefoonfraude. Aanvallers maken valse Microsoft-entiteiten, zoals “Unified Workspace Team” en “CloudSync,” om het vertrouwen van hun doelwitten te winnen. De slachtoffers ontvangen uitnodigingen via e-mail, die afkomstig lijken van het legitieme Microsoft-adres "invites@microsoft.com," en bevatten valse betalingsinformatie, zoals transactiebedragen en klant-ID's.

De aanvallers vragen de ontvangers van de uitnodigingen om contact op te nemen met een telefoonnummer dat wordt gepresenteerd als Microsoft Billing Support. Dit nummer leidt echter direct naar de aanvallers, die vervolgens proberen inloggegevens te stelen en accounts over te nemen. De aanval maakt gebruik van een ontwerpflaws in Microsoft Entra, waarbij het berichtveld in de gastgebruikeraansluitingen lange teksten toestaat, wat de traditionele beveiligingssystemen omzeilt.

Beveiligingsexperts raden aan om verdachte uitnodigingen snel te herkennen door te zoeken naar specifieke aanwijzingen in de e-maillogs, zoals de afzender

“invites@microsoft.com” en verdachte domeinnamen van aanvallers. Organisaties kunnen verdere schade beperken door telefoonnummerblokkades in te stellen en gebruikers te waarschuwen over het verifiëren van Microsoft-communicatie via officiële kanalen.

Npm-malwarecampagne maakt gebruik van Adspect-cloaking voor schadelijke redirects

Een recente malwarecampagne op het npm-platform maakt gebruik van de Adspect-cloakingtechniek om slachtoffers te misleiden en hen om te leiden naar crypto-gerelateerde scamwebsites. De kwaadwillende npm-pakketten zijn ontworpen om een valse CAPTCHA weer te geven en de bezoeker te identificeren op basis van fingerprinting, waarbij potentiële slachtoffers naar de schadelijke sites worden geleid. Als een bezoeker geen onderzoeker is, wordt hij doorgestuurd naar een phishingwebsite die zich voordoet als een legitieme crypto-exchange.

De betrokken malware wordt verspreid via verschillende npm-pakketten, waaronder "signals-embed", "dsidospsodlks" en "integrator-filescrypt2025". De kwaadaardige software maakt gebruik van Adspect-cloaking om te verbergen voor beveiligingsonderzoekers door alleen kwaadaardige inhoud te tonen aan de echte slachtoffers. Als een slachtoffer wordt gedetecteerd, wordt een nep-CAPTCHA gepresenteerd, waarna de bezoeker wordt doorgestuurd naar een crypto-website die mogelijk is ontworpen om persoonlijke gegevens of cryptocurrency van het slachtoffer te stelen.

Wat deze aanval bijzonder maakt, is de manier waarop de Adspect-cloakingtechniek wordt ingezet binnen de npm-supply chain. De gebruikte techniek maakt het mogelijk om verkeersstromen te maskeren, waarbij beveiligingsonderzoekers worden omgeleid naar een lege of onschuldige pagina, terwijl slachtoffers gericht naar de schadelijke bestemming worden gestuurd. Door het gebruik van valse CAPTCHA's en dynamische redirects kan de aanvaller frequent nieuwe schadelijke URL's genereren zonder dat de pakketten opnieuw gepubliceerd hoeven te worden. Dit maakt het moeilijker voor beveiligingsmaatregelen om de aanval proactief te stoppen.

Deze campagne illustreert hoe kwaadaardige actoren het open-source ecosysteem kunnen misbruiken voor het uitvoeren van geavanceerde aanvallen via supply-chain compromissen. Door de inzet van Adspect-cloaking kunnen zij hun malafide

activiteiten verbergen en schade aanrichten zonder snel opgemerkt te worden. Het gebruik van valse crypto-exchange-merken helpt bovendien de geloofwaardigheid van de aanval te vergroten, waardoor de kans dat slachtoffers trappen in de val groter wordt.

Man krijgt taakstraf voor aansluiten van cryptominers op router windmolenpark

Een voormalige technisch manager van een beheermaatschappij van windmolenparken in Nederland is veroordeeld tot een taakstraf van 120 uur vanwege het aansluiten van cryptominers op de router van een windmolenpark. De man had in 2022 drie cryptominingcomputers aangesloten op de netwerkrouter van het park in Gieterveen, en daarnaast twee Helium nodes geplaatst in windturbines van een ander park in Waardpolder. Deze apparaten werden gebruikt om gegevens door te sturen, wat in strijd was met de afspraken van zijn werkgever.

Na de ontdekking van de apparatuur werd de man ontslagen, en de rechter achtte hem schuldig aan zowel diefstal van elektriciteit als computervredebreuk. Het bedrijf dat de windturbines had geleverd, was vlak voor de ontdekking van de cryptominers slachtoffer geworden van een ransomware-aanval. Dit maakte de impact van de misdaden van de verdachte groter. De rechtbank rekende het de man zwaar aan dat hij zijn positie als technical manager had misbruikt en het vertrouwen van zijn werkgever had geschaad.

De rechter besloot, hoewel het Openbaar Ministerie een taakstraf van 240 uur had geëist, om uit te komen op een taakstraf van 120 uur. Ook moet de man een schadevergoeding van 4.155 euro betalen aan de windmolenfabrikant. De zaak benadrukt de risico's van ongeautoriseerd gebruik van infrastructuur in een zakelijke omgeving en de gevolgen van dergelijk misbruik voor zowel de werkgever als de bredere bedrijfsvoering.

Aantal incidenten met nepagenten in Nederland stijgt opnieuw

Het aantal incidenten waarbij criminelen zich voordoen als politiemedewerkers is in 2025 tot en met oktober opgelopen tot 10.631 gevallen. Hoewel de incidenten in de zomermaanden augustus en september afnamen, is er nu weer een stijging waar te nemen. Nepagenten bellen vaak van tevoren om hun komst aan te kondigen of sturen een brief. Ze beweren dat er (gewapende) inbraken in de buurt zijn geweest

en dat ouderen gevaar lopen om ook slachtoffer te worden. Om hen te beschermen, zouden ze waardevolle spullen willen ophalen om deze "veilig te stellen". Deze oplichters gebruiken daarbij soms namen van echte agenten of delen van politie-uniformen.

De politie benadrukt dat echte agenten nooit waardevolle goederen zoals geld, sieraden of bankpassen met pincodes komen ophalen. Bij vermoedens van een nepagent wordt burgers geadviseerd om onmiddellijk 112 te bellen. Dit maakt het niet alleen mogelijk om de situatie snel te verifiëren, maar vergroot ook de kans om de verdachten op heterdaad aan te houden. Gelukkig worden er steeds meer verdachte oplichters gepakt, maar het blijft belangrijk dat mensen melding maken van zowel pogingen als succesvolle oplichting.

De nepagenten richten zich vooral op ouderen, waarvoor in samenwerking met Omroep Max in juli een landelijke campagne is gestart. Ondanks deze inspanningen blijft het aantal incidenten stijgen, wat de noodzaak van waarschuwingen onderstreept. De politie waarschuwt verder dat het niet alleen om materiële schade gaat; slachtoffers ervaren vaak ernstige emotionele gevolgen. In sommige gevallen, zoals bij de gewelddadige dood van een 80-jarige vrouw uit Amsterdam, blijkt dat de nepagenten ook betrokken kunnen zijn bij ernstigere misdrijven.

De politie doet een oproep aan de bevolking om altijd verdachte telefoontjes of bezoeken te melden, ook als het slechts een poging betreft. Dit draagt bij aan het vergroten van de opsporingskracht en helpt de veiligheid in de gemeenschap te waarborgen.

Europol voert actie tegen online radicalisering op gamingplatforms

Op 13 november 2025 voerde Europol in samenwerking met acht Europese landen een gezamenlijke actie uit om online radicalisering tegen te gaan op gaming- en aanverwante platforms. Deze operatie, bekend als Referral Action Day, resulteerde in het verwijderen van duizenden links naar terroristische, racistische en xenofobische propaganda die werd gedeeld op platforms die veel worden gebruikt door jongeren en volwassenen. De landen die deelnamen aan deze actie waren Denemarken, Finland, Duitsland, Luxemburg, Nederland, Portugal, Spanje en het Verenigd Koninkrijk.

Tijdens de actie werden meer dan 5.400 links naar jihadistische inhoud, 1.070 links naar gewelddadige extreem-rechtse en terroristische inhoud en 105 links naar

racistische en xenofobische content verwijderd. De operatie benadrukt de complexiteit van het bestrijden van deze soorten inhoud, die vaak worden verspreid via verschillende lagen van platforms. Zo kan gewelddadige inhoud bijvoorbeeld worden gefilmd in een online spel, gemodificeerd met extremistische jargon of symbolen, en vervolgens gedeeld op mainstream sociale media om een breder publiek te bereiken.

De actie richtte zich niet alleen op gamingplatforms, maar ook op streamingdiensten, community-platforms en hybride platforms die gaming, streaming en sociale interactie combineren. In sommige gevallen werden accounts met namen en profielfoto's die verwezen naar beruchte terroristen aangetroffen, wat de uitdaging vergrootte om dergelijke inhoud te identificeren.

Europol ondersteunt deze gezamenlijke inspanning met operationele vergaderingen en het uitwisselen van informatie en best practices tussen de deelnemende landen. Deze activiteit is onderdeel van een breder programma gericht op het voorkomen van de verspreiding van terroristische inhoud online, zoals beschreven in de EU Verordening over de bestrijding van de verspreiding van terroristische inhoud op het internet.

UK Twitter-hacker moet $5,4 miljoen in Bitcoin terugbetalen

Joseph James O'Connor, de Britse hacker die in 2020 de Twitter-accounts van onder andere voormalig president Barack Obama, Elon Musk en Joe Biden heeft gehackt, is door de Britse autoriteiten verplicht om 5,4 miljoen dollar in Bitcoin terug te betalen. Dit besluit volgt op zijn veroordeling in de Verenigde Staten, waar hij schuld bekende aan onder andere computerinbraak, fraude en afpersing. O'Connor kreeg in 2023 een gevangenisstraf van vijf jaar opgelegd.

De aanval, die plaatsvond in juli 2020, zorgde voor een tijdelijke restrictie van geverifieerde Twitter-accounts nadat de hackers de accounts van verschillende prominente figuren hadden overgenomen. Ze gebruikten deze accounts om digitale valuta te vragen en dreigden met publicatie van privé-informatie. O'Connor werd in 2021 in Spanje gearresteerd en later uitgeleverd aan de VS voor vervolging.

De Britse autoriteiten hebben een civiele verhaalsactie aangespannen om de cryptocurrency die afkomstig was van de hack in beslag te nemen. In totaal werden 42 Bitcoin en andere cryptomiddelen verbonden aan de misdaad veiliggesteld. Deze zullen nu worden geliquideerd door een door de rechtbank aangestelde trustee. De

actie benadrukt de inzet van de Britse wetshandhavers om criminele winsten, ook als de verdachte buiten het VK is veroordeeld, te herwinnen.

Kabinet steunt EU-richtlijnen voor online leeftijdsverificatie

Het demissionaire kabinet heeft zijn steun uitgesproken voor de Europese richtlijnen omtrent online leeftijdsverificatie, die gericht zijn op het verbeteren van de bescherming van minderjarigen op het internet. Deze richtlijnen, opgesteld door de Europese Commissie, stellen online platforms verplicht maatregelen te treffen om de veiligheid van kinderen en jongeren te waarborgen. De maatregelen moeten altijd proportioneel zijn en rekening houden met de privacy en grondrechten van gebruikers.

Een van de centrale elementen van de richtlijnen is de inzet van technologieën voor leeftijdsverificatie die verder gaan dan de traditionele zelfverklaring van een gebruiker, zoals het invoeren van een geboortedatum. In plaats daarvan wordt een betrouwbaardere methode voorgesteld, zoals een eigen white label app, die gebruikers in staat stelt te bewijzen dat zij voldoen aan de minimale leeftijdseisen zonder onterecht persoonlijke gegevens te verstrekken.

Het kabinet onderzoekt of het wenselijk is om een dergelijke app in Nederland te ontwikkelen, en hoe dit technisch en juridisch ingevuld kan worden zonder inbreuk te maken op de privacy van gebruikers. Het gebruik van leeftijdsverificatie wordt echter gezien als een zwaar middel dat ingrijpt in verschillende grondrechten, zoals privacy en gegevensbescherming. Het kabinet benadrukt dat de toepassing van deze technologie zorgvuldig moet worden afgewogen tegen de impact op de gebruikers en de effectiviteit van de maatregel.

Hoewel de richtlijnen niet bindend zijn, kunnen zij de basis vormen voor toekomstige wetgeving en beleidsvorming in de EU. Het kabinet verwacht brede steun voor de richtlijnen binnen de EU-lidstaten, maar houdt vast aan het principe dat elke maatregel die de toegang tot online diensten reguleert, proportioneel moet zijn en het gebruik van alternatieven zonder ernstige inbreuken op de rechten van gebruikers mogelijk moet maken.

Met deze steun voor de EU-richtlijnen benadrukt het kabinet het belang van een gebalanceerde aanpak van online veiligheid, waarin de bescherming van minderjarigen tegen schadelijke online content centraal staat, zonder afbreuk te doen aan fundamentele privacyrechten.

Kamer vraagt opheldering over voorgestelde AVG-aanpassingen

De Europese Commissie heeft onlangs voorstellen gepresenteerd voor aanpassingen aan de Algemene Verordening Gegevensbescherming (AVG), die zorgen oproepen bij privacy-experts en burgerrechtenorganisaties. De wijzigingen, die deel uitmaken van het "Digital Omnibus"-pakket, zouden de fundamenten van de AVG aantasten en hebben aanzienlijke implicaties voor de bescherming van persoonsgegevens in Europa.

De voorgestelde veranderingen richten zich op de definitie van "persoonlijke data" en de rechten van individuen onder de AVG. Tevens wordt beoogd om AI-bedrijven meer mogelijkheden te geven voor het verzamelen en gebruiken van persoonsgegevens om AI-modellen te trainen, wat vooral in het voordeel zou zijn van grote technologiebedrijven. Een andere belangrijke wijziging is de verslapping van de bescherming van gevoelige gegevens zoals gezondheidsinformatie, politieke voorkeuren en seksuele geaardheid. Bovendien zou de mogelijkheid worden gecreëerd voor remote toegang tot persoonlijke data op apparaten zonder de expliciete toestemming van de gebruiker.

Deze veranderingen zijn met name relevant voor organisaties die met persoonlijke gegevens werken, waaronder bedrijven in de AI-sector. De zorgen over deze aanpassingen zijn groot, vooral omdat zij de veiligheid van persoonlijke gegevens kunnen aantasten en nieuwe kwetsbaarheden kunnen creëren voor misbruik. In reactie op de voorgestelde wijzigingen heeft GroenLinks-PvdA-Kamerlid Kathmann Kamervragen gesteld aan minister Karremans van Economische Zaken. Zij wil weten of de Digitale Omnibus de privacybescherming daadwerkelijk zal verzwakken en of de minister van mening is dat de veranderingen kunnen leiden tot deregulering van de privacywetgeving.

Het is van belang om de ontwikkelingen rondom deze hervormingen te blijven volgen, aangezien zij de toekomstige omgang met persoonsgegevens en de bescherming tegen datadiefstal of misbruik kunnen beïnvloeden. De minister heeft drie weken de tijd om te reageren.

Google blijft gegevens ontvangen van gedowngrade Nest-thermostaten

In oktober 2025 beëindigde Google de ondersteuning voor de eerste en tweede generatie Nest Learning-thermostaten, wat betekende dat gebruikers de apparaten niet langer via de Nest- of Google Home-app konden beheren. Echter, uit onderzoek blijkt dat de apparaten nog steeds gegevens blijven versturen naar de servers van Google, ondanks het stopzetten van de remote beheerfunctie. Deze gegevens omvatten onder andere temperatuurinstellingen, luchtvochtigheid en aanwezigheid van een persoon in de ruimte. Beveiligingsonderzoeker Cody Kociemba benadrukt dat deze informatie, die oorspronkelijk voor probleemdiagnoses werd verzameld, nu lijkt door te gaan zonder expliciete toestemming van de gebruikers. De thermostaten blijven nog wel handmatig bedienbaar, maar de communicatie met Google is blijven bestaan, wat vragen oproept over de controle die gebruikers hebben over hun privacy. Tot nu toe heeft Google geen commentaar gegeven op deze situatie.

ICS hoeft slachtoffers van phishing-aanval over "douanekosten" niet te vergoeden

In een recente uitspraak heeft het financiële klachteninstituut Kifid bepaald dat ICS, een bekende creditcardmaatschappij, geen schadevergoeding hoeft te betalen aan twee slachtoffers van een phishingaanval. De slachtoffers ontvingen een sms-bericht, zogenaamd van DHL, waarin werd beweerd dat er een pakket klaarstond en dat een betaling van 2,99 euro voor "douanekosten" vereist was. Via de meegestuurde link kwamen de slachtoffers terecht op een phishingsite en vulden zij hun creditcardgegevens in.

Na het verstrekken van de gegevens werd hun creditcard gekoppeld aan een Apple Pay Wallet op een andere telefoon, waarna duizenden euro's aan frauduleuze transacties werden uitgevoerd. Het ene slachtoffer verloor meer dan 4.000 euro, terwijl het andere slachtoffer bijna 2.700 euro kwijt was.

ICS weigerde de schade te vergoeden, omdat het bedrijf van mening was dat de slachtoffers nalatig waren in het beschermen van hun gegevens. Het klachteninstituut stelde dat de slachtoffers niet in staat waren om voldoende bewijs te leveren over hoe de oplichters toegang kregen tot hun gegevens, waardoor de claim als ongegrond werd afgewezen. Kifid concludeerde dat de slachtoffers zich niet aan de verplichtingen hadden gehouden, zoals het veiligstellen van hun verificatiecodes.

Samsung wordt momenteel bekritiseerd nadat beweringen zijn ontstaan dat Galaxy-smartphones worden geleverd met een app, AppCloud, die niet verwijderd kan

worden zonder ingrijpende systeemwijzigingen. Deze promotionele app, ontwikkeld door het Israëlische bedrijf ironSource, kan zichzelf zelfs opnieuw installeren na updates, wat zorgen oproept over de privacy van gebruikers. Hoewel er geen concrete bewijzen zijn die de app verbinden met spyware of overheidsmonitoring, heeft het gebrek aan transparantie over de werking van de app publieke bezorgdheid aangewakkerd.

Deze situatie brengt de kwestie van ongevraagde, niet-verwijderbare apps op mobiele apparaten naar voren, die mogelijk veiligheidsrisico's met zich meebrengen, aangezien ze zonder de medeweten van de gebruiker deel kunnen uitmaken van het systeem. Experts wijzen op de noodzaak voor meer controle en duidelijkheid over de apps die op smartphones worden vooraf geïnstalleerd, vooral als ze niet eenvoudig kunnen worden verwijderd.

Samsung en Unity, de huidige eigenaar van ironSource, hebben tot nu toe geen officiële reactie gegeven op de beschuldigingen.

Grote Darkweb veilingen van Fortinet VPN-toegangspunten en inloggegevens voor miljoenen

Op 17 november 2025 zijn er op het Dark Web twee zorgwekkende veilingen van Fortinet VPN-toegangspunten en inloggegevens aan het licht gekomen, die wijzen op de toenemende dreiging van cybercriminaliteit gericht op beveiligde netwerken. De eerste veiling betreft de verkoop van 6.000 Fortinet VPN-inloggegevens, waarvoor een vraagprijs van $28.000 wordt gevraagd. Deze gegevens zouden afkomstig zijn van verschillende organisaties die gebruikmaken van Fortinet's VPN-oplossingen. Fortinet is wereldwijd bekend om zijn netwerkbeveiligingsproducten, en de verkoop van deze inloggegevens onderstreept de groeiende vraag naar toegang tot beveiligde netwerken door cybercriminelen. Het verkrijgen van dergelijke toegang biedt kwaadwillenden de mogelijkheid om malware te plaatsen, vertrouwelijke informatie te stelen, of datalekken te veroorzaken, wat grote schade kan aanrichten voor de getroffen organisaties en hun klanten.

De tweede aanbieding op het Dark Web betreft de verkoop van 3.000 FortiGate VPN-toegangspunten, met een prijs van $16.000. Deze toegangspunten zouden toegang verschaffen tot netwerken die gebruikmaken van FortiGate VPN-apparaten, die door veel bedrijven wereldwijd worden ingezet voor het beveiligen van hun infrastructuur. De relatief lage prijs per toegangspunt vergroot de kans dat

cybercriminelen meerdere netwerken kunnen binnendringen en misbruiken voor hun eigen doeleinden. Dit toont aan hoe aantrekkelijk toegang tot deze beveiligde netwerken is voor kwaadwillenden die op zoek zijn naar manieren om netwerken te compromitteren of vertraagde aanvallen uit te voeren.

Deze incidenten benadrukken de ernst van de dreiging die voortkomt uit cybercriminaliteit en het misbruik van VPN-technologieën. Organisaties worden geconfronteerd met toenemende risico's als het gaat om netwerkbeveiliging, en dit maakt het des te belangrijker om kwetsbaarheden snel te identificeren en te verhelpen. Het Dark Web blijft een gevaarlijke marktplaats voor cybercriminelen die gebruik maken van gestolen toegangspunten en inloggegevens om netwerken binnen te dringen en kwaadaardige activiteiten uit te voeren.

NSO Group vernieuwt leiderschap in poging reputatie te herstellen

De Israëlische spywarefirma NSO Group, bekend van de Pegasus-software, heeft een nieuw eigenaarschap en leiderschap aangesteld om haar imago te herstellen. David Friedman, voormalig Amerikaanse ambassadeur in Israël en ex-advocaat van president Trump, is aangesteld als uitvoerend voorzitter en hoopt de Amerikaanse markt opnieuw te betrekken. NSO wil haar technologie inzetten om bij te dragen aan een veiligere wereld, met de belofte voorzichtiger om te gaan met het licentiëren van haar software dan voorheen.

Pegasus, de software van NSO, kwam onder verdenking nadat bleek dat deze werd ingezet om journalisten, activisten en zelfs Amerikaanse ambtenaren af te tappen. Het bedrijf werd daarop in 2021 door de VS op de zwarte lijst gezet, wat de toegang tot bepaalde Amerikaanse technologieën bemoeilijkte.

De Pegasus-software maakt gebruik van zogenaamde "zero-click" aanvallen, waarmee hackers zonder enige interactie van het doelwit toegang krijgen tot gegevens op smartphones, inclusief berichten, bestanden en zelfs de camera en microfoon. Ondanks juridische uitdagingen en een rechtszaak van Meta, blijft NSO zich richten op de verkoop van haar technologie, met de hoop wetshandhavingsinstanties in de VS aan te trekken als klanten.

Dit thema blijft gevoelig, gezien de ethische bezorgdheden rondom het gebruik van dergelijke spyware en de wereldwijde bezorgdheid over de privacy en digitale veiligheid.