Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

29-10-2025:

Gestolen gegevens van Omrin gepubliceerd na ransomware-aanval

Bij de Friese afvalverwerker Omrin zijn persoonlijke gegevens van medewerkers en bedrijfsinformatie gestolen tijdens een ransomware-aanval. De gestolen data, waaronder woonadressen, salarisgegevens, bedrijfsbudgetten en kopieën van identiteitsbewijzen, zijn inmiddels openbaar gemaakt op internet. Het bedrijf heeft aangifte gedaan van een mogelijk datalek bij de Autoriteit Persoonsgegevens en werkt samen met een gespecialiseerd bureau om het volledige verlies van data in kaart te brengen. Omrin meldt dat het al vaker doelwit is geweest van cyberaanvallen, maar dat deze keer de aanvallers succesvol waren. De aanval is opgeëist door de ransomwaregroep Qilin. De schade was groot, met tijdelijke sluitingen van kringloopwinkels en storingen in de klantenservice en de Afvalapp. Hoewel de aanvallers toegang hadden tot de systemen, is nog onduidelijk hoe ze dit precies hebben weten te bereiken.

OpenVPN-kwetsbaarheid stelt Linux- en macOS-systemen bloot aan scriptinjectie-aanvallen

Een nieuwe kwetsbaarheid in vroege versies van OpenVPN is onthuld, waarmee kwaadaardige servers willekeurige commando's op clientmachines kunnen uitvoeren. De kwetsbaarheid, die OpenVPN-versies van 2.7_alpha1 tot 2.7_beta1 beïnvloedt, stelt systemen zoals Linux, macOS en BSD in staat om scriptinjectie-aanvallen uit te voeren. Het probleem ontstaat door onvoldoende sanering van de –dns- en –dhcp-option-argumenten, die zonder controle worden doorgegeven aan het –dns-updown-script. Dit biedt aanvallers de kans om schadelijke commando's in te voeren die met verhoogde rechten op de clientmachine draaien, wat kan leiden tot datadiefstal of malware-injectie. De kwetsbaarheid, bekend als CVE-2025-10680, heeft een CVSS-score van 8,1 en is direct exploiteerbaar via het netwerk zonder authenticatie. OpenVPN heeft snel versie 2.7_beta2 uitgebracht, die kritieke beveiligingsverbeteringen bevat. Gebruikers wordt geadviseerd de update te installeren, maar voor productieomgevingen wordt het gebruik van stabiele versies aanbevolen.

CISA waarschuwt voor kritieke kwetsbaarheden in Veeder-Root-systemen die aanvallers in staat stellen systeemopdrachten uit te voeren

De Amerikaanse Cybersecurity and Infrastructure Security Agency (CISA) heeft een waarschuwing afgegeven over twee ernstige kwetsbaarheden in het TLS4B Automatic Tank Gauge-systeem van Veeder-Root, een essentieel instrument voor de brandstofopslag in de energiesector. Deze kwetsbaarheden kunnen aanvallers in staat stellen om willekeurige systeemopdrachten uit te voeren, wat ernstige verstoringen in de infrastructuur kan veroorzaken. De belangrijkste kwetsbaarheid heeft een CVSS v4-score van 9.4, wat aangeeft dat deze op afstand kan worden uitgebuit met lage complexiteit. Veeder-Root raadt aan onmiddellijk updates uit te voeren om de risico's te beperken. De kwetsbaarheden zijn ontdekt in wereldwijd gebruikte systemen voor het monitoren van ondergrondse opslagtanks. CISA benadrukt dat deze kwetsbaarheden vooral impact hebben op energieoperaties, waar uitval kan leiden tot brandstoftekorten of veiligheidsproblemen.

Kritieke kwetsbaarheid in Ubuntu's Linux kernel stelt aanvallers in staat privileges te escaleren en root toegang te verkrijgen

Een kritieke kwetsbaarheid in de Ubuntu Linux-kernel is ontdekt, waardoor lokale aanvallers hun privileges kunnen escaleren en mogelijk root toegang kunnen verkrijgen op getroffen systemen. De kwetsbaarheid werd onthuld op TyphoonPWN 2025 en heeft zijn oorsprong in een onbalans in het referentietellen van het af_unix-subsysteem, wat leidt tot een use-after-free (UAF) situatie. Het probleem treft Ubuntu 24.04.2 met kernelversie 6.8.0-60-generic. Het is te wijten aan de gedeeltelijke implementatie van upstream Linux-kernelpatches die bugs in het referentietellen van af_unix sockets zouden verhelpen. Aanvallers kunnen deze kwetsbaarheid uitbuiten door het verkeerd beheren van geheugenreferenties, waardoor ze volledige controle over het systeem kunnen krijgen. Canonical heeft snel gereageerd met een update die de kwetsbaarheid verhelpt. Gebruikers van de getroffen versies wordt geadviseerd om onmiddellijk te updaten.

Nieuwe Herodotus Android-malware misleidt detectie door menselijk gedrag na te bootsen

Een nieuwe Android-malwarefamilie, Herodotus, maakt gebruik van willekeurige vertragingen in zijn invoerroutines om menselijk gedrag na te bootsen en zo detectie door beveiligingssoftware te vermijden. De malware wordt aangeboden als een malware-as-a-service (MaaS) voor financieel gemotiveerde cybercriminelen,

waarschijnlijk dezelfde groep achter Brokewell. Herodotus wordt momenteel verspreid via smishing-aanvallen (SMS-phishing) gericht op gebruikers in Italië en Brazilië. De malware probeert de beperkingen van de toegankelijkheidsmachtigingen in Android 13 en latere versies te omzeilen door valse laadschermen weer te geven en gebruikerstoegang toe te staan. Nadat het toegang heeft verkregen, kan de malware tekst invoeren met willekeurige vertragingen tussen 0,3 en 3 seconden, waardoor het lijkt op menselijke typgedrag. Daarnaast biedt het een controlepaneel voor aangepaste SMS-berichten, overlays voor banken en crypto-apps, en het onderscheppen van twee-factor-authenticatiecodes.

Nieuwe Atroposia-malware biedt kwetsbaarheidsscanner

Atroposia is een nieuw malware-as-a-service (MaaS)-platform dat cybercriminelen een remote access trojan (RAT) biedt met functies voor toegang op afstand, gegevensdiefstal en lokale kwetsbaarheidsscanning. Voor een maandabonnement van $200 kunnen aanvallers profiteren van modules zoals verborgen bureaubladtoegang, bestandssysteemcontrole, gegevensuitvoer, clipboard-diefstal en het stelen van inloggegevens en cryptocurrency-wallets. De malware kan communiceren met de command-and-control-infrastructuur via versleutelde kanalen en kan de User Account Control (UAC) van Windows omzeilen. Atroposia beschikt ook over een ingebouwde lokale kwetsbaarheidsscanner die onveilige instellingen en verouderde software detecteert, waarmee aanvallers prioriteit kunnen geven aan exploitatie van kwetsbaarheden. Dit maakt de RAT bijzonder gevaarlijk in bedrijfsomgevingen, waar verouderde VPN-clients of privilege-escalatiefouten kunnen worden misbruikt voor dieper systeemtoegang. Het platform verlaagt de technische drempel voor cybercriminelen, waardoor het een breed scala aan aanvallers aanspreekt.

BlueNoroff's ghostcall en ghosthire campagnes: diepgaande analyse van de laatste dreigingen

BlueNoroff, een bekende APT-groep, heeft zijn aanvallen verder verfijnd met twee nieuwe campagnes: GhostCall en GhostHire. GhostCall richt zich op macOS-apparaten van topfunctionarissen binnen technologiebedrijven en de durfkapitaalsector, waarbij slachtoffers via Telegram worden benaderd en verleid om een vals Zoom-vergadering te betreden. De aanvallers gebruiken echte video-

opnames van eerdere slachtoffers, wat de illusie wekt van een live gesprek. Zodra de slachtoffers hun Zoom-klant bijwerken, worden schadelijke scripts gedownload die malware installeren. GhostHire richt zich op Web3-ontwikkelaars en gebruikt Telegram en GitHub om kwaadaardige bestanden te verspreiden, vermomd als beoordelingsprojecten. Beide campagnes maken gebruik van geavanceerde technieken zoals AI om hun aanvallen te verbeteren en om malware-modules te verbergen.

Waarschuwing voor gratis videogame cheats die infostealer-malware verspreiden

De populaire wens van gamers om competitief voordeel te behalen heeft cybercriminelen de kans geboden om kwaadaardige software te verspreiden via gratis aangeboden game cheats. Cybercriminelen verpakken informatie-steler malware in zogenaamde cheats, waardoor gebruikers onbewust kwaadaardige bestanden downloaden. Deze malware is vaak gekoppeld aan populaire games zoals Fortnite, Apex Legends, Counter-Strike 2 en Roblox. Georganiseerde groepen, zoals de Traffer Teams, spelen een belangrijke rol in de verspreiding van deze malware, door gebruik te maken van platforms als YouTube en TikTok. De malware kan gevoelige gegevens zoals browserwachtwoorden, cookies en cryptowalletinformatie stelen. Spelers worden geadviseerd om verdachte bestanden te scannen en voorzorgsmaatregelen te nemen door antivirussoftware te gebruiken en verdachte bestanden in een virtuele machine te openen.

Gamaredon phishingaanval richt zich op overheidsinstanties en maakt gebruik van WinRAR-kwetsbaarheid

Een nieuwe phishingaanval van de Gamaredon-groep richt zich op overheidsinstanties en maakt gebruik van de kwetsbaarheid in WinRAR. Deze aanvallen worden uitgevoerd door middel van infostealer malware die zich verstopt in ogenschijnlijk onschuldige videospel cheats en mod tools. Dergelijke toepassingen worden gepromoot als prestatieverhogers of hulpmiddelen voor het verbeteren van de game-ervaring, maar bevatten kwaadaardige software die inloggegevens steelt. Dit toont een kwetsbaarheid in het bewustzijn van gebruikers over veilige softwareverificatie en de gevaren van het downloaden van dergelijke programma's van onbetrouwbare bronnen. De malware richt zich specifiek op opgeslagen inloggegevens, cryptocurrency wallets, browser cookies en andere gevoelige

authenticatietokens. Deze gegevens worden vervolgens geëxfiltreerd naar servers die door de aanvallers worden gecontroleerd. Onderzoekers adviseren gebruikers om cheats en mods alleen van officiële bronnen te downloaden en extra beveiligingsmaatregelen, zoals multi-factor authenticatie, te implementeren.

Water Saci hackers maken gebruik van WhatsApp voor verspreiding van SORVEPOTEL malware

Een geavanceerde malwarecampagne die gericht is op Braziliaanse gebruikers maakt gebruik van WhatsApp voor het verspreiden van de SORVEPOTEL malware. Deze campagne, die begon in september 2025, heeft zich in oktober verder ontwikkeld met nieuwe aanvalsmethoden, waaronder een script-gebaseerde aanval. De malware maakt gebruik van meerdere persistentie-mechanismen en een geavanceerde command-and-control (C2) infrastructuur, waarmee aanvallers real-time controle over gecompromitteerde systemen kunnen behouden. Via WhatsApp worden kwaadaardige ZIP-bestanden verspreid naar alle contacten en groepen van geïnfecteerde accounts, wat de verspreiding vergemakkelijkt. De malware gebruikt Visual Basic Script en PowerShell voor fileless executie, wat traditionele detectiemethoden omzeilt. De C2-infrastructuur is gebaseerd op e-mail en HTTP, wat de aanvallers in staat stelt de campagne te monitoren en aan te passen. Deze malware biedt uitgebreide toegang tot besmette systemen, waardoor het een grote bedreiging vormt voor financiële instellingen en bedrijven in Brazilië.

BiDi Swap: Een truc die valse URL's echt doet lijken

De BiDi Swap-techniek maakt misbruik van een browserfout in de manier waarop tekstrichtingen worden verwerkt, wat het mogelijk maakt om valse URL's te creëren die echte websites nabootsen. Deze aanval, die gebruik maakt van de bidirectionele tekstfunctie, zorgt ervoor dat een URL die visueel betrouwbaar lijkt, naar een andere locatie leidt. Door het combineren van van rechts naar links (RTL) en van links naar rechts (LTR) tekstrends, kunnen aanvallers valse subdomeinen of URL-paden maken die het moeilijk maken voor gebruikers om kwaadaardige links te herkennen. Dit soort aanvallen is niet nieuw, maar het wordt steeds vaker gebruikt in phishingaanvallen. Browserleveranciers zoals Chrome, Firefox en Edge hebben al enige bescherming ingebouwd, maar deze blijft vaak onvoldoende. Het wordt

aanbevolen om altijd verdachte URL's te verifiëren en bewustzijn te creëren over de gevaren van dergelijke aanvallen.

C3FaRiR biedt RDP-toegang aan op het darkweb

Een cybercrimineel, opererend onder het alias C3FaRiR, heeft vermoedelijk RDP-toegang aangeboden tot verschillende “houses en workgroup” systemen in meerdere landen. De toegang zou via brute-force methoden zijn verkregen en wordt gepromoot als tijdelijk beschikbaar, met een garantieperiode van slechts twee uur. De startprijs voor deze toegang bedraagt $10. De aanbieding wordt zowel op het clearnet als op het darkweb gepresenteerd. Er wordt gewaarschuwd voor de volatiliteit van de toegang en het tijdelijke karakter ervan, wat de veiligheid en betrouwbaarheid van deze aanbieding beïnvloedt.

Wasp macOS infostealer te koop aangeboden via Darkweb

Een dreigingsactor met de naam iLeakSupp heeft de Wasp-macOS-infostealer gepresenteerd, aangeboden als een Malware-as-a-Service (MaaS) model. Het programma, dat geen bestandselementen bevat en cross-platform werkt, is ontwikkeld met Apple's Open Scripting Architecture (OSA). Het kan draaien op zowel x86-64 als ARM64 architecturen en is compatibel met recente versies van macOS. Wasp heeft een detectiegraad van 0/62 op VirusTotal en biedt verschillende functies, zoals een controlepaneel op basis van React, phishingmogelijkheden voor Ledger Live, en ondersteuning voor het stelen van cryptowallets. Het richt zich vooral op browsers zoals Chrome, Edge, Brave en Firefox. De infostealer is te huur voor $3000 voor een periode van 30 dagen.

Justitie vervolgt leden van sadistische onlinegroep NLM

Justitie vervolgt Justin B., een 25-jarige man uit Eindhoven, en andere leden van de sadistische onlinegroep NLM. Deze groep zou verantwoordelijk zijn voor het aanzetten van jongeren tot gewelddadige daden, waaronder zelfverminking en moord. Leden van de groep zouden via het internet gewelddadige handelingen verheerlijkten en gebruikers aanmoedigden om steeds extremere geweldsmiddelen te gebruiken, waarbij zelfs referenties naar Breivik werden gemaakt. De groep opereerde als een criminele organisatie met terroristisch oogmerk, en de vervolging

van Justin B. en anderen is een reactie op de groeiende bezorgdheid over dergelijke gewelddadige online netwerken.

Tien Fransen aangeklaagd voor online pesten van Brigitte Macron

Tien Fransen staan terecht voor hun rol in het online pesten van Brigitte Macron. De beschuldigden verspreidden schadelijke berichten en valse beschuldigingen via sociale media, wat leidde tot juridische stappen. De zaak heeft veel aandacht getrokken in de Franse media, waarbij de beklaagde Amandine Roy in haar verdediging verklaarde dat zij geen excuses wilde aanbieden aan de Franse eerste dame, maar dat de Macrons hun excuses aan haar zouden moeten aanbieden. Deze zaak benadrukt de ernst van cyberpesten, vooral wanneer het invloed heeft op publieke figuren. Het gerechtelijke proces gaat door en kan gevolgen hebben voor hoe online haat en intimidatie worden aangepakt in Frankrijk.

Politie meldt stijging aangiften verkoopfraude met fatbikes

De politie heeft een aanzienlijke stijging gemeld in het aantal aangiften van verkoopfraude met fatbikes. Het aantal aangiften is in de afgelopen jaren explosief gestegen, van 2 in 2021 naar 725 in 2025, met een totaal schadebedrag van ongeveer 700.000 euro. De meeste slachtoffers deden hun aankopen via webwinkels, maar ook Marktplaats, Facebook en andere sociale media zijn vaak genoemd als platforms voor de fraude. Webshops zoals Fatbike-discounter.com, Fatbikeskopen.nl en Bikevibez.com worden in verband gebracht met de meeste meldingen. De politie waarschuwt consumenten voor malafide webshops, vooral met Black Friday in aantocht, en roept slachtoffers op om aangifte te doen. Dit helpt niet alleen om andere slachtoffers te voorkomen, maar maakt het mogelijk om een onderzoek te starten wanneer er drie of meer meldingen zijn.

Signal heeft geen andere keuze dan AWS te gebruiken door machtsconcentratie

Signal, de versleutelde chatapp, heeft geen keuze dan gebruik te maken van Amazon Web Services (AWS) vanwege de machtsconcentratie van grote techbedrijven zoals Amazon. Meredith Whittaker, hoofd van Signal, benadrukt in berichten op X dat de enorme kosten voor het opzetten en onderhouden van infrastructuren zoals die van AWS, evenals het beperkte aantal bedrijven dat deze

technologie kan leveren, Signal dwingen AWS te gebruiken. Dit werd pijnlijk duidelijk toen een grote storing bij AWS vorige week ervoor zorgde dat veel websites en applicaties, waaronder Signal, tijdelijk niet bereikbaar waren. Whittaker merkt op dat veel gebruikers zich niet realiseren hoe afhankelijk we zijn van enkele grote spelers die de technologische infrastructuur beheersen. Ze hoopt dat deze storing een leermoment zal zijn, zodat het bewustzijn van de risico's van deze machtsconcentratie wordt vergroot.

Google ontkent groot datalek met Gmail-gebruikers

Google heeft wederom ontkend dat het bedrijf te maken heeft gehad met een groot datalek van Gmail-gebruikers. Dit volgt op berichten in de media waarin werd gesuggereerd dat de wachtwoorden van 183 miljoen Gmail-gebruikers zouden zijn gestolen. De gegevens werden in een logbestand van infostealer-malware aangetroffen. Deze malware verzamelt inloggegevens van besmette systemen en stuurt deze naar aanvallers. De betrokken e-mailadressen werden toegevoegd aan de datalekzoekmachine Have I Been Pwned. Google verduidelijkte dat de gestolen gegevens niet afkomstig zijn van een datalek bij Gmail, maar van geïnfecteerde systemen van gebruikers. Eerder dit jaar had Google al gereageerd op berichten over een vermeend beveiligingsprobleem bij Gmail, dat volgens hen ook onjuist was.

Noyb dient strafklacht in tegen gezichtsherkenningsbedrijf Clearview AI

Privacystichting Noyb heeft bij het Oostenrijkse Openbaar Ministerie een strafklacht ingediend tegen Clearview AI en haar managers. Het bedrijf staat bekend om zijn gezichtsherkenningssysteem, dat wereldwijd wordt aangeboden aan opsporings- en politiediensten. Noyb beschuldigt Clearview AI ervan Europese privacyrechten te negeren en noemt het bedrijf een herhaalde overtreding van de Algemene Verordening Gegevensbescherming (AVG). Clearview AI heeft eerder al miljoenenboetes ontvangen van Europese privacytoezichthouders, maar zou de wetgeving niet naleven. De stichting stelt dat het bedrijf de AVG-schendingen omzeilt door het niet naleven van opgelegde boetes en sancties. Als de strafklacht succesvol is, kunnen de managers van Clearview AI mogelijk gevangenisstraffen krijgen en persoonlijk aansprakelijk worden gesteld voor hun acties.

Duitse overheid waarschuwt voor kwetsbare Exchange-servers

De Duitse overheid uit zorgen over het gebruik van verouderde versies van Microsoft Exchange Server bij tienduizenden bedrijven, ziekenhuizen, scholen en andere instellingen. Het Bundesamt für Sicherheit in der Informationstechnik (BSI) meldt dat 92% van de 33.000 on-premises Exchange-servers in Duitsland draait op versies die inmiddels niet meer ondersteund worden, zoals Exchange 2016 en 2019. Het BSI waarschuwt dat bij een kwetsbaarheid in deze versies geen patch zal worden uitgebracht, wat kan leiden tot ernstige beveiligingsrisico's. De overheid adviseert bedrijven en organisaties om onmiddellijk te upgraden naar de ondersteunde Subscription Edition van Exchange Server of naar een alternatieve oplossing te migreren. Verder wordt aangeraden om toegang tot webgebaseerde diensten zoals Outlook Web Access te beperken via vertrouwde IP-adressen of VPN. Het BSI benadrukt dat onbeveiligde servers een ernstige dreiging vormen voor gegevensdiefstal en ransomware-aanvallen.

RDI kondigt intensiever toezicht aan op cyberveiligheid van digitale producten

De Rijksinspectie Digitale Infrastructuur (RDI) heeft in het Meerjarenplan 2026-2030 aangekondigd het toezicht op de cyberveiligheid van digitale producten in 2026 te intensiveren. De focus ligt op het versterken van de digitale weerbaarheid van Nederland, waarbij de veiligheid van digitale producten cruciaal wordt geacht. Aandacht gaat uit naar de impact van updates, waarbij verouderde software of gemiste updates kwetsbaarheden kunnen creëren. De RDI wijst ook op risico's die ontstaan door de ongecontroleerde import van digitale producten, vooral uit landen als China, die kunnen leiden tot storingen in kritieke infrastructuren. Het plan benadrukt ook de noodzaak om accumulatieve storingen door non-compliant producten te voorkomen. Verder wordt de invloed van kunstmatige intelligentie op de productveiligheid genoemd, wat vraagt om nieuwe benaderingen van toezicht en risicobeheer.

Ransomware winsten dalen doordat slachtoffers stoppen met betalen aan hackers

De betalingen aan ransomware-daders zijn gedaald tot een historisch laag niveau, waarbij slechts 23% van de getroffen bedrijven aan de eisen van de aanvallers voldoet. Dit volgt op een afname van het betalingspercentage die al zes jaar in een neerwaartse trend zit. Organisaties hebben sterkere beveiligingsmaatregelen

getroffen, terwijl overheden de druk opvoeren om slachtoffers ervan te weerhouden losgeld te betalen. De meerderheid van de recente aanvallen (76%) betrof datadiefstal, waarbij de aanvallers dreigen de gestolen gegevens openbaar te maken. Deze dubbele afpersing heeft ransomware-groepen ertoe aangezet zich meer te richten op middelgrote bedrijven, die vaker bereid zijn te betalen. Ook is er een verschuiving naar social engineering en het aantrekken van interne medewerkers om aanvallers toegang te geven. Ransomware-groepen blijven hun strategieën aanpassen in reactie op de afnemende winstgevendheid van hun aanvallen.

Onderzoek: darkwebforums delen instructies voor misbruik in kinderopvang

Onderzoekers troffen op afgeschermde fora op het dark web aanwijzingen dat zedendelinquenten handleidingen en ervaringen uitwisselen om toegang te krijgen tot kinderopvanglocaties en misbruik te plegen, terwijl ze ontdekking proberen te vermijden. Anonimiserende browsers en versleutelde berichtenapps faciliteren het delen van materiaal en onderlinge coaching buiten zicht van opsporingsdiensten. Criminologen spreken van grootschalige, georganiseerde netwerken die gedrag normaliseren en risico's vergroten, mede omdat signalen in opvanginstellingen vaak onopgemerkt blijven. In enkele Australische zaken werd een dader via online posts geïdentificeerd, wat leidde tot veroordelingen voor misdrijven tegen vele kinderen; experts stellen dat toezicht en procedures in kinderopvang tekortschieten. Specialisten waarschuwen dat internetplatforms daders strategischer maken en informatie over zwakke plekken snel verspreiden. Zij bepleiten versterkte preventie, betere detectie en nauwere samenwerking tussen instanties om slachtoffers sneller te identificeren en netwerken te ontmantelen.

overheid verliest grip op ict: 'moeten stoppen met deze waanzin'

Het IT-beleid van de Nederlandse overheid staat onder druk, vooral in de aanloop naar de verkiezingen, waar digitalisering weinig aandacht krijgt. Deskundigen wijzen op de verloren grip op ICT, zoals de beslissing van de Belastingdienst om data op te slaan bij Microsoft, en problemen zoals de verouderde ICT-infrastructuur van het Openbaar Ministerie en herhaalde storingen met communicatiesystemen zoals C2000. Experts pleiten voor een verschuiving in perspectief en vinden dat de overheid ICT moet zien als een doorlopend proces, in plaats van een eenmalige

investering. Ze pleiten voor betere samenwerking tussen overheidsinstanties, minder afhankelijkheid van buitenlandse techbedrijven en meer aandacht voor het onderhoud van digitale systemen. Ook wordt het gebrek aan technische expertise in topfuncties van de overheid als een belangrijke belemmering genoemd. Hoewel digitalisering op de politieke agenda staat, twijfelen experts aan de uitvoeringskracht van de regering.

OpenAI deelt cijfers over ChatGPT-gebruikers met suïcidale gedachten

OpenAI heeft nieuwe cijfers gedeeld over het aantal ChatGPT-gebruikers die tekenen van psychose of suïcidale gedachten vertonen. De chatbot heeft wekelijks zo'n 800 miljoen actieve gebruikers. Ongeveer 0,07 procent van deze gebruikers vertoonde signalen die wijzen op een psychose of zelfmoordgedachten, terwijl 0,15 procent gesprekken voerde over mogelijke suïcidale plannen. OpenAI werkt samen met experts om de chatbot beter te laten reageren op zulke gesprekken. Het bedrijf heeft reacties geïmplementeerd die gebruikers aansporen om hulp te zoeken in de echte wereld. Dit volgt op eerdere meldingen, waaronder een rechtszaak waarbij een 16-jarige jongen naar verluidt door ChatGPT werd aangemoedigd zelfmoord te plegen. OpenAI blijft werken aan verbeteringen in de herkenning en begeleiding van gevoelige gesprekken.

81% van de routergebruikers heeft wachtwoord niet veranderd, blootstelling aan hackers

In 2025 bleek uit een onderzoek van Broadband Genie dat 81% van de gebruikers van breedbandrouters nooit het standaard beheerderswachtwoord heeft veranderd, wat hun netwerken blootstelt aan ernstige malware-risico's. Dit gebrek aan bewustzijn werd aangetoond in een enquête onder 3.242 gebruikers, ondanks regelgevende druk en toenemende media-aandacht. Veel consumenten beschouwen de routerconfiguratie als een eenvoudige taak zonder zich bewust te zijn van de risico's. Dit maakt hun apparaten vatbaar voor aanvallen, aangezien de standaard wachtwoorden gemakkelijk te vinden zijn op het internet. De aanvallen maken gebruik van 'credential stuffing', waarbij hackers bekende inloggegevens proberen om toegang te krijgen tot de apparaten. Zodra toegang is verkregen, kunnen aanvallers bijvoorbeeld DNS-instellingen wijzigen of malware installeren, waardoor

de apparaten op afstand kunnen worden beheerd. Dit benadrukt het belang van het veranderen van standaardwachtwoorden om netwerken te beschermen.

Zweedse netbeheerder Svenska Kraftnat meldt inbraak op filesharingsysteem

Svenska Kraftnat, de Zweedse netbeheerder, heeft een inbraak op hun filesharingsysteem gemeld. Criminelen hebben toegang gekregen tot het systeem en de ransomwaregroep Everest heeft de aanval opgeëist. Everest claimt 280 gigabyte aan gegevens te hebben gestolen, hoewel het type gestolen data nog onderzocht wordt. Svenska Kraftnat heeft bevestigd dat missiekritische systemen niet getroffen zijn en de energievoorziening in Zweden niet in gevaar is gebracht. De aanval was beperkt tot een extern filesharingsysteem. Er zijn nog geen details bekend over hoe de aanvallers toegang hebben verkregen. Deze aanval volgt op eerdere aanvallen van dezelfde groep, waaronder een ransomware-aanval op Collins Aerospace, die mogelijk werd uitgevoerd via een gestolen ftp-wachtwoord. Het onderzoek naar de aanval op Svenska Kraftnat loopt nog.