## Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

14-10-2025:

Cyberaanval bij omrin heeft impact op recyclinglocaties en openbare diensten

Omrin, een Fries afvalverwerkingsbedrijf, is sinds zondag getroffen door een ransomware-aanval, waardoor zes van de zeven Estafettewinkels gesloten zijn. De winkels in Leeuwarden, Sneek, en andere locaties zijn niet toegankelijk, met uitzondering van de winkel in Burgum, die alleen contante betalingen accepteert. Het bedrijf meldt een technische storing, veroorzaakt door de aanval, maar de afvalverwerking zelf is niet in gevaar. Milieustraten blijven open en het ophalen van grof vuil gaat door, hoewel nieuwe afspraken alleen per e-mail gemaakt kunnen worden. Omrin onderzoekt de aanval, maar wil geen details geven over het geëiste losgeld of de herkomst van de aanval. Eerdere aanvallen op lokale overheden en bedrijven, zoals het Frisius MC ziekenhuis en Wetsus, maken duidelijk dat dergelijke cyberaanvallen steeds vaker voorkomen in de regio.

Criminelen publiceren miljoenen gestolen records van salesforce-klanten

Criminelen hebben miljoenen gestolen records van Salesforce-klanten openbaar gemaakt, waaronder gegevens van 7,3 miljoen passagiers van Vietnam Airlines en 5,7 miljoen passagiers van Qantas. De aanvallers gebruikten een derde partij platform om klantgegevens te stelen. Qantas bevestigde de diefstal van naam, e-mailadres, geboortedatum, telefoonnummer, en maaltijdvoorkeuren van haar passagiers. Salesforce, een veelgebruikte leverancier van CRM-software, werd recentelijk gecompromitteerd door aanvallers die gebruikmaakten van social engineering en gestolen tokens van Salesloft. Andere getroffen bedrijven omvatten Albertsons, GAP, Fujifilm en Engie Resources. De publicatie van de gestolen gegevens komt na meerdere meldingen van datalekken die Salesforce-omgevingen betreffen. De situatie benadrukt het risico van cloudgebaseerde platformen en de kwetsbaarheid van derde partijen in het beschermen van klantinformatie.

Bun.nl slachtoffer van ThreeAM ransomware-aanval

Bun.nl, een retailbedrijf uit Nederland, is recent het slachtoffer geworden van een aanval door de ransomwaregroep ThreeAM. De aanval werd op 13 oktober 2025 gemeld. Er is nog weinig bekend over de specifieke details van de aanval, zoals de omvang van de schade of de eisen van de aanvallers. ThreeAM is een actieve groep

die bekend staat om het versleutelen van bedrijfsdata en het eisen van losgeld in ruil voor decryptiesleutels. De aanval heeft mogelijk invloed op de operationele capaciteit van het getroffen bedrijf. Dit incident benadrukt de voortdurende dreiging van ransomware-aanvallen voor bedrijven in Nederland, die steeds vaker het doelwit zijn van dergelijke cyberaanvallen. De autoriteiten en de getroffen organisatie werken waarschijnlijk samen om de situatie te onderzoeken en verdere schade te beperken.

Stijging van incidenten bij defensiefaciliteiten in de VS en Duitsland temidden van wereldwijde spanningen

De recente explosie in Tennessee bij Accurate Energetic Systems, op 10 oktober 2025, maakt deel uit van een zorgwekkende toename van incidenten bij Amerikaanse en Duitse defensiefaciliteiten, die belangrijke leveranciers zijn van militair materieel te midden van de oorlog in Oekraïne. De Verenigde Staten hebben te maken met operationele ongelukken, terwijl Duitsland wordt geconfronteerd met vermoedelijke Russische sabotage. In de VS zijn de incidenten de afgelopen achttien maanden verdubbeld, met een brand in Pennsylvania en een explosie in Tennessee, terwijl Duitsland drie verdachte incidenten ervaarde, waaronder brandstichting en een cyberaanval. De Duitse autoriteiten onderzoeken deze gevallen als sabotage, en er worden links gelegd naar Russische invloed. De incidenten benadrukken de kwetsbaarheden in de defensieve toeleveringsketens van de NAVO en roepen op tot verbeterde veiligheid en tegenmaatregelen.

Waarschuwing voor meerdere kwetsbaarheden in Newforma Info Exchange en Project Center Server

Er zijn meerdere ernstige kwetsbaarheden ontdekt in de Newforma Info Exchange (NIX) en Newforma Project Center Server (NPCS). Deze kwetsbaarheden kunnen aanvallers in staat stellen volledige controle over de getroffen servers te krijgen. De CVE-2025-35050 maakt het mogelijk om op afstand code uit te voeren met hoge privileges via een kwetsbaar NIX-eindpunt, wat een risico vormt voor systemen die verbonden zijn met NPCS. Andere kwetsbaarheden, zoals CVE-2025-35051 en CVE-2025-35055, stellen aanvallers in staat ongeauthenticeerde toegang te krijgen tot kritieke systemen. Dit kan leiden tot datalekken en ernstige gevolgen voor de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens. Organisaties worden

aangeraden om netwerktoegang tot kwetsbare eindpunten te beperken en de monitoring te verbeteren om verdachte activiteiten snel te detecteren.

Kwetsbaarheid in Happy DOM blootlegt 2,7 miljoen gebruikers aan RCE-aanvallen

Er is een ernstige kwetsbaarheid ontdekt in Happy DOM, een populaire JavaScript DOM-implementatie, die versies tot v19 beïnvloedt. Deze kwetsbaarheid verhoogt het risico op Remote Code Execution (RCE)-aanvallen, wat mogelijk impact heeft op de 2,7 miljoen wekelijkse gebruikers van het pakket. Het probleem ontstaat doordat de Node.js VM Context, die door Happy DOM wordt gebruikt, geen volledig geïsoleerde omgeving biedt. Dit maakt het mogelijk voor niet-vertrouwde code om te ontsnappen en toegang te krijgen tot onderliggende systeemfunctionaliteiten. De belangrijkste oorzaak is dat JavaScript-evaluatie standaard is ingeschakeld, wat een beveiligingsrisico vormt wanneer onbetrouwbare code wordt uitgevoerd. Aangezien de kwetsbaarheid ook Server-Side Rendering (SSR)-toepassingen betreft, kunnen aanvallers gevoelige gegevens stelen, interne systemen compromitteren of code uitvoeren. Happy DOM heeft een patch uitgebracht; gebruikers wordt aangeraden om snel naar versie 20 of hoger te upgraden.

7-Zip dicht kwetsbaarheden die remote code execution via zip-bestanden mogelijk maken

In de populaire archiveringssoftware 7-Zip zijn twee kwetsbaarheden ontdekt die remote code execution mogelijk maken bij het verwerken van speciaal geprepareerde zip-bestanden. Deze kwetsbaarheden, aangeduid als CVE-2025-11001 en CVE-2025-11002, ontstonden bij het verwerken van symbolische links binnen zip-bestanden. Aanvallers konden bestanden naar andere directories schrijven en daardoor malware of andere kwaadaardige code laden. De kwetsbaarheden werden gepatcht in versie 25.00 van 7-Zip, die op 5 juli 2025 werd uitgebracht. Het bestaan van de kwetsbaarheden werd pas recent bekendgemaakt, hoewel ze al in mei waren gemeld bij de ontwikkelaar. De impact van de lekken is beoordeeld met een score van 7.0 op een schaal van 10, omdat het slachtoffer het zip-bestand zelf moet openen om getroffen te worden.

Microsoft sluit IE-modus af na misbruik door hackers

Microsoft heeft de Internet Explorer (IE) modus in de Edge-browser aangepast na meldingen in augustus 2025 dat onbekende hackers deze legacy-functie misbruikten om ongeautoriseerde toegang te verkrijgen tot gebruikersapparaten. De aanvallers maakten gebruik van verouderde kwetsbaarheden in de Chakra-engine van Internet Explorer en pasten sociale-engineeringtechnieken toe om slachtoffers naar gemanipuleerde websites te leiden. Na het herladen van de pagina in IE-modus, konden de aanvallers op afstand code uitvoeren en hun privileges verhogen om volledige controle over het apparaat van het slachtoffer te verkrijgen. Microsoft heeft als reactie de IE-modus verder beperkt. Gebruikers moeten nu handmatig websites toevoegen aan een lijst om de IE-modus te kunnen activeren, waarmee de toegang voor aanvallers wordt bemoeilijkt. Dit besluit heeft tot doel de beveiliging te verbeteren, terwijl de compatibiliteit met legacy-webinhoud behouden blijft.

Invoicely-databaselek blootlegt 180.000 gevoelige records

Een cybersecurityonderzoeker ontdekte dat bijna 180.000 bestanden, waaronder persoonlijke gegevens (PII) en bankinformatie, onbeschermd waren opgeslagen in een database die gekoppeld is aan het platform Invoicely. Deze database bevatte facturen, belastingformulieren, cheque-afbeeldingen en persoonlijke gegevens zoals namen, adressen, telefoonnummers en belastingnummers. De blootstelling van dergelijke gegevens vormt een ernstig risico voor identiteitsdiefstal en financiële fraude. Cybercriminelen kunnen de gegevens gebruiken voor gerichte aanvallen, zoals spear-phishing of valse facturatiefraude. De database werd snel offline gehaald na ontdekking, maar het is nog onduidelijk hoe lang de informatie publiekelijk toegankelijk was of of onbevoegden toegang hebben gehad. Gebruikers wordt geadviseerd om multi-factor authenticatie te gebruiken en wachtwoorden niet opnieuw te gebruiken om verdere schade te voorkomen.

Kritieke kwetsbaarheid in AMD's SEV-SNP stelt hackers in staat vertrouwelijke data te stelen

Er is een ernstige kwetsbaarheid ontdekt in AMD's Secure Encrypted Virtualization met Secure Nested Paging (SEV-SNP), een technologie die wordt gebruikt door grote cloudproviders zoals AWS, Azure en Google Cloud. De aanval, genaamd RMPocalypse, maakt misbruik van een fout in de initialisatie van de Reverse Map Table (RMP), die bedoeld is om de geheugenintegriteit te waarborgen en te

voorkomen dat hypervisors versleutelde virtuele machines (VM's) manipuleren. Hackers kunnen door deze kwetsbaarheid de RMP-entries vervalsen, waardoor de geheimhouding en integriteit van de gegevens wordt geschonden. De exploitatie van deze kwetsbaarheid kan leiden tot het uitlekken van gevoelige gegevens zoals AI-modellen en bedrijfsworkloads. AMD is op de hoogte van het probleem en werkt aan een oplossing, maar er zijn nog geen patches beschikbaar voor de getroffen hardware.

Meer dan 30 potentiële slachtoffers geïdentificeerd tijdens internationale Hackathon tegen mensenhandel

Van 15 tot 19 september 2025 vond de vierde editie van de EMPACT Trafficking in Human Beings (THB) Hackathon plaats, ondersteund door Europol. Nederland leidde deze actie, met steun van Duitsland en het Verenigd Koninkrijk. De hackathon richtte zich op het opsporen van online mensenhandel, waarbij 73 experts uit 26 landen deelnamen. Gedurende de actieweek werden 33 potentiële slachtoffers van mensenhandel geïdentificeerd, evenals 31 verdachten. In totaal werden 44 onlineplatforms onderzocht, waar aanwijzingen voor mensenhandel werden ontdekt, waaronder platforms voor seksuele en arbeidsgerelateerde uitbuiting. Daarnaast werd een toename van advertenties die door kunstmatige intelligentie werden gegenereerd vastgesteld, evenals een verschuiving naar cryptovaluta als betaalmethode. De hackathon benadrukte de groeiende rol van online platforms in de uitbuiting van mensen en de noodzaak voor intensieve grensoverschrijdende samenwerking.

Duitse politie sluit 1.400 fraudewebsites na grote operatie

In een gezamenlijke operatie onder leiding van de Duitse politie, de financiële toezichthouder BaFin, Europol en Bulgaarse autoriteiten zijn 1.400 illegale websites gesloten die betrokken waren bij cybertradingfraude. Deze websites, die voornamelijk actief waren in Oost-Europa, wervden gebruikers om geld te investeren in frauduleuze beleggingsaccounts. De slachtoffers werden vaak maandenlang misleid voordat ze ontdekten dat hun geld niet was geïnvesteerd. De operatie, genaamd "Heracles," is een vervolg op een eerdere actie in juni, waarbij 800 fraudewebsites werden afgesloten. De autoriteiten gaven aan dat de cybercriminelen steeds professioneler te werk gaan, waarbij kunstmatige intelligentie werd ingezet

om nieuwe, illegale websites te creëren. Door de operationele maatregelen is de technische infrastructuur van de daders aanzienlijk verzwakt, hoewel er nog steeds pogingen worden ondernomen om toegang te krijgen tot de getroffen websites.

Vietnam Airlines lekt persoonlijke gegevens van 7,3 miljoen passagiers

Vietnam Airlines heeft de persoonlijke gegevens van 7,3 miljoen passagiers gelekt, waaronder namen, telefoonnummers, e-mailadressen, geboortedatums en informatie over hun loyaliteitsprogramma. De gegevens werden gestolen door criminelen die in juni inbraken op de Salesforce-omgeving van de luchtvaartmaatschappij. Salesforce, een populaire CRM-softwareleverancier, werd eerder dit jaar getroffen door aanvallen die mogelijk gebruik maakten van gestolen tokens en social engineering. E-mailadressen van de getroffen passagiers zijn toegevoegd aan de datalekzoekmachine Have I Been Pwned. Van de gestolen e-mailadressen was 39 procent al eerder in andere datalekken bekend. Het is mogelijk dat ook klanten uit Nederland en België getroffen zijn, gezien de internationale reikwijdte van Vietnam Airlines en het gebruik van de zoekmachine om datalekken te controleren. Dit datalek heeft implicaties voor de privacy en veiligheid van persoonlijke gegevens, ook voor de inwoners van deze landen.

Beveiliging van goedkope Chinese camera's stelt gebruikers bloot aan risico's

Goedkope camera's uit China blijken ernstig beveiligingsproblemen te vertonen, wat hackers in staat stelt om live mee te kijken in privéruimtes van gebruikers. Dit werd ontdekt door de Nederlandse ethische hacker Wouter van Dongen, die de kwetsbaarheden in de apparaten blootlegde. De camera's, die vaak via online marktplaatsen worden verkocht, gebruiken onvoldoende beveiligingsmaatregelen zoals zwakke wachtwoorden en verouderde software. Dit maakt het mogelijk voor kwaadwillenden om de controle over de camera's over te nemen, zonder dat gebruikers het merken. Van Dongen benadrukt de gevaren voor de privacy van consumenten en waarschuwt voor het gebruik van goedkope, onbetrouwbare technologie. Het probleem heeft wereldwijd aandacht getrokken, aangezien dergelijke apparaten in veel huishoudens te vinden zijn.

Cloudserviceproviders moeten transparant zijn over opslaglocatie van data

De Rijksinspectie Digitale Infrastructuur (RDI) heeft cloudserviceproviders aangespoord om duidelijk aan klanten te maken waar hun gegevens precies zijn opgeslagen. Dit komt naar voren als onderdeel van de implementatie van de Cyberbeveiligingswet (Cbw), die in de tweede helft van 2026 in werking treedt. Cloudproviders moeten volgens de wet risico's rondom databeveiliging in kaart brengen en passende maatregelen nemen. De RDI benadrukt dat het voor klanten essentieel is om te weten waar hun data zich bevindt, omdat dit gevolgen kan hebben voor de privacy en integriteit, vooral als de opslaglocatie onder een andere jurisdictie valt. Daarnaast moeten providers klanten ondersteunen bij het veilig en overdraagbaar houden van data. De RDI zal in de toekomst proactief toezicht houden op cloudserviceproviders om naleving van de wet te waarborgen.

Huisartsenspoedposten voldoen vaak niet aan NEN 7510-norm voor informatiebeveiliging

Uit onderzoek van de Inspectie Gezondheidszorg en Jeugd (IGJ) blijkt dat veel huisartsenspoedposten in Nederland niet voldoen aan de NEN 7510-norm voor informatiebeveiliging. Van de 49 onderzochte organisaties voldoen er slechts zes aan de norm. De NEN 7510 is verplicht voor zorginstellingen en bepaalt hoe zij hun informatiebeveiliging moeten organiseren. Ondanks het gebrek aan certificering is er wel bewustzijn over het belang van goede beveiliging. Veel organisaties hebben maatregelen getroffen, zoals het implementeren van multifactorauthenticatie en het trainen van medewerkers. De IGJ heeft aanvullende vragen gesteld aan de organisaties die niet voldoen en afspraken gemaakt over het behalen van de norm. Alle betrokkenen hebben beloofd hun informatiebeveiliging uiterlijk eind 2026 op orde te hebben.

Android spyware met Rails-gebaseerd C2-systeem op Dark Web te koop

Op het Dark Web wordt momenteel een Android spyware-tool aangeboden die een command-and-control (C2) systeem gebruikt, gebouwd met het Rails-framework en ondersteund door Metasploit en ADB. De spyware stelt aanvallers in staat om Android-apparaten op afstand te controleren. Het gebruik van dergelijke malware kan ernstige privacy- en veiligheidsrisico's voor gebruikers met zich meebrengen, aangezien het volledige toegang tot persoonlijke gegevens en communicatie kan bieden. Deze tool kan ook worden ingezet voor het uitvoeren van

spionageactiviteiten of andere vormen van digitale misdrijven. De verkoop van dergelijke malware is een indicatie van de voortdurende groei van cyberdreigingen op het Dark Web, waar tools en diensten voor cybercriminaliteit steeds vaker worden verhandeld.

Opnieuw telefoontjes van een Engelstalig of Nederlandstalig bandje

Er zijn opnieuw meldingen van oplichting via telefoontjes waarin een Engels of Nederlands gesproken bandje te horen is. De bellers doen zich voor als vertegenwoordigers van verschillende officiële instanties, zoals de Nationale Politie Amsterdam, de Hoge Raad, of een Europese bank. De telefoonnummers lijken afkomstig van vertrouwde bronnen, maar zijn gespooft, wat betekent dat oplichters een ander nummer laten zien dan dat ze daadwerkelijk gebruiken. De bellers maken slachtoffers bang door te zeggen dat hun BSN-nummer misbruikt is of dat er een arrestatiebevel tegen hen loopt. Vervolgens worden slachtoffers gevraagd om persoonlijke gegevens door te geven, geld over te maken naar opgegeven rekeningen of zelfs software te downloaden, zodat de oplichters toegang krijgen tot hun computer. Het advies is om nooit geld over te maken of software te downloaden op verzoek van onbekende bellers.