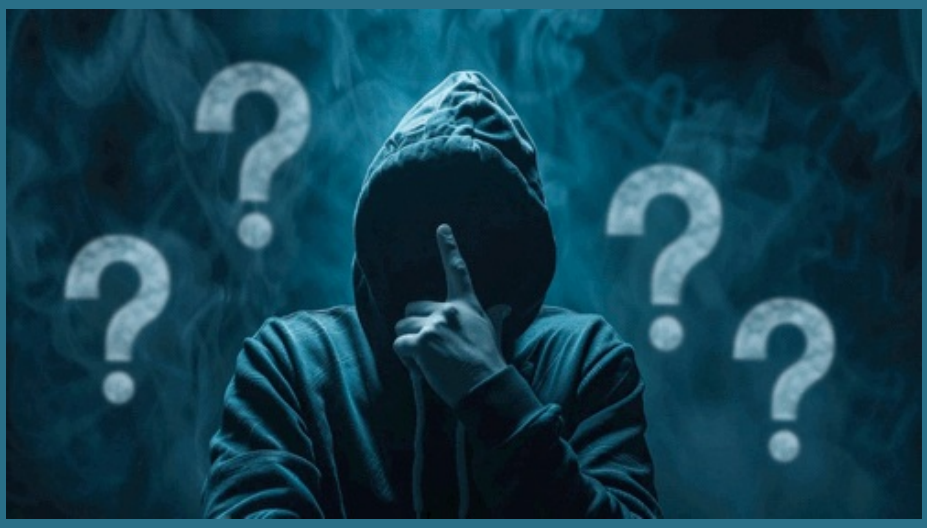
Cybercrimeinfo

"Omdat wat waardevol is, beschermd moet worden"

Nieuwsbrief 395



Ben jij up-to-date met het cybernieuws van week 49-2025?

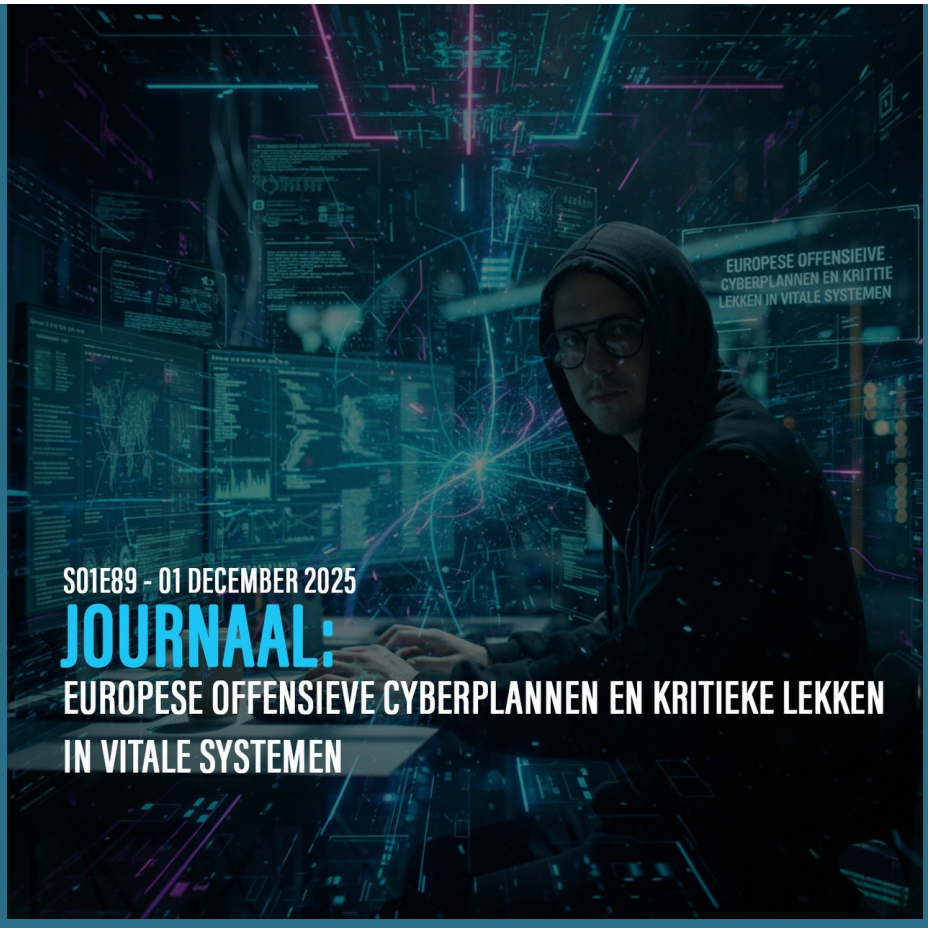
De digitale dreigingen van de afgelopen week variëren van geopolitieke spanningen tot verrassende natuurverschijnselen. Terwijl het Belgische bpost worstelde met de gevolgen van een aanval door de Tridentlocker groep, stonden systeembeheerders op scherp door twee kritieke kwetsbaarheden met de hoogst mogelijke CVSS-score van 10.0 in zowel React Server Components als Apache Tika.
Maar het gevaar schuilt niet alleen in kwaadaardige code. Wist je bijvoorbeeld dat intense zonnestraling verantwoordelijk was voor storingen in duizenden Airbus A320 cockpits? Op het wereldtoneel zien we een verharding: de NAVO overweegt nu preventieve offensieve cyberoperaties als antwoord op Russische agressie, terwijl groepen als TwoNet en Warp Panda industriële systemen en VMware-servers bestoken.
Ook in eigen land is er nieuws, de Belastingdienst blijft tot 2028 gebruikmaken van het omstreden 'Klant Toezicht Model'. Van onzichtbare Unicode tekens in Visual Studio Code tot spionagesoftware die via UDP communiceert, de aanvalstechnieken worden steeds geavanceerder.
Weet jij welk land SIM-binding verplicht stelt of welke enorme som cryptovaluta Europol in beslag nam? Test je kennis en digitale weerbaarheid in de quiz van deze week!
Veel succes!

QUIZ 49-2025

Strategisch Dreigingsrapport Cyberveiligheid week 49-2025

Het rapport biedt een holistische analyse van het huidige cyberdreigingslandschap in de Benelux, waar geopolitieke spanningen, geavanceerde cybercriminaliteit en kwetsbaarheden in technologie samenkomen. De analyse toont aan hoe statelijke actoren zoals Rusland, China, Iran en Noord-Korea digitale agressie inzetten, van desinformatie tot cyberaanvallen, wat direct invloed heeft op de stabiliteit van de regio. Dit wordt versterkt door incidenten in vitale sectoren zoals de logistiek, telecom en overheid, waarbij ransomware, DDoS aanvallen en datalekken opvallen. Bovendien wordt de voortdurende groei van geavanceerde malware en evasietechnieken benadrukt, evenals de kwetsbaarheden in webtechnologie en industriële controlesystemen. De maatschappelijke impact van deze dreigingen, waaronder privacyrisico's en fraude, vraagt om een geïntegreerde verdediging, waarbij samenwerking tussen overheden, de private sector en internationale partners essentieel is. Het rapport benadrukt het belang van supply chain beveiliging en maatschappelijke weerbaarheid voor een veilige digitale toekomst.

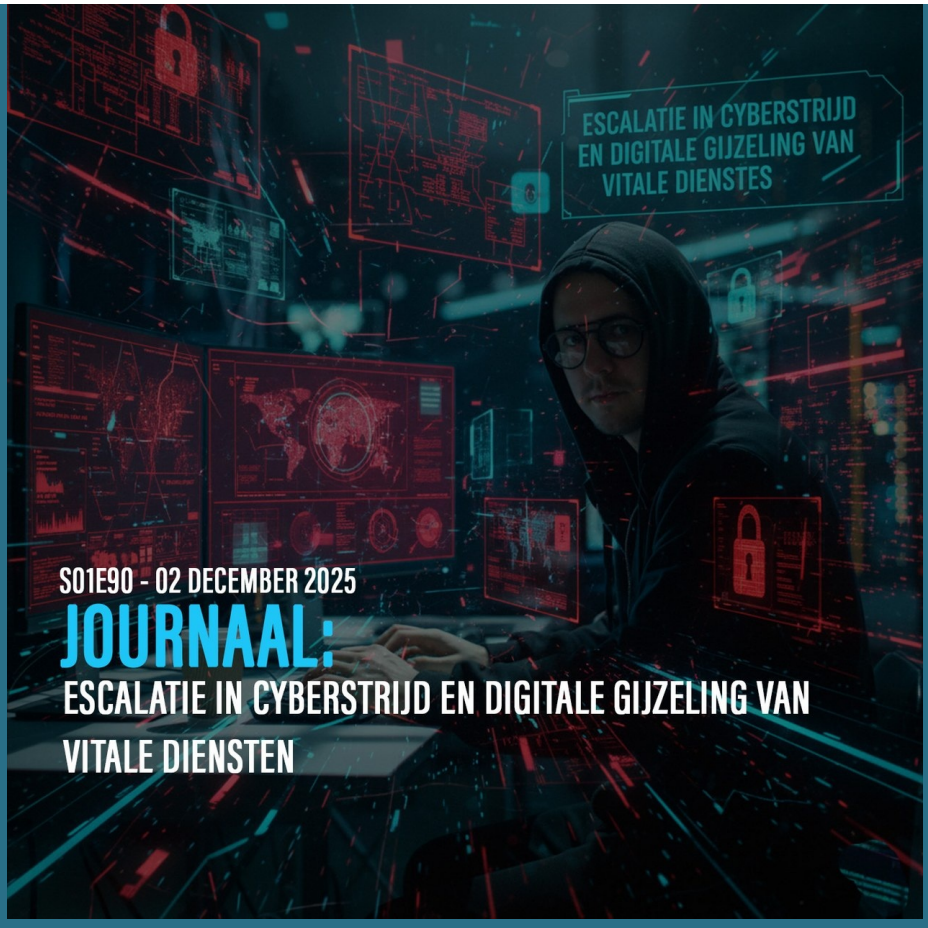
RAPPORT 49-2025



Europese offensieve cyberplannen en kritieke lekken in vitale systemen

Europa en de NAVO overwegen offensieve cyberoperaties als reactie op de hybride dreigingen vanuit Rusland, waaronder sabotage, desinformatie en GPS verstoringen. Er is een toename van exploitatie van kwetsbaarheden, zoals bij GitLab, Airbus en in software van de luchtvaartsector. In Nederland en België zijn er gerichte aanvallen op netwerken, met specifieke kwetsbaarheden in tools als Metabase en SolarWinds Serv-U. Daarnaast zijn er zorgen over de verkoop van malware tools die beveiligingssystemen kunnen uitschakelen, wat de risico's voor organisaties vergroot.

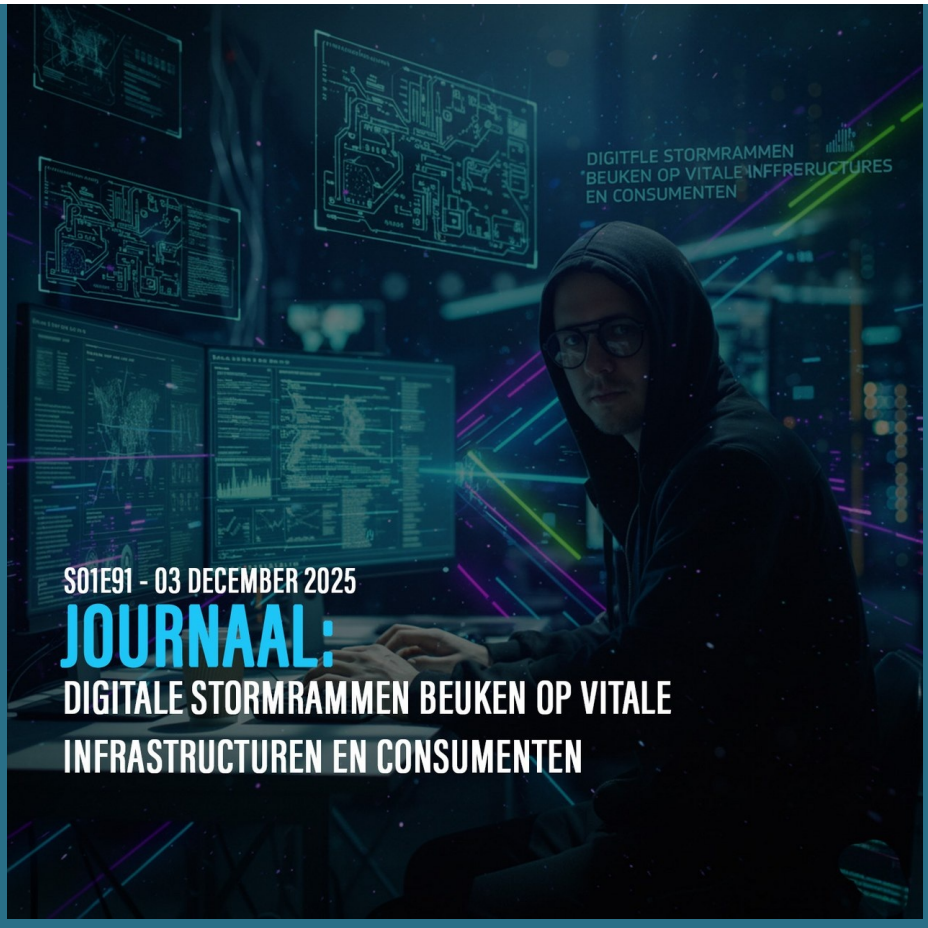
LEES VERDER



Escalatie in cyberstrijd en digitale gijzeling van vitale diensten

Recentelijke cyberaanvallen richten zich op vitale infrastructuren in de Benelux. Het Belgische postbedrijf bpost werd getroffen door Tridentlocker ransomware, wat mogelijk invloed had op de werking van hun systemen voor sortering en transport van post. Ook bij KPN in Nederland was er mogelijk een datalek, wat zorgwekkende implicaties heeft voor klantgegevens. Internationaal stelen cybercriminelen steeds grotere hoeveelheden persoonsgegevens, zoals in Zuid-Korea, waar 33 miljoen klantgegevens werden buitgemaakt. Tegelijkertijd nemen geopolitieke spanningen toe, waarbij de NAVO overweegt preventieve digitale aanvallen tegen Rusland te ondernemen.

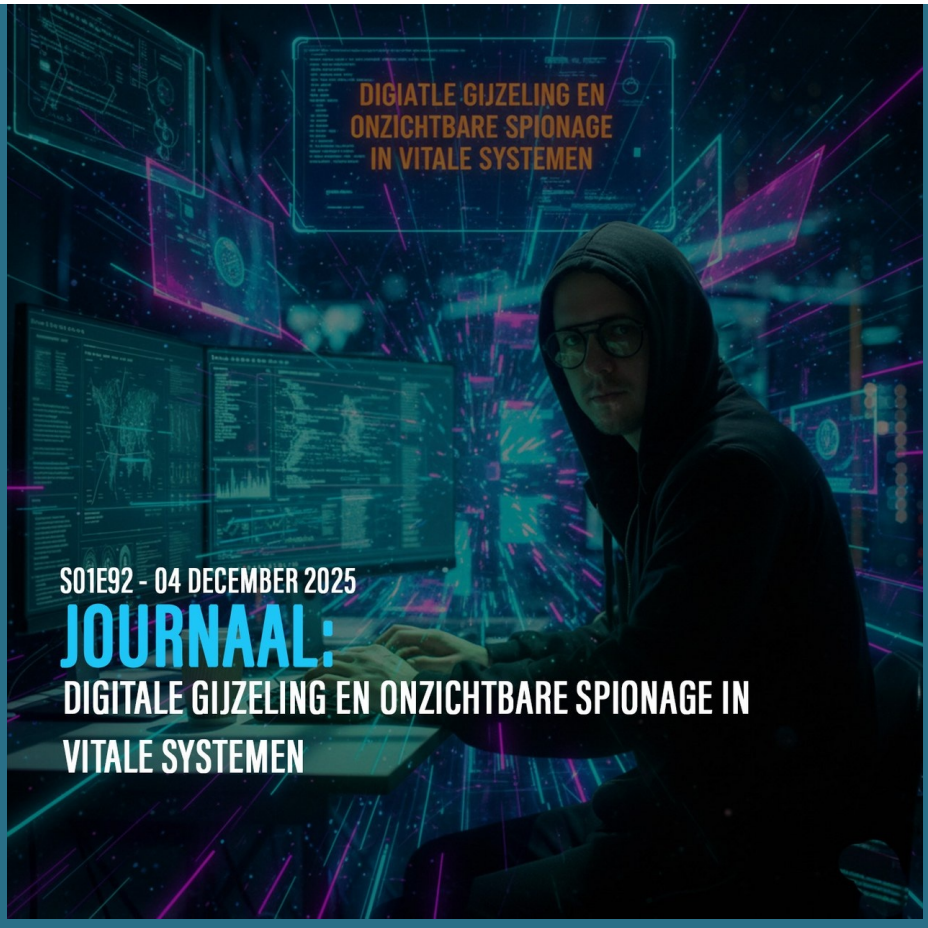
LEES VERDER



Digitale stormrammen beuken op vitale infrastructuren en consumenten

De digitale dreigingen nemen snel toe, met zowel statelijke actoren als opportunistische criminelen die nieuwe manieren vinden om systemen binnen te dringen. Er zijn meer dan 2.000 valse webshops die consumenten bestoken, terwijl hackers via malware en phishingaanvallen zakelijke netwerken proberen te compromitteren. Android- en ontwikkeltools bevatten kwetsbaarheden, terwijl nieuwe malwarefamilies zoals Arkanix en KimJongRAT zich richten op kleine bedrijven en cryptovaluta. Staatsactoren gebruiken geavanceerde spionage- en identiteitsdiefstaltechnieken, terwijl de overheid werkt aan digitale soevereiniteit met plannen voor een eigen overheidscloud.

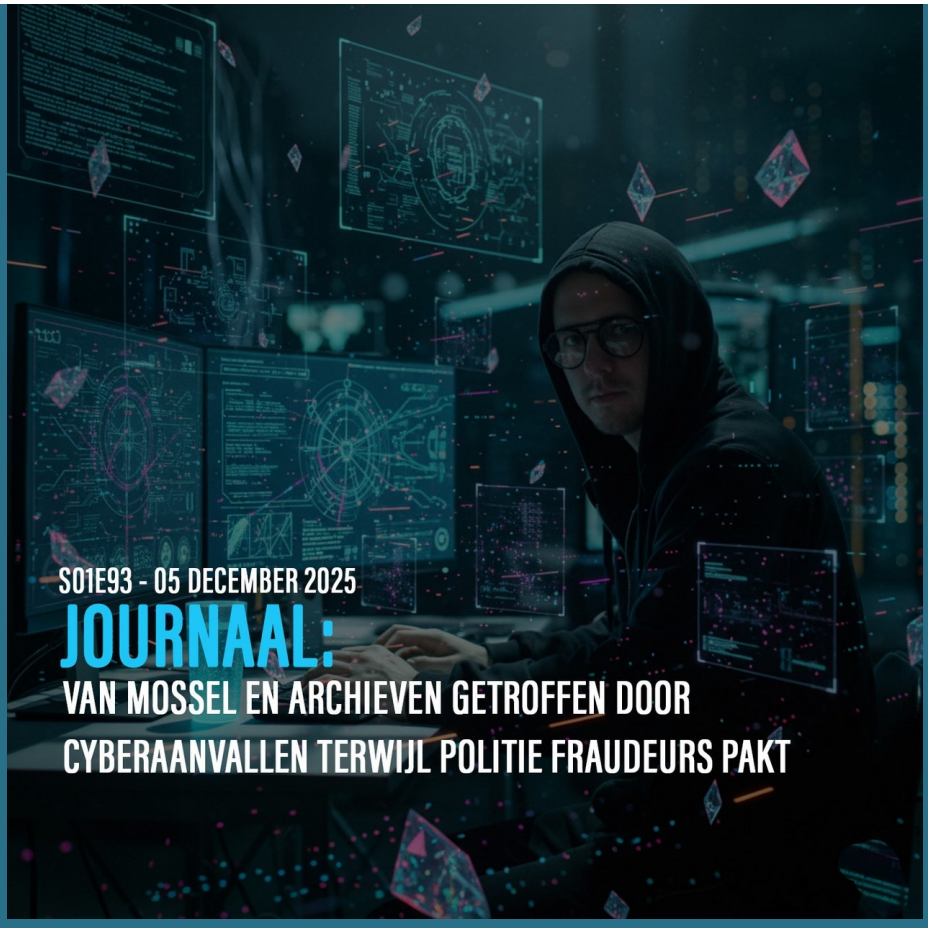
LEES VERDER



Digitale gijzeling en onzichtbare spionage in vitale systemen

Recentelijk zijn er verschillende belangrijke digitale incidenten in Nederland en België geweest, waaronder een ransomware aanval op Bpost, waarbij 30GB aan gegevens werd buitgemaakt, en een grote storing bij telecomprovider Odido, die interne netwerkproblemen veroorzaakte. Wereldwijd was er ook een significante verstoring van ChatGPT diensten. Beveiligingslekken in populaire plugins zoals WordPress en Notepad++ bedreigen websites, terwijl IoT apparaten zoals dashcams kwetsbaar blijken voor overname via onveilige verbindingen. Geavanceerde malware zoals Shai-Hulud 2.0 en Water Saci blijft ook circuleren.

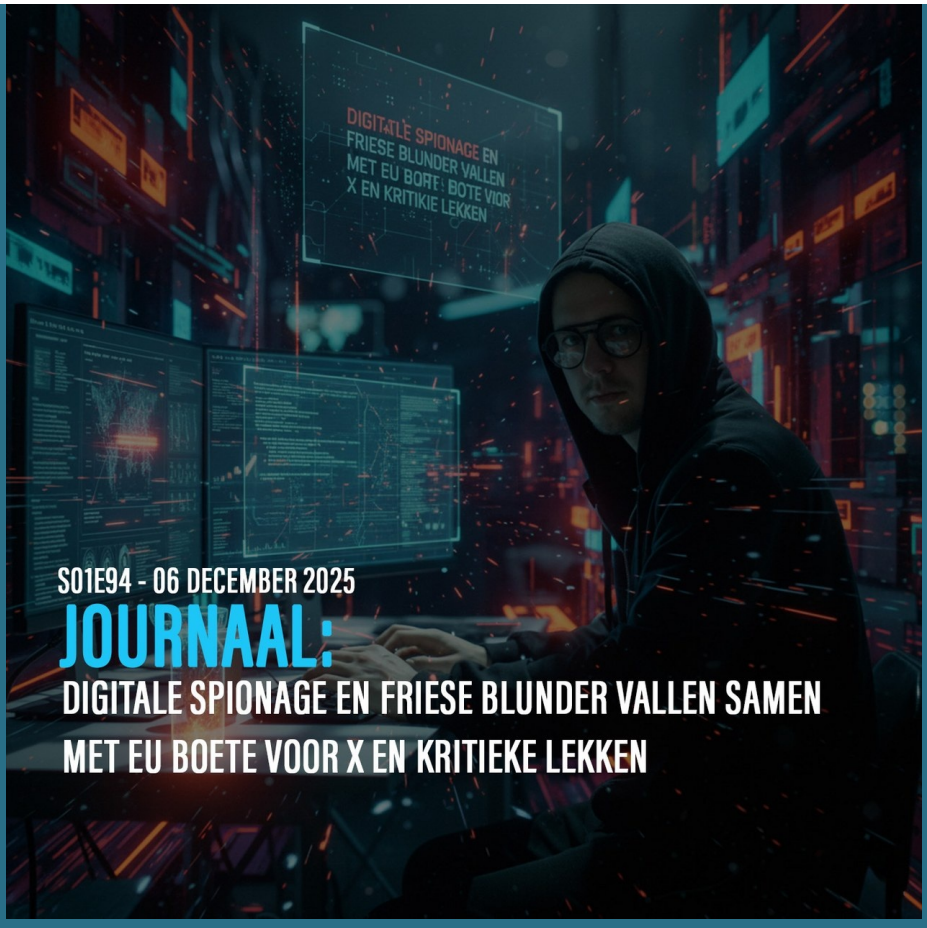
LEES VERDER



Van Mossel en archieven getroffen door cyberaanvallen terwijl politie fraudeurs pakt

Van Mossel, de grootste dealerholding van Nederland, werd getroffen door een cyberaanval waarbij drie van hun servers werden geïnfecteerd. Onbevoegden kregen toegang tot hun infrastructuur, maar het is nog onzeker of er gevoelige gegevens zijn gestolen. Tegelijkertijd werd de website van de Belgische Staatsarchieven verstoord door een DDoS aanval van BD Anonymous, wat de toegang tot belangrijke documenten tijdelijk blokkeerde. Dit komt te midden van diverse kwetsbaarheden in software en industriële systemen die actief worden misbruikt door cybercriminelen.

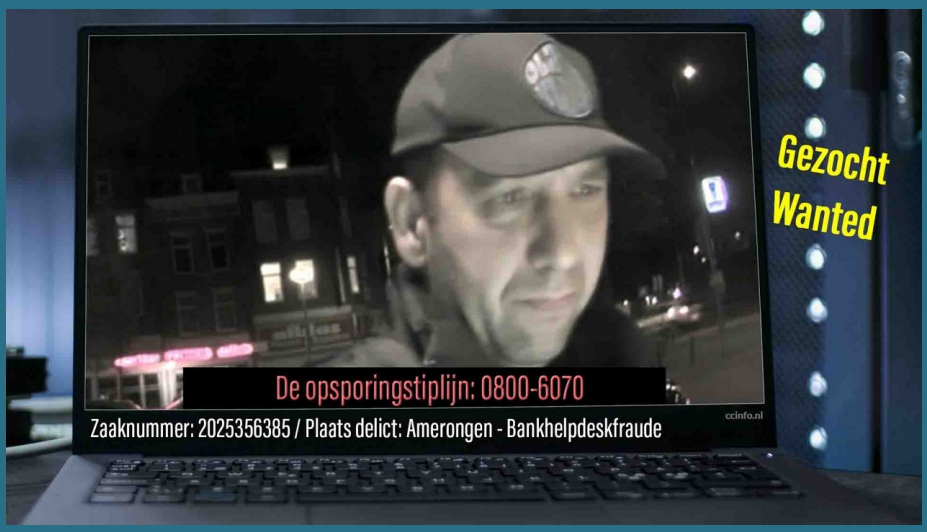
LEES VERDER



Digitale spionage en Friese blunder vallen samen met EU boete voor X en kritieke lekken

Het digitale landschap wordt bedreigd door zowel menselijke fouten als geavanceerde cyberaanvallen. Een e-mailfout in Dantumadiel leidde tot een privacyblunder, terwijl ransomware aanvallen de farmaceutische sector troffen. Kwetsbaarheden in Apache Tika en Array Networks vpn apparaten vormen serieuze risico's voor systeembeheerders. Daarnaast verspreidt malware via verschillende aanvalsvectoren zoals de Rust en USB drives. De EU heeft een boete opgelegd aan X voor desinformatie, terwijl Russische hackers zich richten op diplomaten via phishing. Geopolitieke instabiliteit vergroot de dreiging van cybercriminaliteit.

LEES VERDER



Amerongen - Bankhelpdeskfraude

In Amerongen werd een blinde vrouw twee keer slachtoffer van bankhelpdeskfraude. De oplichters deden zich eerst voor als politieagenten die haar eerdere oplichting kwamen onderzoeken. Ze maakten gebruik van de kwetsbaarheid van het slachtoffer, die vanwege haar blindheid geen

telefoonnummers kon verifiëren. Het incident toont hoe criminelen de kwetsbaarheid van mensen misbruiken en maakt duidelijk dat georganiseerde misdaad steeds meer gebruik maakt van 'Fraud-as-a-Service'. Dit benadrukt de noodzaak van waakzaamheid en het beschermen van kwetsbare personen tegen dergelijke tactieken.

LEES VERDER

Luister naar de discussiepodcast over het nieuws van de afgelopen week.

Luister de podcast nu op Youtube

Luister de podcast nu op Spotify

Meer leren over cybercrime? Ontdek de verschillende vormen en begrippen

In de Cybercrimeinfo Bibliotheek vind je een uitgebreide verzameling van termen en verschillende vormen van cybercriminaliteit. Van phishing en malware tot ransomware en andere digitale dreigingen, we leggen elke vorm duidelijk uit. Zo krijg je inzicht in wat deze aanvallen inhouden, hoe ze werken en welke risico's ze met zich meebrengen.

Of je nu op zoek bent naar uitleg over specifieke cybercrime termen of meer wilt leren over de verschillende soorten digitale bedreigingen, onze bibliotheek biedt de kennis die je nodig hebt om jezelf beter te beschermen.

Verdiep je in de wereld van cybercrime en vergroot je digitale weerbaarheid.

BEKIJK DE BIBLIOTHEEK

Beantwoorde vragen en tips voor digitale weerbaarheid

Op deze pagina vind je antwoorden op veelgestelde vragen, nuttige tips en praktische hulpmiddelen om je digitale veiligheid te verbeteren. Of je nu meer wilt weten over bescherming tegen cyberdreigingen of jezelf beter wilt wapenen tegen online gevaren, wij bieden de informatie die je nodig hebt.

BEKIJK DE TIPS

Veelgestelde vragen over digitale veiligheid en cybercrime

Op Cybercrimeinfo vind je antwoorden op de meest gestelde vragen over cybersecurity en cybercrime. Leer hoe je jezelf en je organisatie kunt beschermen tegen digitale dreigingen, van phishing en malware tot ransomware en DDoS-aanvallen. We bieden duidelijke uitleg en praktische tips om je digitale veiligheid te versterken.

ONTDEK DE ANTWOORDEN

Vergroot je kennis en vaardigheden

Wil je je kennis over cybersecurity en het darkweb uitbreiden? Bij de Leerplek van Cybercrimeinfo vind je een breed aanbod van cursussen, tutorials en quizzen die je helpen up-to-date te blijven met de nieuwste technieken en dreigingen. Of je nu net begint of al een expert bent, onze interactieve leeromgeving biedt de uitdaging die je nodig hebt om jezelf verder te ontwikkelen.
Test je kennis met uitdagende quizzen en verdien toegang tot de exclusieve Perfecte Score Club. Voor opsporingsambtenaren bieden we binnenkort speciaal op maat gemaakte quizzen aan.

TEST JE KENNIS

Contact met Cybercrimeinfo

Heb je een vraag of probleem? Vul het formulier in en stel je vraag. We reageren zo snel mogelijk, maar houd er rekening mee dat het door de hoge aantallen vragen soms enkele dagen kan duren.

STEL JE VRAAG

Steun Cybercrimeinfo en help de strijd tegen cybercriminaliteit

Elke dag zetten wij ons in om je op de hoogte te houden van de laatste cyberdreigingen en trends. Onze missie is om jou en anderen te beschermen tegen de groeiende risico's in de digitale wereld. Maar we kunnen dit niet alleen. Jouw steun maakt het verschil.
Door te doneren help je ons waardevolle informatie te blijven leveren, nieuwe tools te ontwikkelen en de bewustwording over cybercriminaliteit te vergroten. Elke bijdrage, groot of klein, draagt bij aan de bescherming van digitale veiligheid.
Wil je ons steunen?

Samen maken we de online wereld een stukje veiliger.
Bedankt voor je steun!

❤ STEUN ONS NU

Dagelijks cyber journaal van Cybercrimeinfo

Het Dagelijks Cyber Journaal biedt dagelijkse updates over de belangrijkste cyberdreigingen en incidenten in België en Nederland. Dit is bedoeld voor mensen die de ontwikkelingen in cybercrime willen volgen, maar geen tijd hebben om alles bij te houden. Het biedt een efficiënte manier om snel up-to-date te blijven zonder uren te spenderen aan het zoeken naar relevante informatie. De updates zijn beschikbaar in zowel tekst als via een dagelijkse podcast op Spotify en YouTube.

Ontvang dagelijks het cyber journaal tussen 12:00 en 14:00 (behalve zondag).
Schrijf je in en ontvang het automatisch in je mailbox.

E-mailadres *

Voornaam

Achternaam

Inschrijven

Inschrijven

Ontvang dagelijks het cyber journaal tussen 12:00 en 14:00 (behalve zondag). Schrijf je in en ontvang het automatisch in je mailbox.

INSCHRIJVEN

Share Tweet Share Pinterest Bluesky Mastodon

Deze e-mail is verstuurd aan {{email}}.
Als u geen nieuwsbrief meer wilt ontvangen, kunt u zich hier afmelden.
U kunt ook uw gegevens inzien en wijzigen.
Voor een goede ontvangst voegt u info@cybercrimeinfo.nl toe aan uw adresboek.