Cybercrimeinfo

"Omdat wat waardevol is, beschermd moet worden"

NB384

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

Luister de podcast nu op Youtube

Luister de podcast nu op Spotify

Vraag van de week: Ben jij getroffen door het datalek bij Bevolkingsonderzoek Nederland, wat nu?

De afgelopen week kreeg ik veel vragen van slachtoffers van het datalek bij Bevolkingsonderzoek Nederland. Daarom heb ik een artikel geschreven waarin ik de belangrijkste vragen beantwoord.

In juli 2025 werd Bevolkingsonderzoek Nederland slachtoffer van een omvangrijke cyberaanval, waarbij een ransomwaregroep genaamd Nova toegang kreeg tot gevoelige gegevens van duizenden patiënten. Het datalek werd pas in september 2025 openbaar gemaakt, wat betekende dat de getroffen personen enkele maanden in onzekerheid verkeerden. Wat betekent dit voor hen, wat zijn de risico's

van zo'n datalek, en wat kunnen zij doen om zichzelf te beschermen? Dit artikel onderzoekt de ernst van het datalek, de implicaties van gestolen gegevens, en geeft praktische adviezen over wat getroffen personen kunnen doen om verdere schade te voorkomen.

Lees verder

Beëindiging Windows 10 ondersteuning, AI gedreven malware, VoidProxy phishing en export censuurtechnologieën

De beëindiging van de ondersteuning voor Windows 10 door Microsoft in oktober 2025 vergroot de kans op cyberaanvallen, omdat oudere systemen kwetsbaar worden zonder beveiligingsupdates. Nieuwe malwarecampagnes, waaronder die van EvilAI en VoidProxy, gebruiken kunstmatige intelligentie en geavanceerde phishingtechnieken om gegevens te stelen, zelfs via multi-factor authenticatie. Hacktivistische groepen breiden hun invloed uit door samenwerkingen en grotere aanvallen, terwijl China censuurtechnologieën exporteert, wat de digitale rechten wereldwijd bedreigt. Deze ontwikkelingen verhogen de complexiteit van digitale dreigingen en vereisen voortdurende waakzaamheid.

Lees verder

Ransomware treft Venlogistics en CAS EXhibition DDoS aanvallen verstoren overheid kwetsbaarheden in LangChainGo en Microsoft

Ransomware heeft verschillende bedrijven getroffen, waaronder Venlogistics Nederland en CAS EXhibition Partners, die beide werden verstoord door aanvallen van respectievelijk de Incransom en Lynx ransomwaregroepen. In België werd Volumex Lease getroffen door de Radar ransomware. Daarnaast werd de Rijksoverheid Nederland getroffen door een langdurige DDoS-aanval, die de werkbaarheid van duizenden ambtenaren verstoorde. Tevens werden kwetsbaarheden ontdekt in software zoals CUPS, LangChainGo en Microsoft, wat het risico op cyberaanvallen vergroot. Geopolitieke spanningen leidden tot aanvallen door de pro-Russische groep SectorJ149, die kritieke infrastructuren in Zuid-Korea en Oekraïne aanviel.

Lees verder

Ransomware in scheepsbouw en meubels en nieuwe dreigingen uit geopolitieke spanningen vergroten cyberrisico’s

Op 16 september 2025 werden de Nederlandse bedrijven Ferus Smit en Jansen Furniture getroffen door ransomware-aanvallen. Ferus Smit, een scheepsbouwbedrijf, werd aangevallen door de Warlock groep, terwijl Jansen Furniture, een meubelproducent, werd aangevallen door Imncrew. Beide bedrijven hadden moeite om hun systemen te herstellen na de diefstal van gegevens. Daarnaast werden er kwetsbaarheden ontdekt in veelgebruikte software, waaronder Microsoft Exchange en WordPress, die bedrijven oproepen om hun systemen bij te werken. Nieuwe dreigingen, zoals de Coinbase Cartel en APT28, vergroten de cyberrisico's wereldwijd. Geopolitieke spanningen spelen een steeds grotere rol in cyberaanvallen.

Lees verder

Vurbis en Kering getroffen door datalekken en kwetsbaarheden in WatchGuard en Linux verhogen wereldwijde dreigingen

Vurbis en Kering zijn recent getroffen door datalekken waarbij persoonlijke gegevens van gebruikers zijn blootgesteld. Vurbis, een IT-dienstverlener uit Nederland, heeft gegevens zoals e-mailadressen en telefoonnummers verloren, die nu te koop worden aangeboden. Ook de Franse modegigant Kering, bekend van merken zoals Gucci en Balenciaga, werd getroffen, waarbij gegevens van miljoenen klanten werden gestolen door de hacker Shiny Hunters. Daarnaast zijn kwetsbaarheden ontdekt in WatchGuard Fireware OS en de Linux Kernel, wat de cyberrisico's wereldwijd verhoogt. Bedrijven worden aangespoord om deze beveiligingslekken snel te verhelpen.

Lees verder

Beveiligingsproblemen bij grote diensten bedreigen jouw privacy en veiligheid

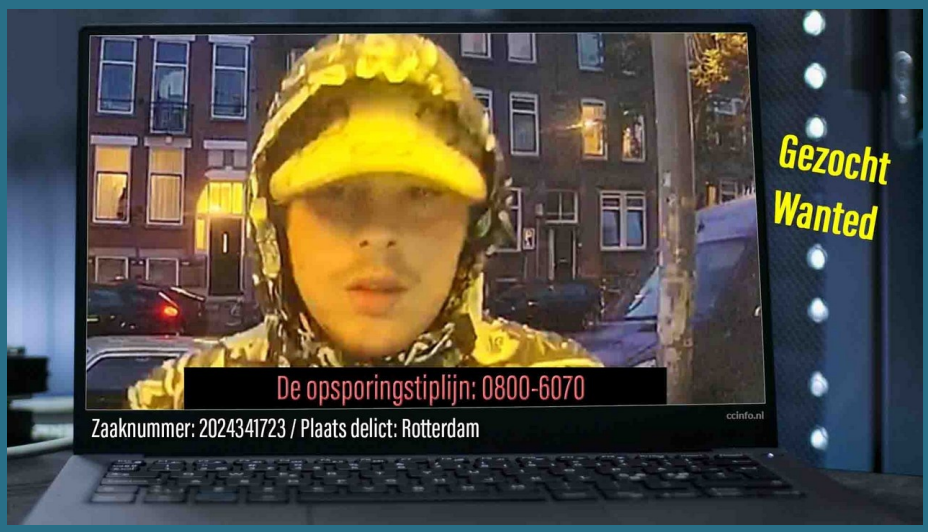
Beveiligingsproblemen in grote diensten vormen een aanzienlijke bedreiging voor de privacy en veiligheid van gebruikers. SonicWall, een beveiligingssoftwareleverancier, werd getroffen door een hack waarbij belangrijke configuratiebestanden werden gestolen. PureVPN had een lek waardoor gebruikers' IP-adressen zichtbaar werden bij verbroken verbindingen. Ook werd een kwetsbaarheid in Google Chrome ontdekt die aanvallers in staat stelde kwaadaardige code uit te voeren. Daarnaast verspreidde nieuwe ransomware zich specifiek gericht op virtuele omgevingen, en werd een Trojan ontdekt die gegevens steelt via vervalste softwarepakketten. Bedrijven en gebruikers worden aangespoord hun beveiliging te versterken en snel software-updates door te voeren.

Lees verder

Russische hackgroepen en AI phishing bedreigen de veiligheid van bedrijven, overheden en burgers

Russische hackgroepen en AI-gestuurde phishing vormen een groeiende dreiging voor bedrijven, overheden en burgers wereldwijd. De samenwerking tussen de Russische groepen Gamaredon en Turla heeft geleid tot cyberespionage, waarbij Kazuar-malware wordt ingezet tegen Oekraïense doelwitten, maar ook wereldwijd gevolgen heeft. Daarnaast is er een toename van phishing-aanvallen en datalekken, zoals het incident in Spanje, waar persoonlijke gegevens van politici werden blootgesteld. AI maakt phishing-aanvallen effectiever, waardoor traditionele beveiligingssystemen moeite hebben deze te detecteren.

Lees verder



Bankfraude via telefoon en koerier: Oplichting met pinpas bij Geldmaat Rotterdam

Op 11 oktober 2024 werd een man uit Ooltgensplaat slachtoffer van bankfraude in Rotterdam. Hij ontving een telefoontje van een vrouw die zich als ING-medewerker voordeed. Ze beweerde dat er cybercriminelen bezig waren met zijn rekening en

vroeg hem om zijn pinpas, pincodes en contant geld in een envelop te stoppen voor de veiligheid. Een koerier zou de spullen ophalen. Later werd er met de pinpas gepind bij een Geldmaat-automaat in Rotterdam. De politie is op zoek naar de dader.

Lees verder

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