Cybercrimeinfo

"Omdat wat waardevol is, beschermd moet worden"

Nieuwsbrief 394

Ben jij klaar voor de harde realiteit van Week 48-2025?

De grens tussen de digitale en de fysieke wereld vervaagt steeds meer, en dat is deze week pijnlijk duidelijk geworden. Ben jij op de hoogte van wat er gebeurde boven vliegbasis Volkel en waarom Defensie zich genoodzaakt zag om in te grijpen? Weet jij waarom het kabinet zich zorgen maakt over de veiligheid van jouw DigiD gegevens bij de mogelijke overname van Solvinity?
Deze week gaat verder dan alleen datalekken. We zagen hoe 3,5 miljard accounts uit WhatsApp werden getrokken en hoe een kritiek lek in Oracle met een score van 9.8 de deuren wagenwijd openzette voor hackers. Maar de dreiging is ook tastbaar: van fysieke ontvoeringen van cryptobezitters in Nederland tot een miljoeneninvestering van Rusland om verkiezingen in Moldavië te beïnvloeden.
Denk jij dat je veilig bent? Uit recent onderzoek blijkt dat slechts 10% van de Nederlanders online oplichting foutloos weet te herkennen. Test of jij bij die 10% hoort en of je weet waarom de Franse overheid je plotseling afraadt om biometrische ontgrendeling te gebruiken.
Doe de Wekelijkse Digitale Weerbaarheid Quiz en ontdek of jouw kennis up to date is in een wereld vol spionage, kritieke kwetsbaarheden en digitale oorlogvoering.

QUIZ 48-2025

Strategisch Dreigingsrapport Cyberveiligheid week 48-2025

Het strategisch dreigingsrapport voor week 48 van 2025 analyseert de toenemende overlap tussen geopolitiek en cyberdreigingen. Statelijke actoren spelen een centrale rol in cyberaanvallen, waarbij ze zowel economische sabotage als politieke destabilisatie beogen. Landen als Rusland, Noord-Korea en Iran zetten cybercapaciteiten in om westerse democratieën te ondermijnen, terwijl China zijn digitale spionagecapaciteiten uitbreidt. Het rapport benadrukt ook de kwetsbaarheid van digitale toeleveringsketens en kerninfrastructuren, en de gevaren van kunstmatige intelligentie, die zowel als wapen als kwetsbaarheid fungeert. Daarnaast wordt de vervaging van de grens tussen digitale en fysieke dreigingen besproken, wat leidt tot nieuwe veiligheidsrisico's voor zowel de samenleving als de economie. Het rapport sluit af met strategische aanbevelingen voor beleidsmakers om een adaptieve en geïntegreerde veiligheidsstrategie te ontwikkelen.

Rapport 48-2025

Digitale soevereiniteit onder druk door spionage,

drones bij Volkel en miljarden gegevenslekken

Een grootschalig datalek bij Iberia en een ernstig incident bij WhatsApp tonen de risico's van toeleveringsketens en onbeveiligde interfaces. Ook wordt er gewaarschuwd voor actief misbruik van kritieke softwarefouten in diverse systemen. Spionageactiviteiten, waaronder digitale misleiding en menselijke infiltratie, vormen steeds grotere dreigingen, met China als belangrijke speler. Daarnaast zijn er zorgen over de beveiliging van militaire objecten na drones boven Volkel en de geopolitieke inzet van cybercapaciteiten in de 'grijze zone'. Tegelijkertijd worden privacywetgeving en digitale soevereiniteit onder druk gezet.

LEES VERDER

Geopolitieke spanningen en blockchainmisbruik domineren het digitale speelveld

Geopolitieke spanningen en blockchainmisbruik bepalen momenteel het digitale landschap. Er zijn steeds meer meldingen van fysiek geweld tegen cryptobezitters, waarbij criminelen valse belastingformulieren gebruiken om persoonlijke gegevens te stelen. Ook zijn er grote datalekken bij financiële instellingen en een datadiefstal via Mailchimp. Daarnaast worden kritieke softwarelekken ontdekt in cloudinfrastructuren en softwareketens, wat de veiligheid van systemen bedreigt. Cybercriminelen maken gebruik van geavanceerde technieken, zoals EtherHiding op de Binance Smart Chain, om malware via blockchain te verspreiden en te updaten.

LEES VERDER

Hybride oorlogsvoering en geraffineerde bankfraude domineren het digitale landschap

Het digitale landschap wordt steeds complexer, met hybride oorlogsvoering en geavanceerde bankfraude die een prominente rol spelen. Russische actoren investeren miljoenen in cyberaanvallen en desinformatiecampagnes, terwijl criminelen zich richten op bankrekeningfraude via phishing en accountovernames. De financiële schade door deze methoden is al enorm. Daarnaast worden er ernstige kwetsbaarheden ontdekt, zoals in ftp-software en online codeformatters, die de veiligheid van systemen wereldwijd bedreigen. Ook de dreiging van spyware via chatapps en gerichte malware-aanvallen op creatieve professionals neemt toe.

LEES VERDER

Digitale sabotage door staatshackers en listige manipulatie van consumenten

Het digitale landschap wordt gekenmerkt door steeds geavanceerdere dreigingen. Noord-Koreaanse en Russische hackers richten zich op vitale infrastructuren en bedrijven, terwijl criminelen oplichterspraktijken zoals phishing en malwareverspreiding toepassen. Phishing-aanvallen richten zich onder andere op consumenten van Albert Heijn, terwijl softwareontwikkelaars misleid worden via een schadelijke extensie in de Visual Studio Code Marketplace. Kritieke kwetsbaarheden in routers en bedrijfsnetwerken blijven een groot probleem. De grenzen tussen fysieke en digitale criminaliteit vervagen, met steeds complexere vormen van cybercriminaliteit en de inzet van kunstmatige intelligentie.

LEES VERDER

Digitale infrastructuur onder vuur door ketenproblemen en misleiding

Digitale infrastructuren worden steeds vaker getroffen door ketenproblemen en misleidende praktijken, waarbij zowel publieke als private sectoren het doelwit zijn. Aanvallen op externe dienstverleners hebben geleid tot verstoringen in IT-systemen en datalekken, zoals bij telecombedrijven en grote bedrijven als Asahi. Verder komen er kritieke softwarekwetsbaarheden aan het licht, waaronder bij OpenAI en het gebruik van gevaarlijke malware in populaire games. Ook fraude en onveilige handel blijven toenemen, wat de weerbaarheid van de digitale infrastructuur verder onder druk zet.

LEES VERDER

Digitale destabilisatie door statelijke allianties en geavanceerde fraude

De digitale dreigingen blijven zich snel ontwikkelen, met een toenemende samenwerking tussen statelijke hackergroepen en de inzet van geavanceerde fraude. Zo werd de Zuid-Koreaanse cryptobeurs Upbit slachtoffer van een diefstal van 30 miljoen dollar, vermoedelijk uitgevoerd door de Lazarus groep. Ook werden verouderde scripts en kwetsbaarheden in systemen ontdekt, zoals een exploit voor iOS en een zero-click aanval. Geopolitieke spanningen leiden tot een intensivering van cyberaanvallen, met Rusland en Noord-Korea die hun krachten bundelen. Cybercriminelen maken steeds vaker gebruik van AI en misbruik van populaire platforms.

LEES VERDER

Sprundel / Etten-Leur - Bankhelpdeskfraude

In Etten-Leur werd een vrouw van in de tachtig het slachtoffer van bankhelpdeskfraude. Ze werd telefonisch benaderd door oplichters die zich voordeden als bankmedewerkers en haar vertrouwden met valse verhalen over

verdachte transacties. Na haar bankpassen en codes op hun verzoek in een envelop te stoppen, werd er een koerier naar haar huis gestuurd om de envelop op te halen. Later werd er met de gestolen pas geld opgenomen. De politie zoekt de verdachte die het geld heeft gepind.

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.