Cybercrimeinfo

"Omdat wat waardevol is, beschermd moet worden"

Nieuwsbrief 399

De wekelijkse digitale weerbaarheid quiz: Week 01-2026

Welkom bij de eerste update van 2026. Het nieuwe jaar is direct van start gegaan met significante incidenten en een evolutie in aanvalstechnieken. Terwijl BD Anonymous op oudejaarsavond de Belgische CPH Bank platlegde, werden in New York tijdens de inauguratie specifieke hardware tools zoals de Flipper Zero preventief verboden.

Op technisch vlak zien we een zorgwekkende verschuiving. Met PromptLock is de eerste ransomware geïdentificeerd die generatieve AI gebruikt voor dynamische scripts, en de tool VOID KILLER opereert inmiddels op kernelniveau (Ring 0) om EDR-systemen uit te schakelen. Daarnaast vragen kritieke kwetsbaarheden in SmarterMail (CVSS 10.0) en IBM API Connect (CVSS 9.8) om onmiddellijke aandacht van beheerders.

Bent u daarnaast op de hoogte van de Kamervragen over Chinese Kaifa sensoren, de miljoenschikking van Disney en de nieuwe OWASP Agentic AI risico's?

Toets uw kennis van de actuele stand van zaken in de Wekelijkse Digitale Weerbaarheid Quiz: Week 01-2026.

QUIZ 01-2026

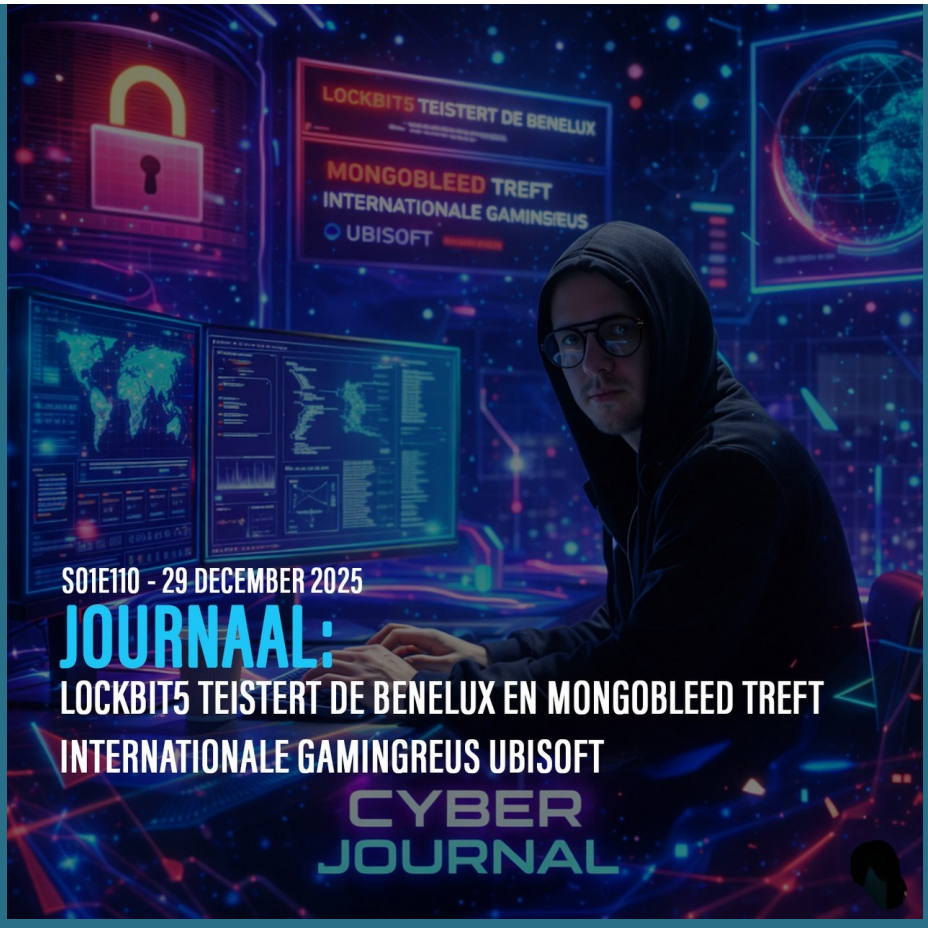
Strategisch dreigingsrapport cyberveiligheid week 01-2026

Het dreigingslandschap kenmerkt zich begin 2026 door een fundamentele verschuiving waarbij de grenzen tussen de digitale en fysieke wereld in hoog tempo vervagen. Deze transitie zorgt voor een complexe veiligheidssituatie waarin criminele netwerken en geopolitieke belangen steeds meer met elkaar verweven raken. Het traditionele onderscheid tussen vrede en oorlog maakt plaats voor structurele onzekerheid, wat vraagt om een strategie die verder reikt dan uitsluitend technische beveiliging.

Op geopolitiek vlak vormt Rusland een prominente dreiging door de inzet van hybride strategieën die digitale aanvallen combineren met desinformatie en economische druk. Inlichtingendiensten waarschuwen voor voorbereidingshandelingen gericht op sabotage van vitale infrastructuur in de Noordzee, waarbij zelfs lokale jongeren worden gerekruteerd voor fysieke verkenningen. China concentreert zich daarentegen op hoogwaardige spionage via geavanceerde malware die diep in systemen doordringt en detectie langdurig weet te ontwijken. Iran hanteert een tactiek van gerichte inlichtingenoperaties en psychologische druk op specifieke personen binnen de defensie- en veiligheidssector.

De georganiseerde cybercriminaliteit heeft zich ondertussen ontwikkeld tot een professionele industrie met een bedrijfsmatige aanpak. Ransomware blijft een groot risico voor de bedrijfscontinuïteit, waarbij groeperingen steeds vaker dreigen met het publiceren van gestolen data als drukmiddel. Aanvallen via phishing en social engineering worden geraffineerder doordat criminelen misbruik maken van legitieme infrastructuur van vertrouwde diensten, zich specifiek richten op de cryptosector of zich via sms en telefoon voordoen als overheidsinstanties. Tot slot vormt de compromittering van de toeleveringsketen een groot strategisch gevaar, omdat aanvallers via één besmette softwareleverancier direct toegang kunnen krijgen tot grote aantallen slachtoffers.

RAPPORT 01-2026



Lockbit5 teistert de Benelux en MongoBleed treft internationale gamingreus Ubisoft

Een golf van cyberaanvallen teistert de Benelux, waarbij ransomwarebende Lockbit5 diverse lokale bedrijven en instellingen heeft getroffen. Internationaal zorgt het kritieke MongoBleed lek voor grote problemen, waaronder bij gamingreus Ubisoft. Naast deze technische kwetsbaarheden kampen multinationals met grootschalige datadiefstal en misbruiken criminelen legitieme infrastructuur voor fraude. Opvallend is ook de inzet van een Nederlandse tiener voor spionage en de toenemende dreiging van hybride oorlogsvoering, waarbij geopolitieke spanningen zich vertalen naar het digitale domein.

LEES VERDER

Internationale cyberdreiging door AI aanvallen en datalekken in kritieke systemen

De internationale digitale veiligheid staat onder druk door een toename van complexe AI gestuurde aanvallen en ernstige datalekken. Recente incidenten tonen de kwetsbaarheid van kritieke infrastructuur, zoals de Roemeense energiesector en diverse overheidsinstanties. Grote hoeveelheden gevoelige informatie, waaronder inloggegevens van WordPress sites en klantgegevens van e-commercegiganten, liggen op straat. Daarnaast vormen technische zwakheden in software zoals MongoDB en firmware van netwerkapparatuur wereldwijd een groot risico voor grootschalige spionage en ongeautoriseerde toegang tot systemen.

LEES VERDER

Belgische CPH Bank doelwit van DDoS en Chinese slimme meters onder vergrootglas in Nederland

Een agressieve toename van cyberaanvallen en sabotage raakt vitale sectoren wereldwijd. De Belgische CPH Bank kampte met een zware DDoS aanval, terwijl in de cryptowereld miljoenen werden buitgemaakt via geavanceerde hacks. Tegelijkertijd vormen kritieke softwarelekken bij IBM en nieuwe AI gestuurde malware ernstige risico's. In Nederland zijn politieke zorgen gerezen over de veiligheid van slimme energiemeters met Chinese onderdelen vanwege mogelijke spionage. Ook illegale handel in hardware en privacyschendingen blijven het digitale landschap domineren.

LEES VERDER

Sint Annaland / Tholen - Nepagent

Twee mannen die zich voordeden als politieagenten hebben in Sint Annaland een vrouw beroofd via een babbeltruc. De oplichters belden het slachtoffer eerst met een waarschuwing over inbrekers, waarna ze haar overtuigden om waardevolle spullen af te staan voor ‘beveiliging’. De politie is op zoek naar de daders en waarschuwt burgers dringend: echte agenten zullen nooit vragen om geld of sieraden af te geven. Wees alert op deze manipulatie en vraag bij twijfel altijd om legitimatie.

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

Het Cyber Journaal

Het Cyber Journaal biedt meerdere keren per week een overzicht van de belangrijkste cyberdreigingen en incidenten in België en Nederland. Het is bedoeld voor mensen die de ontwikkelingen in cybercrime willen volgen, maar niet de tijd hebben om alle bronnen zelf bij te houden. Het journaal maakt het mogelijk om efficiënt en snel inzicht te krijgen in relevante informatie zonder langdurig te hoeven zoeken. De updates zijn beschikbaar in tekstvorm en gelijktijdig als podcast via Spotify en YouTube.

Het Cyber Journaal verschijnt meerdere keren per week, doorgaans tussen 12:00 en 14:00 uur. Schrijf je in en ontvang het automatisch in je mailbox.

E-mailadres *

Voornaam

Inschrijven

Inschrijven

Ontvang meerdere keren per week het Cyber Journaal met actuele ontwikkelingen en dreigingen in de digitale wereld. Het journaal verschijnt doorgaans tussen 12:00 en 14:00 uur en wordt automatisch per e-mail toegestuurd. Gelijktijdig verschijnt ook de bijbehorende podcast.

INSCHRIJVEN

Share Tweet Share Pinterest Bluesky Mastodon