NIEUWSBRIEF 402

"Omdat wat waardevol is, beschermd moet worden"

QUIZ

Quiz week 04-2026: Van AI gegenereerde malware tot governance vraagstukken bij de overheid

De actualiteit van week 4 in 2026 laat zien dat het dreigingslandschap zich in hoog tempo diversifieert. Aanvallers richten zich niet alleen op technische kwetsbaarheden, maar misbruiken ook legitieme infrastructuren en platformen op innovatieve wijzen.

In deze editie van de Wekelijkse Digitale Weerbaarheid Quiz toetsen we uw kennis over een aantal opvallende incidenten en trends:
Evasie-technieken: Bent u bekend met de GhostPoster-campagne die steganografie in PNG-logo's gebruikt, of de 'PixelCode'-techniek waarbij executables worden verstopt in YouTube-videoframes?
Nederlandse Belangen: We behandelen de bezwaren van Bits of Freedom omtrent de Amerikaanse Cloud Act bij de overname van Solvinity, en de kritiek van Follow the Money op de transitie van S/MIME naar TLS bij De Nederlandsche Bank.
Cloud & AI Security: Van privilege escalation binnen Google Vertex AI tot de 'VoidLink'-malware die met behulp van AI-modellen in minder dan een week werd gegenereerd.
IoT & Automotive: De succesvolle root-toegang op een Tesla tijdens Pwn2Own en de 'WhisperPair'-kwetsbaarheid die afluisteren via Bluetooth mogelijk maakt.

Deze quiz bestaat uit 20 vragen die diep ingaan op de technische specificaties (CVE's, attack vectors) en bestuurlijke risico's van de afgelopen week. Beschikt u over de actuele kennis die nodig is om deze casussen te duiden?

➤ START DE QUIZ »

RAPPORT

Dreigingsrapport Cyberveiligheid: Week 04-2026

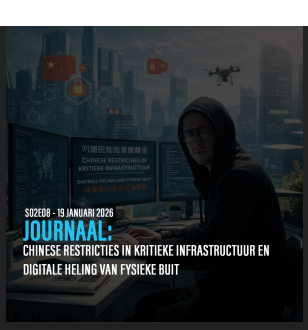
Het strategisch dreigingsrapport van week 4 uit 2026 schetst een fundamentele verschuiving in het cyberlandschap, waarbij de focus van aanvallers is verplaatst van technische exploits naar het manipuleren van vertrouwde infrastructuren en menselijke processen. De browser fungeert inmiddels als het primaire aanvalsoppervlak, wat wordt geïllustreerd door de GhostPoster campagne waarbij malafide extensies jarenlang onopgemerkt in officiële winkels verbleven. Daarnaast zetten criminelen in op methoden zoals de CrashFix techniek van de KongTuke groep, waarbij gebruikers via geënsceneerde browsercrashes en psychologische druk worden verleid om zelf schadelijke commando's uit te voeren. Ook organisatorische onderdelen zoals helpdesks vormen een zwakke plek, omdat aanvallers via social engineering en realtime phishingkits verificaties en MFA procedures weten te omzeilen. De snelle opkomst van AI en cloudtechnologie creëert tevens nieuwe risico's, zoals schaduw IT en malware die via legitieme platforms zoals YouTube wordt verspreid. Als reactie hierop adviseert het rapport striktere maatregelen, waaronder het gebruik van FIDO2 sleutels, gedragsgebaseerde detectie en het versterken van de digitale soevereiniteit om minder afhankelijk te zijn van niet Europese technologie.

➤ LEES HET RAPPORT »

CYBER JOURNAAL

Chinese restricties in kritieke infrastructuur en digitale heling van fysieke buit

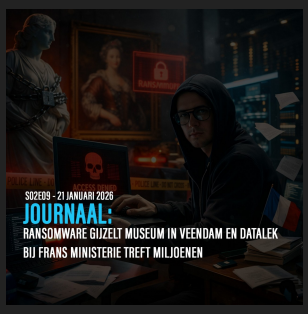
De Europese Commissie overweegt Chinese technologie uit kritieke infrastructuur te weren wegens spionagezorgen. Tegelijkertijd vervaagt de grens tussen fysieke en digitale



criminaliteit, waarbij gestolen goederen steeds vaker online worden verhandeld. Wereldwijd kampen organisaties met ernstige kwetsbaarheden in netwerkapparatuur, terwijl opsporingsdiensten successen boeken tegen een groot ransomwarekartel. Ondanks deze arrestaties blijft waakzaamheid geboden vanwege toenemende destructieve wiper-aanvallen en geavanceerde phishingmethoden die zowel bedrijven als consumenten raken.

➤ LEES HET HELE ARTIKEL »

CYBER JOURNAAL



Ransomware gijzelt museum in Veendam en datalek bij Frans ministerie treft miljoenen

Een ransomware-aanval trof het Veenkoloniaal Museum, terwijl een datalek bij een Frans ministerie miljoenen burgers raakte. In Nederland zorgde een bankstoring voor discussie over financiële vrijheid. Wereldwijd kampen organisaties met kritieke lekken in software en hardware, en opkomende AI-malware die detectie ontwijkt. Hoewel opsporingsdiensten successen boeken tegen criminele netwerken, neemt digitale sabotage in geopolitieke conflicten toe. Beleidsmakers richten zich ondertussen op digitale autonomie en het waarborgen van privacy bij nieuwe betaalmethoden.

➤ LEES HET HELE ARTIKEL »

CYBER JOURNAAL

Belgische zorg en industrie onder druk door ransomware en wereldwijde waarschuwing voor kritieke lekken in netwerksoftware

De Belgische zorg en industrie kampen met ernstige verstoringen door ransomware, waarbij ziekenhuizen offline werken en bedrijven worden afgeperst. Tegelijkertijd waarschuwen experts wereldwijd voor kritieke lekken in veelgebruikte netwerksoftware van onder meer Citrix en Cisco. Cybercriminelen gebruiken geavanceerde technieken zoals malware in video's en valse helpdeskberichten. Daarnaast nemen bankfraude en spionage door statelijke actoren toe, terwijl de discussie over digitale soevereiniteit en de kwetsbaarheid van vitale systemen oplaait.

➤ LEES HET HELE ARTIKEL »

OPSPORING

IJmuiden en Enkhuizen - Bankhelpdeskfraude

De politie is op zoek naar een vrouwelijke verdachte die verantwoordelijk is voor bankhelpdeskfraude in IJmuiden en Enkhuizen. De vrouw deed zich telefonisch voor als bankmedewerker en bezocht vervolgens oudere slachtoffers thuis om zogenaamd hun bezittingen veilig te stellen. Hierbij maakte ze op brutale wijze contant geld, bankpassen en dierbare sieraden buit, waarbij ze zelfs ringen van vingers verwijderde. De verdachte is een jonge vrouw met donker haar. Getuigen worden dringend verzocht contact op te nemen met de politie.

➤ LEES HET HELE ARTIKEL »

LUISTER & KIJK

Liever luisteren of kijken?

Geen tijd om te lezen? Blijf op de hoogte via uw favoriete platform. Kies voor de snelle update, de diepgaande analyse of de visuele presentatie.

Spotify Audio »
DAGELIJKS JOURNAAL (3 min)
DIEPTE ANALYSE (15 min)

YouTube Video »

VISUELE PRESENTATIE (5 min)

SUPPORT

Help Cybercrimeinfo in de lucht te houden

Onze tools, journalen en waarschuwingen zijn gratis voor iedereen. Maar onderzoek en hosting kosten geld. Waardeert u onze intelligence? Help ons dan met een eenmalige donatie. Elke bijdrage maakt de digitale wereld een stukje veiliger.

➤ IK WIL GRAAG STEUNEN »

Share Tweet Share Pinterest Whatsapp Bluesky Mastodon