NIEUWSBRIEF 401

"Omdat wat waardevol is, beschermd moet worden"

QUIZ

Digitale Weerbaarheid Quiz: Week 03-2026

De digitale dreiging is niet langer een “ver van mijn bed show”. Wist u dat inmiddels de helft van alle politieaangiften in Nederland betrekking heeft op digitale criminaliteit? De afgelopen week (Week 03-2026) heeft opnieuw bewezen hoe kwetsbaar onze infrastructuur en privacy zijn. Van een enorm datalek waarbij 17,5 miljoen Instagram accounts betrokken waren, tot de noodgedwongen overstap op papieren dossiers bij ziekenhuis AZ Monica na een ransomware aanval, de impact is overal voelbaar.

In deze editie van de Wekelijkse Digitale Weerbaarheid Quiz testen we of u op de hoogte bent van de nieuwste, geavanceerde aanvalsmethoden. Weet u bijvoorbeeld hoe de MacSync malware Apple’s Gatekeeper omzeilt, of waarom een Android zeroday inmiddels 1 miljoen dollar waard is op de zwarte markt? Daarnaast kijken we naar geopolitieke spanningen, zoals de inzet van het Chinese Hurricane 3000 wapensysteem en de Russische aanvallen op de Poolse energie infrastructuur.

Maar ook uw persoonlijke veiligheid staat op het spel. Weet u waarom het afplakken van gezichten met emoji's op foto's zinloos is geworden door AI, en herkent u een ‘Browser in the Browser’ phishingaanval voordat het te laat is?
Heeft u het nieuws scherp gevolgd of bent u het volgende doelwit?
Start de quiz hieronder en test uw kennis over de digitale actualiteit van deze week.

➤ START DE QUIZ »

RAPPORT

Dreigingsrapport Cyberveiligheid: Week 03-2026

Het operationele landschap van januari 2026 dwingt tot een fundamentele herziening van de nationale veiligheidsstrategie, omdat cyberoperaties zijn uitgegroeid tot primaire aanvalsvectoren die de vitale sector direct ondermijnen. De Cyber Security Raad waarschuwt voor maatschappelijke ontwrichting en acht een structurele investering van 690 miljoen euro noodzakelijk om vitale processen te beschermen tegen statelijke actoren. Een analyse van de sabotage van de Poolse energie-infrastructuur in december 2025 toont aan dat decentrale communicatieprotocollen nieuwe en kritieke kwetsbaarheden vormen.

Tegelijkertijd vindt er een geopolitieke wedloop plaats rondom Chinese kwantumtechnologie, die de huidige encryptiestandaarden onder druk zet en leidt tot een strategie waarbij data nu wordt onderschept om later te ontsleutelen. Kunstmatige intelligentie zorgt voor een verdere escalatie door malware te genereren die zich real-time aanpast, waardoor traditionele detectiemethoden tekortschieten. Deze ontwikkelingen hebben inmiddels geleid tot ernstige incidenten in de zorg, de financiële sector en de logistiek, waarbij lokale aanvallen direct regionale gevolgen hebben.

Als reactie hierop worden dwingende maatregelen geadviseerd, zoals de automatisering van security operations en een strikte inperking van AI-bevoegdheden binnen netwerken. Daarnaast is het cruciaal om het aanvalsoppervlak te verkleinen en kwetsbaarheden agressief te patchen, zodat de digitale soevereiniteit en het autonome functioneren van Nederland gewaarborgd blijven.

➤ LEES HET RAPPORT »

CYBER JOURNAAL

Wereldwijd datalek bij Instagram en Nederlandse politieactie tegen sadistische chatgroepen

Een grootschalig datalek bij Instagram heeft miljoenen gebruikersgegevens blootgelegd, terwijl in Nederland de politie succesvol optrad tegen sadistische online chatgroepen die jongeren uitbuiten. Daarnaast teisterden DDoS-aanvallen diverse Nederlandse instellingen zoals PostNL en banken. Experts waarschuwen tevens voor kritieke kwetsbaarheden in software en nieuwe geavanceerde malware die beveiligingen omzeilt. Internationale opsporingsdiensten boekten gelijktijdig resultaat tegen grootschalige fraudenetwerken, terwijl geopolitieke spanningen leiden tot aangescherpte digitale defensiestrategieën en de ontwikkeling van innovatieve wapensystemen tegen drones.

➤ LEES HET HELE ARTIKEL »

CYBER JOURNAAL

Gijzelsoftware ontregelt ziekenhuis in Antwerpen en kritiek lek in mailservers bedreigt Benelux

Een ransomware-aanval heeft het Antwerpse ziekenhuis AZ Monica platgelegd, wat leidde tot geannuleerde operaties en patiëntenstops. Daarnaast lopen Benelux-bedrijven gevaar door een kritiek lek in SmarterMail-servers. Wereldwijd kampen organisaties zoals Interrail met datalekken, terwijl Microsoft en Siemens cruciale updates uitbrengen tegen ernstige kwetsbaarheden. De digitale dreiging neemt verder toe door geavanceerde spionage, mobiele malware en fraudenetwerken, waardoor vitale sectoren en persoonsgegevens onder constante druk staan.

➤ LEES HET HELE ARTIKEL »

CYBER JOURNAAL

Antwerps ziekenhuis draait op halve kracht door ransomware en toename van fraude via Booking.com in Nederland

Het Antwerpse ziekenhuis AZ Monica is ernstig ontregeld door een ransomware-aanval, waardoor de zorgcapaciteit is gehalveerd en personeel noodgedwongen op papier werkt. Patiëntgegevens lijken vooralsnog veilig. Daarnaast waarschuwt de Fraudehelpdesk voor een explosieve toename van oplichting via Booking.com, waarbij criminelen via gehackte hotelaccounts toeslaan. Wereldwijd zorgen datalekken, kritieke softwarekwetsbaarheden en geavanceerde AI-malware voor verdere digitale onrust en oplopende geopolitieke spanningen.

➤ LEES HET HELE ARTIKEL »

OPSPORING

Apeldoorn - Phishing

Een inwoner van Apeldoorn is slachtoffer geworden van een geraffineerde phishingfraude waarbij tweeduizend euro is buitgemaakt. De criminelen gebruikten een valse e-mail en een misleidend telefoongesprek om de man een nieuwe bankpas te laten aanvragen. Vervolgens hengelde een verdachte deze pas uit de brievenbus van het slachtoffer. Dankzij een alerte getuige is er een foto van de dader beschikbaar. De politie roept mensen op die de verdachte herkennen om zich te melden.

➤ 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