Jubileumeditie: Analyses, Podcasts en weekoverzicht 02-2026.

Bekijk de webversie

NIEUWSBRIEF 400

"Omdat wat waardevol is, beschermd moet worden"

Welkom bij deze jubileumeditie. Al 400 edities lang houden we de vinger aan de pols van het digitale dreigingslandschap. Ook deze week hebben we weer de belangrijkste analyses en incidenten voor u samengevat.

QUIZ

Digitale Weerbaarheid Quiz: Week 02-2026

De start van 2026 laat zien dat het digitale dreigingslandschap diverser en intensiever is dan ooit. Terwijl Taiwan dagelijks een recordaantal van 2,63 miljoen Chinese inbraakpogingen moet pareren, zien we in Europa fysieke sabotage van het stroomnet in Berlijn door de 'Vulkangruppe'. In deze editie toetsen we uw kennis van de meest kritieke kwetsbaarheden en incidenten van de afgelopen week. Bent u volledig op de hoogte van CVE-2025-26529 in Moodle en de 'N8scape' sandbox bypass? Weet u hoe de 'ClickFix' campagne hotelmedewerkers misleidt via nagemaakte BSOD schermen, en bent u bekend met het 1:2 versleutelingspatroon van de 'CrazyHunter' ransomware? Van de bluetooth kwetsbaarheid in Whill rolstoelen tot de onthutsende 54% succesratio van AI gedreven phishing, de details doen ertoe. Zoals Stan Duijf (Hoofd Operatiën Cyber, Politie) deze week stelde, de urgentie van cybercrime is inmiddels vergelijkbaar met die van een liquidatie op straat. Beschikt u over de actuele intelligence om uw organisatie te beschermen? Start de quiz en meet uw kennis aan de hand van 20 prangende vragen.

➤ START DE QUIZ »

RAPPORT

Dreigingsrapport Cyberveiligheid: Week 02-2026

Het huidige digitale landschap wordt gekenmerkt door een versnelde evolutie van dreigingen, waarbij de professionele aanpak van cybercriminele netwerken en de inzet van kunstmatige intelligentie de boventoon voeren. De analyse van het actuele dreigingsbeeld richt zich op de toenemende geopolitieke spanningen, de industrialisatie van criminaliteit via as-a-service modellen en de strategische risico's van opkomende technologieën. Statelijke actoren uit landen zoals China en Rusland richten zich op langdurige spionage en de infiltratie van kritieke infrastructuur, waarbij zij gebruikmaken van geavanceerde malware en phishing om strategische posities te verwerven. De integratie van digitale oorlogsvoering in fysieke conflicten, zoals geïllustreerd door de uitschakeling van elektriciteitsnetten, benadrukt de kwetsbaarheid van nationale soevereiniteit in het digitale domein.

➤ LEES HET RAPPORT »

CYBER JOURNAAL

Amerikaanse sabotageclaim in Venezuela en cyberdreiging bij Belgische gemeente

De actuele analyse belicht een sterke verwevenheid tussen fysieke conflicten en cyberdreigingen. Opmerkelijk is de Amerikaanse claim over digitale sabotage van het Venezolaanse stroomnet en een kritiek lek in onderwijsplatform Moodle. Terwijl een Belgische gemeente onterecht doelwit leek van activisten, kampt de energiesector met grootschalige datadiefstal. Daarnaast waarschuwt onderzoek voor de veerkracht van criminele netwerken na arrestaties. De inzet van kunstmatige intelligentie en misleiding bij militaire operaties onderstreept de toenemende complexiteit van hybride oorlogvoering.

➤ LEES HET HELE ARTIKEL »

CYBER JOURNAAL

Nederlandse rechter fluit Meta terug en malwarecampagne teistert Europese hotels

De Nederlandse rechter heeft bepaald dat Meta de chronologische tijdlijnvoorkeur van gebruikers moet respecteren, wat een belangrijke overwinning voor digitale burgerrechten betekent. Ondertussen kampt de hotelsector met malware en vinden er grootschalige datalekken plaats bij bedrijven als Sedgwick. Experts waarschuwen voor de snelle ontwikkeling van AI-dreigingen, zoals geavanceerde phishing en het omzeilen van beveiligingsfilters. De politie benadrukt bovendien de groeiende samenwerking tussen cybercriminelen en statelijke actoren, wat vraagt om een urgentere aanpak van digitale misdaad.

➤ LEES HET HELE ARTIKEL »

CYBER JOURNAAL

Sabotage stroomnet Berlijn en datalekclaim bij ASML in Nederland

Het digitale domein wordt geteisterd door sabotage, spionage en storingen. In Berlijn leidde een aanval tot stroomuitval, terwijl in Nederland Vodafone kampte met netwerkproblemen en ASML een datalekclaim moest ontzenuwen. De grens tussen fysieke en digitale veiligheid vervaagt door hacks op elektrische rolstoelen en vitale infrastructuur in Venezuela. Daarnaast waarschuwen experts voor kritieke kwetsbaarheden in software en geavanceerde malware, terwijl Nederlandse overheidsinstanties fuseren om de digitale weerbaarheid te vergroten.

➤ LEES HET HELE ARTIKEL »

OPSPORING

Oudenbosch / Rotterdam - VIN-fraude

WhatsApp-fraude, ook wel VIN-fraude genoemd, is een geraffineerde vorm van oplichting waarbij criminelen zich voordoen als bekenden in nood. Door psychologische manipulatie en smoesjes over kapotte telefoons winnen zij het vertrouwen van slachtoffers om vervolgens om dringende betalingen te vragen. Deze digitale misdaad heeft vaak een fysieke kant, waarbij buitgemaakt geld direct wordt omgezet in goederen. Alertheid en persoonlijke verificatie via een telefoontje of controlevraag zijn essentieel om deze hybride vorm van criminaliteit te stoppen.

➤ 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 »