# NIEUWSBRIEF 403

**"Omdat wat waardevol is, beschermd moet worden"**

QUIZ

## Quiz week 05-2026: Van Koninklijke identiteitsfraude tot de 31,4 Tbps DDoS aanval

In het snel veranderende dreigingslandschap is actuele kennis uw eerste verdedigingslinie. Week 5 van 2026 kenmerkte zich door een complexe mix van geopolitieke cyberoorlogvoering, geavanceerde social engineering en kritieke kwetsbaarheden in vitale infrastructuur. Bent u volledig op de hoogte van de risico's die uw organisatie en de maatschappij raken?

Deze week zagen we hoe social engineering nieuwe vormen aanneemt, fraudeurs richtten zich specifiek op Belgische bedrijfsleiders door de identiteit van de Koning en zijn kabinetschef te misbruiken. Tegelijkertijd waarschuwt de FBI voor fysieke diefstal van Windows laptops, waarbij criminelen zich specifiek richten op BitLocker encryptiesleutels. Ook phishing blijft evolueren; herkent uw beveiligingsteam de 'rn' typefout techniek, waarbij domeinnamen visueel worden gemanipuleerd om Microsoft en Marriott te imiteren?

Op strategisch niveau zijn de cijfers zorgwekkend: uit onderzoek van de NOS blijkt dat 67% van de Nederlandse vitale infrastructuur afhankelijk is van Amerikaanse clouddiensten. Daarnaast zien we een samensmelting van fysieke en digitale fraude, zoals in Drenthe, waar een gekloonde PostNL-terminal werd ingezet voor miljoenenfraude bij Amazon.

Ook op het wereldtoneel verschuiven de fronten. Terwijl de NAVO een geautomatiseerde AI verdedigingslinie ontwikkelt, focust de beruchte Lazarus groep zich nu op spionage bij Europese dronefabrikanten en verbreekt het Aisuru/Kimwolf botnet records met een DDoS aanval van 31,4 Tbps.

Van de impact van Dynowiper malware tot datalekken bij SoundCloud (30 miljoen getroffenen) en ransomware gevolgen bij ziekenhuisgroep AZ Monica, de actualiteit vereist scherpte.

Test uw 'Situational Awareness'.
Beschikt u over de feitenkennis die nodig is om deze dreigingen te duiden? Doe de quiz en meet uw kennis van het nieuws van de afgelopen week.

**➤ START DE QUIZ »**

RAPPORT

## Strategische dreigingsanalyse van Digiweerbaar

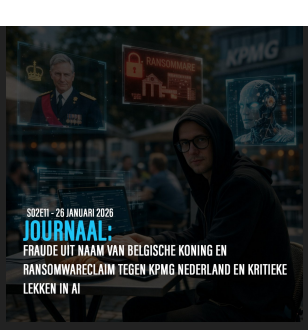
Dit wekelijkse rapport biedt een strategische dreigingsanalyse van actuele cyber en geopolitieke ontwikkelingen die de digitale autonomie en vitale infrastructuur van Nederland raken. Het geeft inzicht in afhankelijkheden, kwetsbaarheden en het veranderende dreigingslandschap, met focus op overheid, zorg en kritieke sectoren. Het rapport ondersteunt besluitvorming door risico's en trends helder en samenhangend te duiden.

**➤ NU 30 DAGEN GRATIS »**

CYBER JOURNAAL

### Fraude uit naam van Belgische koning en ransomwareclaim tegen KPMG Nederland en kritieke lekken in AI

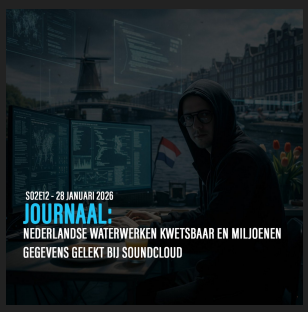
Er is sprake van meerdere cyberincidenten, waaronder fraude waarbij criminelen zich voordoen als de Belgische koning en




zijn kabinetschef om geld van bedrijven af te troggelen. Daarnaast heeft de ransomwaregroep Nova KPMG Nederland aangevallen, waarbij gevoelige data werd gestolen. Verder zijn er ernstige kwetsbaarheden ontdekt in AI-systemen van Microsoft en andere technologieën, terwijl de auto-industrie getroffen werd door demonstraties van zeroday kwetsbaarheden. Ook zijn er op het dark web gegevens van duizenden accounts gelekt door malware-infecties.

**➤ LEES HET HELE ARTIKEL »**

## CYBER JOURNAAL




**Nederlandse waterwerken kwetsbaar en miljoenen gegevens gelekt bij SoundCloud**

Een groot datalek bij SoundCloud heeft de gegevens van 30 miljoen gebruikers blootgelegd, waaronder e-mailadressen en locatie-informatie, doordat aanvallers toegang kregen tot een onbeveiligd dashboard. In Nederland is de digitale beveiliging van waterwerken zoals sluizen en bruggen kwetsbaar, wat grote risico's voor sabotage met zich meebrengt. Daarnaast werden kritieke kwetsbaarheden ontdekt in systemen van Citrix, SmarterMail en WinRAR, die door cybercriminelen actief worden misbruikt om gegevens te stelen of malware te verspreiden.

**➤ LEES HET HELE ARTIKEL »**

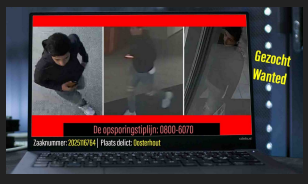
## CYBER JOURNAAL


**Sabotage Pools stroomnet en datalek Nederlandse huisartsenpost naast loonproblemen in Belgische zorg**

Recent waren er meerdere cyberincidenten die zowel lokale als internationale gevolgen hadden. In Polen werd een gecoördineerde aanval op het stroomnet uitgevoerd, vermoedelijk door de Russische groep Sandworm. In Nederland leidde een datalek bij huisartsenorganisatie Medrie tot de blootstelling van patiëntgegevens. Tegelijkertijd worstelen Belgische ziekenhuizen met de nasleep van een ransomware-aanval die de salarisbetalingen verstoorde. Cybercriminelen blijven nieuwe tactieken ontwikkelen, zoals het gebruik van AI en misleidende extensies, waardoor de dreiging voor zowel organisaties als consumenten toeneemt.

**➤ LEES HET HELE ARTIKEL »**

## OPSPORING




**Oosterhout - Oplichting**

In Oosterhout werd een oudere vrouw slachtoffer van een geavanceerde babbeltruc waarbij de oplichter zich voordeed als politieagent. Door psychologische manipulatie werd zij overtuigd haar bankpassen en sieraden af te geven aan een jongeman die snel voor haar deur stond. De gestolen pinpas werd vrijwel direct in de buurt gebruikt. Het onderzoek heeft geleid naar een vermoedelijk minderjarige verdachte, wiens beelden nu openbaar zijn om tips te verzamelen. De zaak benadrukt de gevaren van social engineering en misleiding.

**➤ 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