Cybercrimeinfo (ccinfo.nl)

Het onzichtbare zichtbaar maken

Nieuwsbrief 376

Podcast

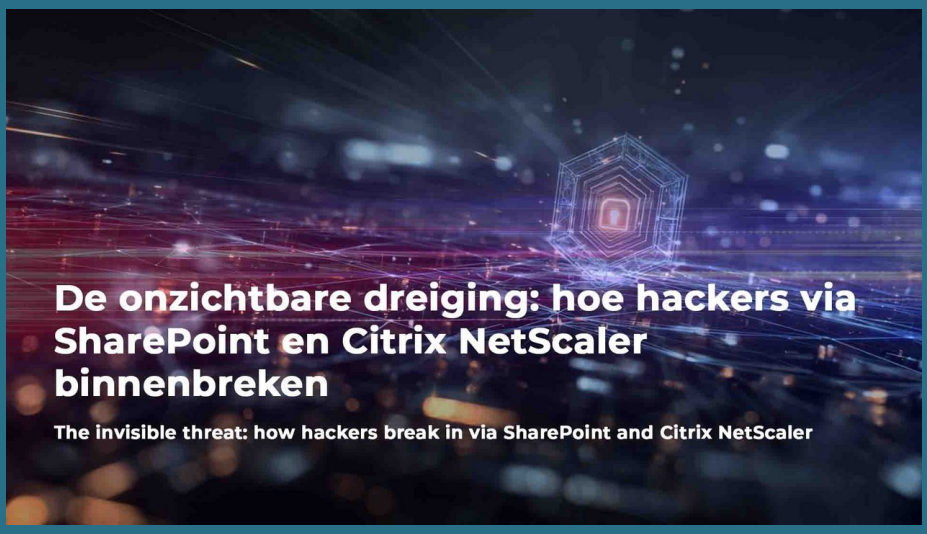
Podcast

Reading in another language

Hoe hackers jouw systemen binnenkomen: de cruciale rol van snel patchen tegen AI gedreven aanvallen

Cybercriminelen maken steeds slimmer gebruik van technologie om kwetsbaarheden in systemen te vinden en uit te buiten. De snelheid waarmee aanvallen plaatsvinden neemt toe, vooral dankzij de inzet van kunstmatige intelligentie. In dit artikel ontdek je hoe je systemen kunt beschermen door snel kwetsbaarheden te patchen en hoe de European Vulnerability Database (EUVD) je daarbij kan ondersteunen. Leer waarom het essentieel is om proactief te reageren en hoe je kunt voorkomen dat je systemen het slachtoffer worden van deze steeds sneller evoluerende dreigingen.

Lees verder



Reading in another language

De onzichtbare dreiging: hoe hackers via SharePoint en Citrix NetScaler binnenbreken

Cybercriminelen worden steeds slimmer in het misbruiken van kwetsbaarheden in veelgebruikte systemen. Recentelijk kwamen zowel Microsoft SharePoint als Citrix NetScaler in het vizier van geavanceerde aanvallers, wat heeft geleid tot aanzienlijke schade voor bedrijven en overheden wereldwijd. Hoe precies maken deze hackers gebruik van deze zwakke plekken? Wat is de impact van deze aanvallen en vooral: hoe kun jij jezelf en je organisatie hiertegen wapenen? In dit artikel duiken we diep in de recente dreigingen en geven we praktische adviezen om je systemen beter te beschermen.

Lees verder

Reading in another language

Rusland's digitale aanval op Nederland: wanneer een cyberaanval oorlog wordt

De digitale dreigingen tegen Nederland nemen toe, en de recente cyberaanval op het Openbaar Ministerie werpt belangrijke vragen op over de grenzen van cyberoorlog. Was dit slechts een aanval op kritieke infrastructuur, of kunnen we dit al zien als een daad van agressie die de grens naar oorlog overschrijdt? Dit artikel onderzoekt de implicaties van deze digitale aanval, de rol van Rusland, en de vraag of dit de basis kan

vormen voor NAVO-artikel 5. Ontdek hoe cyberaanvallen de traditionele opvattingen over oorlogvoering uitdagen en wat dit betekent voor de nationale veiligheid.

Lees verder

Reading in another language

Vraag van de week: kan een simpele foto je apparaat infecteren met malware?

Stel je voor: je opent een afbeelding die je via e-mail of sociale media hebt ontvangen, en ineens is je apparaat geïnfecteerd met malware. Het klinkt misschien onwaarschijnlijk, maar cybercriminelen gebruiken steeds vaker technieken waarbij ze onschuldige foto's inzetten om kwaadaardige software te verspreiden, zonder dat je zelf iets hoeft te downloaden of klikken. In dit artikel leggen we uit hoe deze aanvallen werken en welke stappen je kunt nemen om jezelf te beschermen tegen deze onverwachte bedreiging.

Lees verder

Reading in another language

De donkere handel in gestolen reisdocumenten: Hoe cybercriminelen identiteiten stelen en misbruiken

De handel in gestolen reisdocumenten is de laatste jaren uitgegroeid tot

een zorgwekkende dreiging voor zowel de veiligheid van individuen als voor de samenleving. Cybercriminelen hebben steeds geavanceerdere manieren gevonden om persoonlijke gegevens te stelen en deze te verkopen op het darkweb. Wat zijn de risico's van deze handel en hoe kunnen we onszelf beschermen tegen identiteitsdiefstal? Dit artikel biedt inzicht in de methoden van cybercriminelen, de waarde van gestolen documenten en de ernstige gevolgen voor zowel slachtoffers als de samenleving. Lees verder om te ontdekken hoe deze criminele praktijken werken en welke stappen je kunt nemen om jezelf te beschermen.

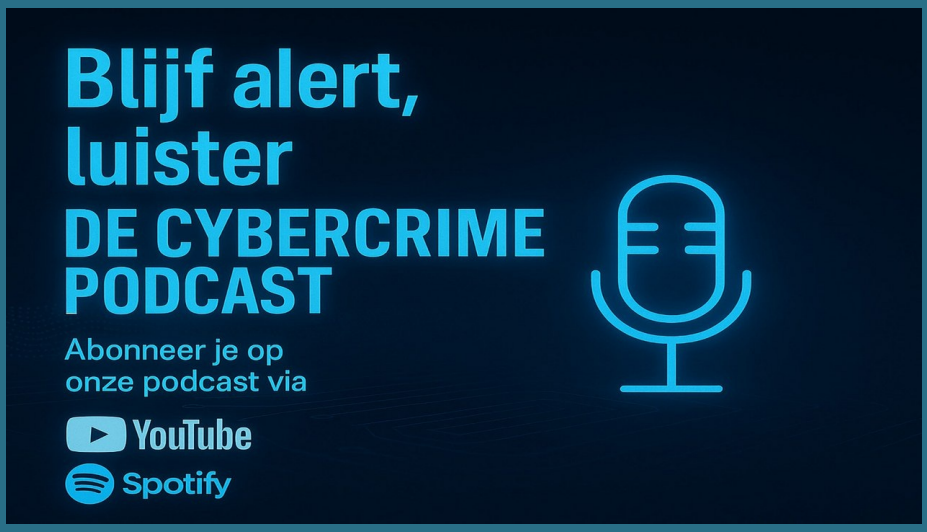
Lees verder

Reading in another language

Eersel - Nepagent

In Eersel werd een oudere vrouw slachtoffer van een geraffineerde oplichting door zogenaamde nepagenten. De criminelen overtuigden haar om waardevolle spullen, waaronder bankpassen, in veiligheid te stellen bij de politie. Wat volgde was een reeks misselijkmakende misdaden, waarbij duizenden euro's werden verduisterd. Ontdek hoe deze nepagenten te werk gaan, hoe je ze kunt herkennen en wat je moet doen om jezelf te beschermen tegen deze gevaarlijke vorm van oplichting.

Lees verder



De Cybercrime Podcast van Cybercrimeinfo

Wil je altijd op de hoogte blijven van het laatste cybernieuws? Abonneer je dan op **De Cybercrime Podcast**. Je ontvangt dagelijks een korte

update met betrouwbare informatie over actuele dreigingen, trends en praktische adviezen. De inhoud is zorgvuldig samengesteld door Cybercrimeinfo en eenvoudig te volgen via AI-gegenereerde Nederlandse stemmen. Luister waar en wanneer je wilt via **YouTube** of **Spotify** en versterk je digitale weerbaarheid. Abonneren is gratis en zo geregeld.

AI Chatbots Cybercrimeinfo

AI Chatbots | Ontdek **CyberWijzer**, **RechtRaadgever** en **NIS2Wijzer**, 24/7 beschikbaar voor hulp bij cybercriminaliteit, strafrecht en NIS2-wetgeving. Als je hulp nodig hebt bij het installeren of gebruiken van MindYourPass, gebruik dan AI Gids **VeiligSlot**. De AI **HRMWijzer** bevindt zich momenteel in de testfase van ontwikkeling en biedt richtlijnen en informatie over verschillende aspecten van HRM binnen de politie.

Reading in another language

Waarom jouw donatie aan Cybercrimeinfo essentieel is

Beste lezer,
In een wereld waarin digitale dreigingen steeds geavanceerder en talrijker worden, speelt Cybercrimeinfo een cruciale rol in de strijd tegen cybercriminaliteit. Als onafhankelijke organisatie, volledig gedreven door vrijwilligers, zetten wij ons in om het publiek te informeren en beschermen tegen de gevaren van het digitale tijdperk.

Jouw donatie maakt het verschil. Dit is waarom:

- **Een onafhankelijke en betrouwbare bron van informatie**
  Cybercrimeinfo is geen onderdeel van de Nederlandse Politie. Wij bieden een onpartijdige en toegankelijke bron van actuele informatie over cyberdreigingen, oplichtingstechnieken en

preventiemethoden.

- **Bewustwording en preventie mogelijk maken**
  Met jouw donatie help je ons om kennis en bewustzijn over cybercriminaliteit te vergroten. Onze artikelen, nieuwsupdates en praktische tips dragen direct bij aan het voorkomen van digitale misdrijven.
- **Ondersteuning van operationele kosten**
  Donaties worden direct gebruikt voor het hosten van onze website en het up-to-date houden van technologische middelen. Hierdoor kunnen we cybercriminelen blijven volgen en jullie informeren over de nieuwste digitale dreigingen.

Elke bijdrage, groot of klein, is van onschatbare waarde in onze strijd tegen cybercriminaliteit. Met jouw steun kunnen we blijven werken aan een veiliger digitaal landschap voor iedereen.

Doneer nu via onze doneerpagina (kies zelf het bedrag dat je wilt doneren) of gebruik de onderstaande QR-code.

We waarderen je steun enorm en bedanken je alvast voor je bijdrage aan deze belangrijke zaak.

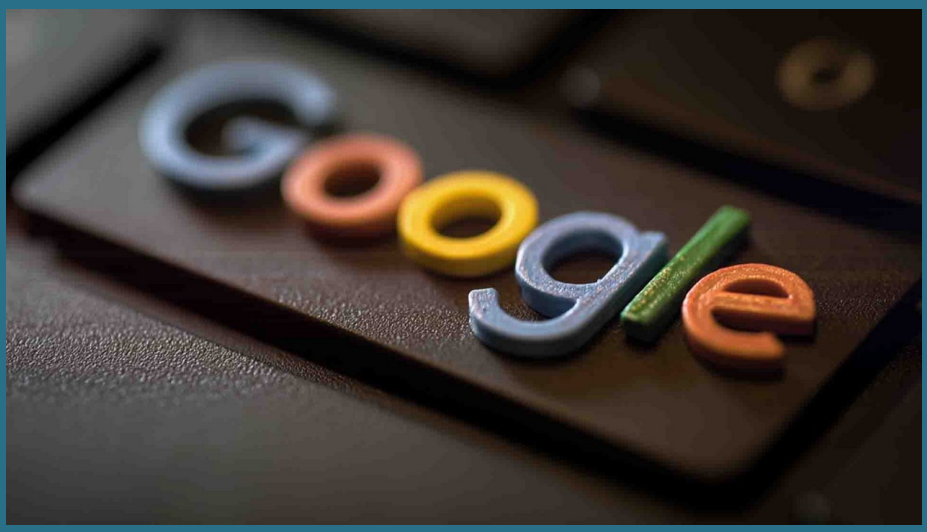
Met vriendelijke groet,
Het team van Cybercrimeinfo

Doneer | Cybercrimeinfo.nl (ccinfo.nl)

Doneer pagina

Geen budget? Geen probleem!

Help ons de zichtbaarheid van Cybercrimeinfo te vergroten met jouw Google review!



Laat jouw stem horen: Steun ons met een Google review!

Wij streven er voortdurend naar om de zichtbaarheid en bereikbaarheid van Cybercrimeinfo te verbeteren. Een fantastische manier waarop jij ons hierbij kunt helpen, is door een review achter te laten op Google. Jouw feedback is onmisbaar voor ons en helpt anderen om ons makkelijker te

vinden.
Het plaatsen van een recensie is simpel en kost slechts een minuutje van je tijd. Klik op de volgende link om jouw ervaringen te delen: **Schrijf een review.**
Elke review draagt bij aan onze missie om iedereen beter te informeren over cyberveiligheid. Jouw steun is voor ons ontzettend waardevol!
Hartelijk dank voor je betrokkenheid.

Non-profit team Cybercrimeinfo (ccinfo)

Schrijf een review

Share Tweet Share Pinterest Bluesky Mastodon