Nieuwsbrief 339

Reading in □□ or another language

De impact van Trumps herverkiezing op cyberveiligheid in Europa

De herverkiezing van Donald Trump kan grote gevolgen hebben voor de cyberveiligheid in Europa. Trump's beleidsvoorstel 'Project 2025' beoogt een beperking van de Amerikaanse cyberdefensie, door de verantwoordelijkheden van de Cybersecurity and Infrastructure Security Agency (CISA) te verminderen. Dit zou de internationale samenwerking op cybergebied verzwakken, wat vooral voor Europa riskant is, aangezien het regelmatig wordt geconfronteerd met grensoverschrijdende cyberdreigingen. Bovendien zou een afname van de Amerikaanse capaciteit cybercriminelen ruimte geven om vaker toe te slaan, wat de kwetsbaarheid van Europese infrastructuren vergroot.
Gezien deze ontwikkelingen is het cruciaal dat Europese landen hun eigen cyberverdediging versterken, bijvoorbeeld door intensievere samenwerking binnen de EU, technologische innovaties en opleidingsprogramma's. Het oprichten van het European Cybersecurity Competence Centre biedt een kans voor Europa om minder afhankelijk te worden van de VS en zichzelf beter voor te bereiden op de toenemende digitale dreigingen.

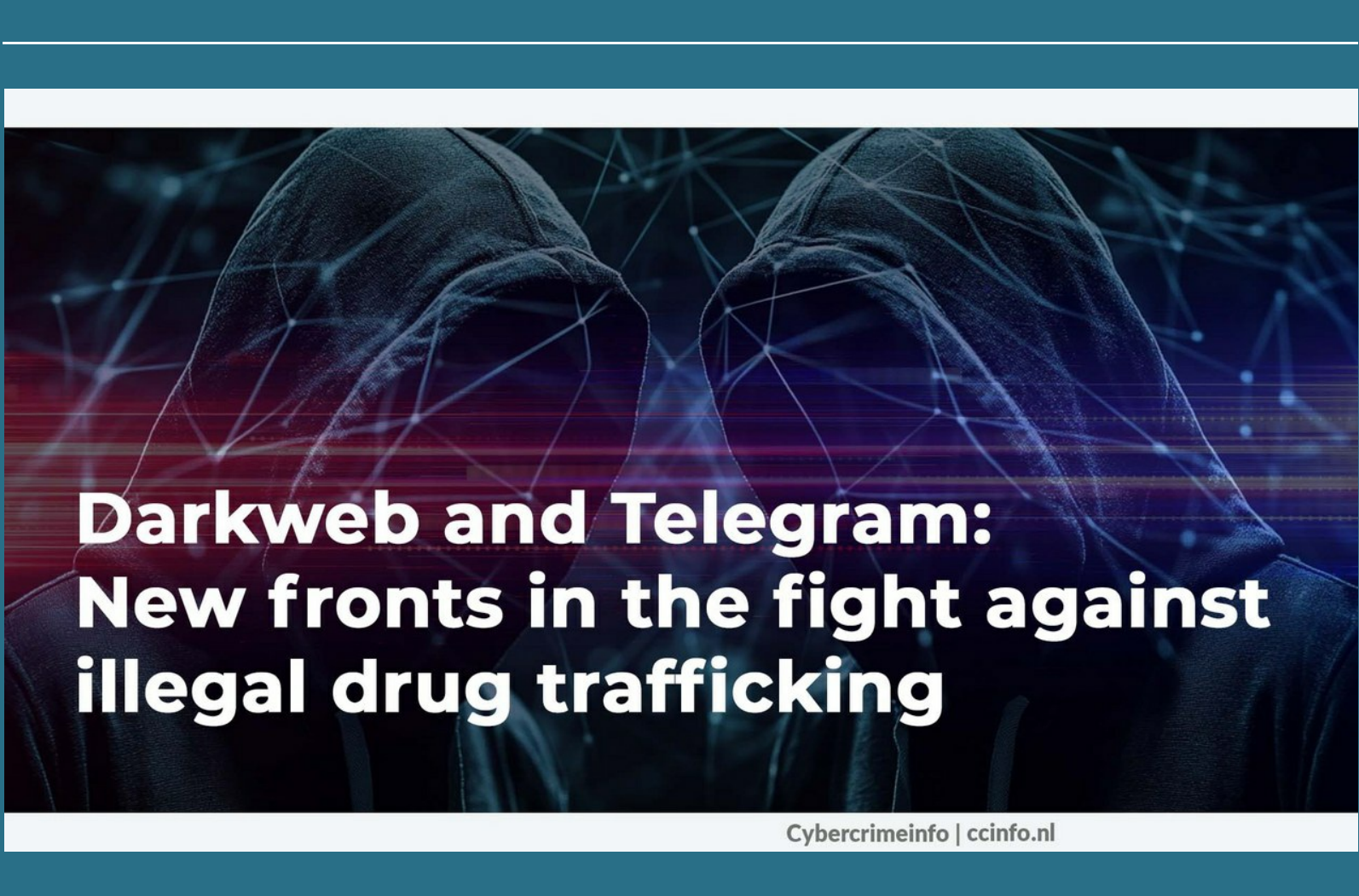
Lees verder

Reading in □□ or another language

Cyberoorlog nieuws 2024 oktober

In oktober 2024 werd Europa geconfronteerd met een reeks gecoördineerde cyberaanvallen, waaronder DDoS-aanvallen op overheidswebsites en kritieke infrastructuur in onder andere Nederland, België en Oekraïne. Russische hackergroepen, zoals de Russian Cyber Army, richtten zich op digitale systemen om ze te overbelasten, terwijl pro-Russische groepen in België meerdere websites van provincies en havens aanvielen. In Oekraïne gebruikten hackers nieuwe technieken om overheidsinstellingen en bedrijven binnen te dringen en gevoelige data te stelen. Bovendien werden ook desinformatiecampagnes versterkt, met doelwitten zoals Moldavië en de VS, waarbij geprobeerd werd politieke invloed uit te oefenen. In het Midden-Oosten werden ziekenhuizen en overheidsinstellingen in Israël getroffen door aanvallen die zowel desinformatie als ransomware omvatten. Deze gebeurtenissen onderstrepen de groeiende rol van cyberaanvallen in geopolitieke conflicten, waarbij landen en bedrijven worden aangemoedigd om hun cyberbeveiliging te versterken.

Lees verder



Reading in □□ or another language

Darkweb en Telegram: Nieuwe fronten in de strijd tegen illegale drugshandel

De illegale handel in drugs via digitale platforms zoals het darkweb en Telegram groeit snel. Deze platforms bieden criminelen anonimiteit, wat het voor wetshandhavers moeilijk maakt om in te grijpen. Het darkweb is een populaire marktplaats voor drugs en andere illegale goederen, terwijl Telegram wordt gebruikt voor het plaatsen van drugsadvertenties in openbare groepen, wat leidt tot duizenden verboden aanbiedingen per jaar.
Om deze dreiging aan te pakken, werken politie, Douane en bedrijven zoals DPD Nederland samen. Zij hebben bijvoorbeeld een gezamenlijke actieweek gehouden om illegale pakketten te onderscheppen. Dit heeft geleid tot de oprichting van het Hit and Run Postteam (HARP), dat gericht is op het scannen van verdachte post en pakketten. Technologie en bewustwording zijn cruciaal in deze strijd. De samenwerking tussen publieke en private partijen blijft noodzakelijk om de logistieke sector en de maatschappij te beschermen tegen criminele netwerken.

Lees verder

Reading in □□ or another language

Slachtofferanalyse en Trends van Week 44-2024

In week 44 van 2024 namen cyberaanvallen wereldwijd toe, met een focus op ransomware en datalekken. Sectoren die traditioneel minder doelwit waren, zoals de bouw, worden nu steeds vaker getroffen. Zo werd het Nederlandse bouwbedrijf Hemubo aangevallen, waarbij gevoelige gegevens mogelijk op het darkweb belandden. Ook grote organisaties, zoals de Duitse Kamer van Koophandel en apotheekgroothandel AEP, werden getroffen, wat de kwetsbaarheid van internationale bedrijven benadrukt. Daarnaast leidden datalekken, zoals de verspreiding van 190.000 Belgische inloggegevens op het darkweb, tot verhoogde risico's op identiteitsdiefstal en phishing. Overheidsinstellingen en de zorgsector zijn eveneens kwetsbaar, zoals bleek uit de aanval op het Indiase Fortis-ziekenhuisnetwerk. Het is duidelijk dat geen enkele sector veilig is, waardoor het essentieel is voor organisaties om hun cyberbeveiliging te versterken en proactieve maatregelen te nemen tegen deze dreigingen.

Lees verder

Reading in □□ or another language

Cyberweerbaarheid in Nederland: Innovatieve krachten tegen digitale dreigingen

In Nederland worden steeds meer innovatieve initiatieven ontwikkeld om de cyberweerbaarheid te verbeteren. Twee opvallende projecten zijn de "Friese agrarische sector Cyberproof" en de "Cyber Ambassadeurs". Het eerste project richt zich op het beschermen van boeren tegen cyberdreigingen die voortkomen uit de toenemende digitalisering van boerderijen. Door middel van trainingen en bewustwording helpt het initiatief boeren zich beter te wapenen tegen cyberaanvallen. Het tweede project, de "Cyber Ambassadeurs", zet vrijwilligers in om lokale gemeenschappen voor te lichten over online veiligheid. Dit programma, dat bijvoorbeeld in Breda succesvol werd uitgevoerd, helpt burgers zich te beschermen tegen phishing, fraude en andere vormen van cybercriminaliteit. Beide initiatieven benadrukken het belang van lokale betrokkenheid en samenwerking, waardoor cyberveiligheid toegankelijker wordt voor een breed publiek. Deze initiatieven dragen bij aan een veiliger digitaal Nederland en laten zien hoe gemeenschappen samen de strijd tegen cyberdreigingen aangaan.

Lees verder

Reading in □□ or another language

Alkmaar - Helpdesk fraude

Op 26 april 2024 werd een 78-jarige vrouw uit Alkmaar slachtoffer van bankmedewerkerfraude. Ze werd gebeld door een zogenaamde bankmedewerker die haar waarschuwde voor verdachte activiteiten op haar rekening. De oplichters vroegen haar om sieraden en een bankpas af te geven voor "veiligheidsredenen". Vertrouwend op de geloofwaardigheid van de oproep, gaf de vrouw haar sieraden, waaronder een trouwring, en haar bankpas mee. Later bleek dat er 800 euro van haar rekening was opgenomen. De dader die het geld opnam, was gekleed in een djellaba, hoofddoek en zonnebril. De politie vraagt getuigen om zich te melden.
Bankmedewerkerfraude is een vorm van oplichting waarbij criminelen zich voordoen als medewerkers van financiële instellingen om toegang te krijgen tot persoonlijke en financiële gegevens van slachtoffers. Het is belangrijk alert te zijn op dergelijke oplichters en nooit vertrouwelijke informatie te delen via onverwachte telefoongesprekken.

Lees verder

Reading in □□ or another language

Verbeter je cyberveiligheid: Test je kennis met onze interactieve quizzen

Verken de wereld van cybersecurity en het darkweb met onze interactieve quizzen op CyberCrimeInfo. Of je nu een beginner bent of een doorgewinterde expert, onze quizzen bieden een leuke en uitdagende manier om je kennis uit te breiden.

Wat kun je verwachten?

- **Leer in je eigen tempo:** Ontdek en test je vaardigheden wanneer het jou het beste uitkomt.
- **Ontvang feedback:** Krijg gedetailleerde feedback na elke quiz, zodat je precies weet waar je staat en waar je nog kunt verbeteren.
- **Verdien speciale erkenning:** Behaal een perfecte score en ontvang speciale erkenning voor je prestaties.

Ben je klaar om je kennis te testen en jezelf te meten met anderen? Begin vandaag nog aan je leerreis en vraag je toegangscode aan!

Naar quizzen

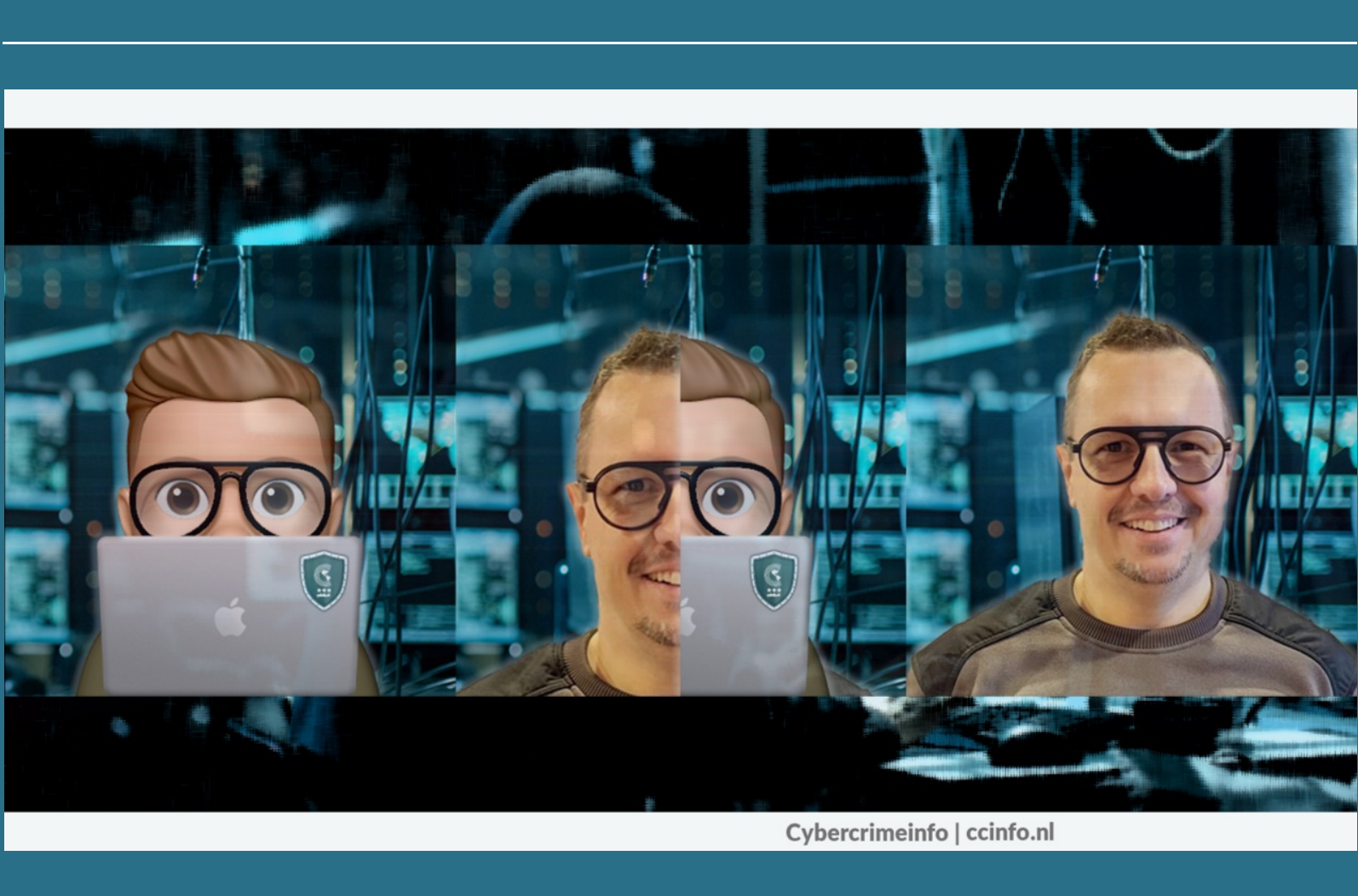
De Perfecte Score Club!

Topscorer	Punten	Wanneer
Joost W.	10	04-08-2024
Jasper	10	23-05-2024
Johan	10	16-03-2024
Philip S.	9	17-03-2024
Maxim	9	16-03-2024
Aart	7	21-06-2024
Thijs	7	09-04-2024
Kenan	7	30-03-2024

NIEUW TOEGEVOEGD

Maximaal te behalen **punten: 20**
Aantal deelnemers tot nu toe: 941

Totaal overzicht De Perfecte Score Club!



Reading in □□ or another language

Waarom jouw donatie aan Cybercrimeinfo essentieel is

Beste lezer,
In een wereld waar digitale dreigingen steeds geavanceerder en talrijker worden, speelt Cybercrimeinfo een cruciale rol in de strijd tegen cybercriminaliteit. Wij zijn een onafhankelijke organisatie, gedreven door vrijwilligers, die zich inzet voor het informeren en beschermen van het publiek tegen de gevaren van het digitale tijdperk.
Jouw donatie maakt het verschil. Hier is waarom:

1. **Onafhankelijke en Belangrijke 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.
2. **Bijdragen aan Bewustwording en Preventie:** Door te doneren help je ons in de missie om kennis en bewustzijn over cybercriminaliteit te vergroten. Onze artikelen, nieuwsupdates en praktische tips dragen bij aan het voorkomen van digitale misdrijven.
3. **Ondersteuning van Onze Operationele Kosten:** Donaties worden direct gebruikt voor het hosten van de website en het vernieuwen van onze technologische middelen. Dit stelt ons in staat om op de voet te volgen hoe cybercriminelen opereren en jullie te informeren over de nieuwste digitale gevaren.

Elke bijdrage, hoe klein ook, is van onschatbare waarde in onze continue strijd tegen cybercriminaliteit. Met jouw steun kunnen we blijven werken aan een veiliger digitaal landschap voor iedereen.
We waarderen je steun enorm en bedanken je alvast voor je bijdrage aan deze belangrijke zaak.

Doneren kan via de **doneer pagina** (Kies nu zelf het bedrag dat je wilt doneren!) of via onderstaande QR code.

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

Share Tweet Share Pinterest