Cybercrimeinfo.nl (ccinfo.nl) Bekijk de webversie

Nieuwsbrief 343

Reading in □□ or another language

Cyberoorlog nieuws 2024 november

In november 2024 intensiveerden Rusland, China en Noord-Korea cyberaanvallen die de wereldwijde veiligheid en geopolitiek beïnvloedden. Rusland saboteerde satellietverbindingen, wat leidde tot verstoorde tv-uitzendingen in Europa. China richtte zich op spionage en telecomnetwerken, terwijl Noord-Korea actief was in cryptohacks en malware. Hacktivisten veroorzaakten datalekken in Algerije en Israël, wat politieke onrust teweegbracht. Deze gebeurtenissen benadrukken de complexiteit van moderne cyberoorlogvoering en de diverse dreigingen van zowel staats- als niet-staatsactoren. De reacties op deze aanvallen, zoals formele klachten bij internationale organisaties, weerspiegelen de ernst van de situatie en de noodzaak van verhoogde cybersecuritymaatregelen wereldwijd.

Lees verder

Reading in □□ or another language

Analyse van kwetsbaarheden op het gebied van cyberbeveiliging november 2024

In november 2024 zijn verschillende kritieke kwetsbaarheden ontdekt en gepatcht in software en IoT-apparaten, waaronder zero-day aanvallen. Microsoft bracht updates uit voor 91 kwetsbaarheden, waarvan er vier actief werden misbruikt, zoals een NTLM-hash openbaarmaking en privilege escalatie in Windows Taakplanner. Andere significante kwetsbaarheden omvatten spoofing in Microsoft Exchange Server en privilege escalatie in Active Directory Certificate Services. Daarnaast werden kwetsbaarheden gevonden in IoT-apparaten zoals Philips Smart Verlichting en netwerkopslagapparaten van QNAP en Synology. Deze ontwikkelingen benadrukken de toenemende complexiteit van cyberoorlogvoering en onderstrepen het belang van tijdige updates om bedrijven te beschermen tegen potentiële aanvallen en datalekken.

Lees verder

Reading in □□ or another language

Hoe het darkweb de wereldwijde drugshandel faciliteert

In een recente zaak in Nederland werd onthuld hoe een criminele organisatie drugs wereldwijd verkocht via het darkweb en reguliere postverzendingen. De criminelen gebruikten alledaagse objecten om drugs te verbergen en communiceerden via versleutelde apps, wat illustreert hoe het darkweb de internationale drugshandel vergemakkelijkt. Deze zaak benadrukt de groeiende rol van het darkweb in illegale handel, de uitdagingen voor wetshandhaving, en de gevaren voor de samenleving door de anonimiteit en wereldwijde bereikbaarheid van deze platforms. Het incident onderstreept de noodzaak voor verbeterde technologie en internationale samenwerking om effectief op te treden tegen dergelijke criminele activiteiten.

Lees verder

Reading in □□ or another language

Slachtofferanalyse en Trends van Week 48-2024

In week 48 van 2024 werden wereldwijd diverse significante cyberaanvallen gemeld, waaronder ransomware-aanvallen op Belgische en Nederlandse bedrijven zoals Extra, Kela Health en VISUfarma. Deze incidenten hebben niet alleen grote financiële gevolgen, maar benadrukken ook de kwetsbaarheid van sectoren als retail en gezondheidszorg. Daarnaast werden grootschalige datalekken gemeld, waarbij persoonlijke gegevens zoals e-mailadressen en wachtwoorden werden buitgemaakt. Voor bedrijven en consumenten is het essentieel om proactief te zijn met beveiligingsmaatregelen zoals encryptie, netwerksegmentatie en training in cyberhygiëne. Deze maatregelen helpen de impact van cyberaanvallen te beperken en de veiligheid te waarborgen.

Lees verder

Reading in □□ or another language

Tip van de week: Digitale veiligheid in de keten: lessen voor thuis en op het werk

In het artikel "Digitale veiligheid in de keten: lessen voor thuis en op het werk" wordt de toenemende kwetsbaarheid van zowel bedrijfs- als thuisnetwerken besproken. Het benadrukt de risico's van ketenafhankelijkheden, zoals onveilige apparaten en zwakke wachtwoordbeveiliging, die leiden tot data-inbreuken. Het artikel vergelijkt de beveiligingsuitdagingen van bedrijfsnetwerken met die van thuisnetwerken en benadrukt het belang van een integrale aanpak voor digitale beveiliging. Praktische tips worden gegeven om thuisnetwerken te versterken, inclusief het gebruik van sterke wachtwoorden, regelmatige software-updates en bewustwording van digitale gevaren.

Lees verder

Reading in □□ or another language

Tilburg - Helpdesk fraude

In Tilburg heeft een onbekende man op 1 juni 2024 geld opgenomen met een gestolen bankpas, wat leidt tot een politieonderzoek en een oproep aan het publiek om informatie te delen. Dit incident staat symbool voor de voortdurende praktijken van oplichters die zich voordoen als bankmedewerkers om persoonlijke gegevens te stelen en bankrekeningen te plunderen. De politie benadrukt dat legitieme banken nooit om dergelijke informatie vragen en adviseert het publiek alert te blijven. Het delen van tips kan cruciaal zijn voor het oplossen van deze zaak en het voorkomen van verdere slachtoffers. Wees waakzaam voor soortgelijke vormen van fraude, zoals vishing en smishing, die ook gericht zijn op het verkrijgen van persoonlijke gegevens via misleidende communicatie.

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: 948 (+1)

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