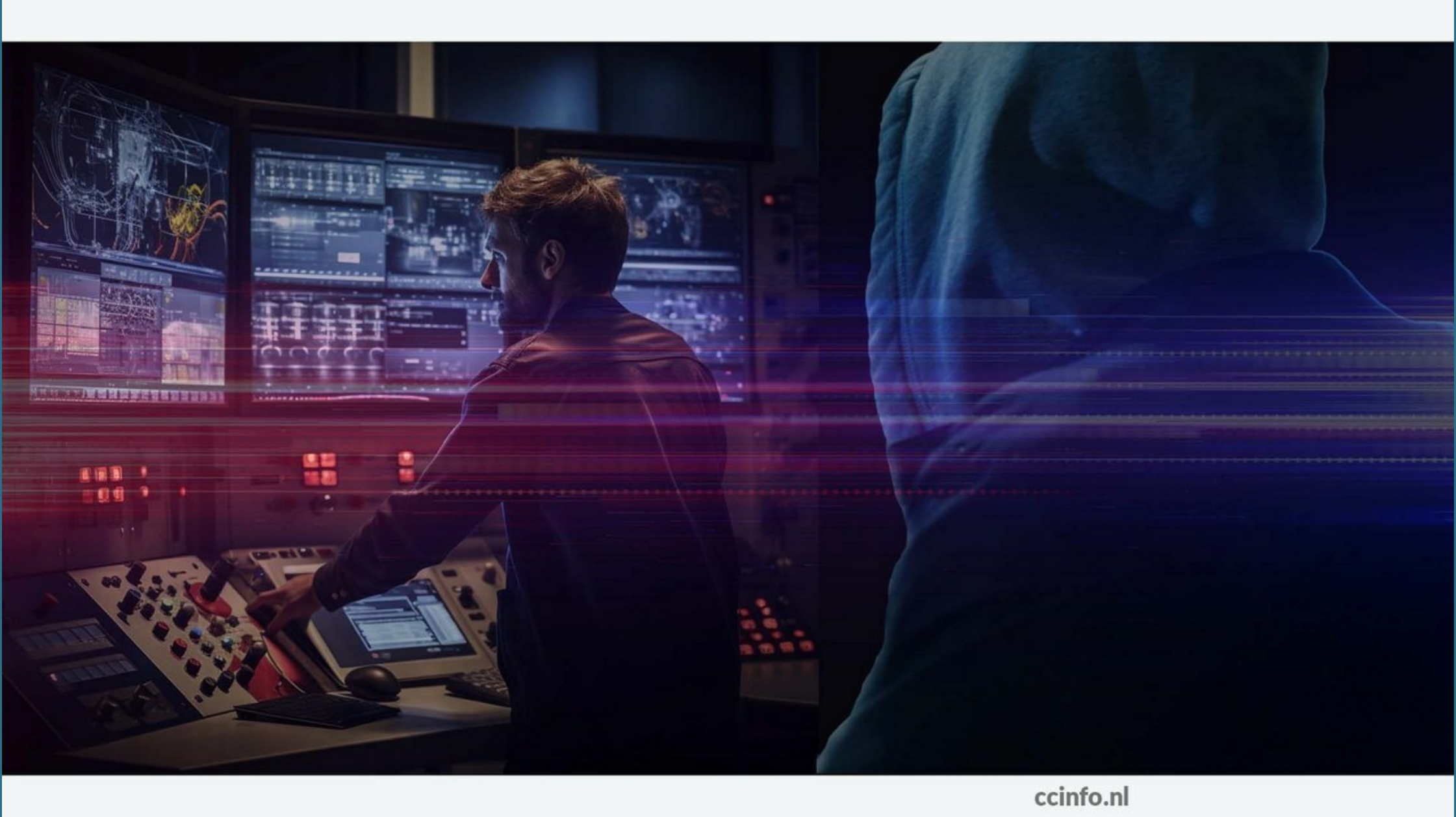
Nieuwsbrief 289 - Week 47-2023


ccinfo.nl

Navigeren door de evoluerende cyberdreigingen in industriële controlesystemen

Navigeren door de evoluerende cyberdreigingen in industriële controlesystemen wordt steeds urgenter. Deze systemen, vitaal voor onze infrastructuur, staan onder toenemende druk van cyberaanvallen, zoals benadrukt door de SANS ICS/OT Cybersecurity Survey van 2023. Kritieke infrastructuren, zoals energiecentrales en waterbehandelingsfaciliteiten, zijn toenemend doelwit van ransomware. Met de opkomst van nieuwe aanvalsmethoden specifiek gericht op ICS, is het essentieel dat organisaties anticiperen op beveiligingsrisico's door hun verdediging voortdurend te evalueren en te verbeteren.

Lees verder


ccinfo.nl

Cyberveiligheid en Retail Innovatie

In het artikel "Cyberveiligheid en Retail Innovatie" op CyberCrimeInfo.nl wordt diepgaand ingegaan op de recente ontwikkelingen in de Nederlandse retailsector op het gebied van digitale veiligheid en innovatie. Het Adyen Retail Report 2023, dat data van 12.000 bedrijven uit 24 landen omvat, belicht hoe Nederlandse retailers investeren in technologieën zoals omnichannel ervaringen, kunstmatige intelligentie, en marketing automation om te voldoen aan de veranderende consumentenbehoeften. Het rapport benadrukt ook het toenemende belang van cyberveiligheid, waarbij 94% van de Nederlandse retailers plannen heeft om hun bedrijven te verbeteren en te beschermen tegen cyberaanvallen. Dit omvat investeringen in encryptie, tweefactorauthenticatie en regelmatige veiligheidsaudits, in lijn met de AVG. Voor een uitgebreid inzicht in deze evoluties en de toekomstige richting van de retailsector, lees verder op CyberCrimeInfo.nl.

Lees verder


ccinfo.nl

De duistere diepten van het darkweb: Nederland's strijd tegen kinderpornografie

In het hart van Nederland's digitale duisternis woedt een onzichtbare strijd tegen kinderpornografie, een strijd waarbij de politie en organisaties zoals "Stop it Now!" een voorhoederol vervullen. Hun recente landelijke actieweek benadrukt de ernst van deze inspanningen: 95 waarschuwingen aan individuen om te stoppen met het downloaden van verboden materiaal, 55 huiszoekingen, en de inbeslagname van talrijke gegevensdragers. Deze actie illustreert niet alleen de proactieve aanpak van de Nederlandse politie, maar benadrukt ook het belang van vroegtijdige interventie om verdere betrokkenheid bij en de verspreiding van kindermisbruikbeelden te voorkomen. Dit diepgaande artikel onthult de complexiteit en de noodzakelijke samenwerking die nodig is in deze strijd, en belicht de cruciale rol van het Team Bestrijding Kinderporno en Kindersekstoerisme (TBKK). Ontdek meer over Nederland's aanpak en de impact van het darkweb op deze ernstige misdaden.

Lees verder

ccinfo.nl

Overzicht van slachtoffers cyberaanvallen week 46-2023

In week 46 van 2023 heeft CyberCrimeInfo.nl een gedetailleerd overzicht gepubliceerd van recente wereldwijde cyberaanvallen, waarbij verschillende sectoren en landen zijn getroffen. Opvallende incidenten zijn onder andere aanvallen op overheidsinstanties via een zerodaylek in Zimbra, een cyberaanval op Toyota Financial Services door Medusa Ransomware, en gerichte aanvallen door Russische hackers op ambassades met een WinRAR exploit en Ngrok. In Nederland zijn bedrijven zoals Nomot, Tunstall, de gemeente Vlaardingen en uitgeverij Em. de Jong getroffen. Andere landen, waaronder Duitsland, Finland en de Verenigde Staten, hebben ook significante aanvallen ervaren. De FBI en CISA waarschuwen voor toenemende ransomware-aanvallen, waarbij kwetsbaarheden in Windows, Sophos, Oracle en AMD CPU's worden uitgebuit. Dit overzicht benadrukt de noodzaak van verhoogde waakzaamheid en versterkte cyberbeveiligingsmaatregelen. Voor het volledige verslag van de cyberaanvallen van de afgelopen week, klik hieronder.

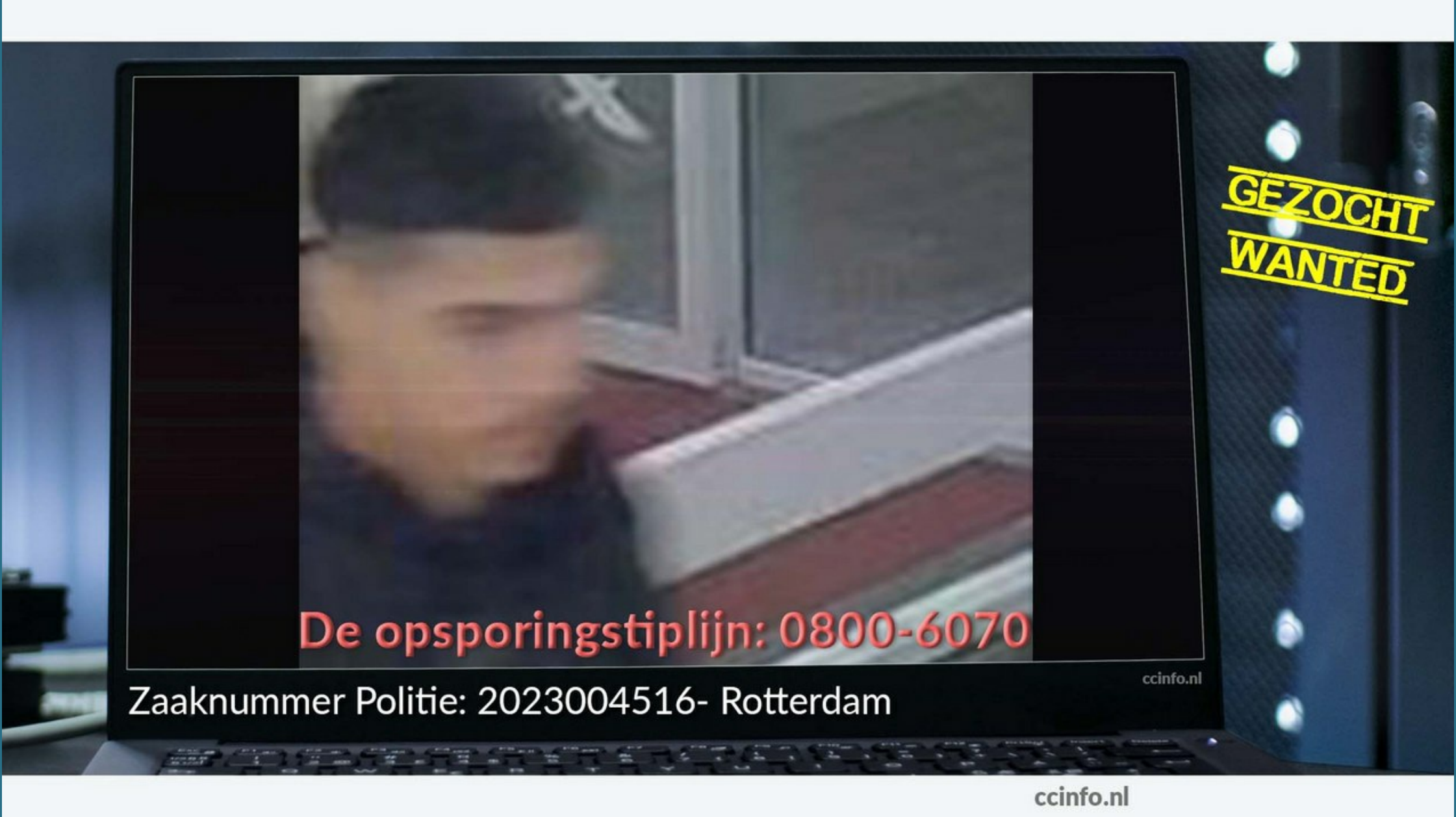
Lees verder

ccinfo.nl

Tip van de week: Cyberveiligheid op wielen - Bescherm uw slimme auto tegen cybercrime

In een wereld waar technologie steeds meer geïntegreerd is in ons dagelijks leven, vormen slimme auto's een opkomende trend die zowel gemak als nieuwe veiligheidsuitdagingen met zich meebrengt. Onze huidige 'Tip van de Week' op CyberCrimeInfo.nl richt zich op het beschermen van uw slimme auto tegen cybercriminaliteit. We belichten de kwetsbaarheden van deze technologisch geavanceerde voertuigen, zoals het risico op hacken van sleutelloze toegangssystemen en het manipuleren van autonome rijsoftware. Aan de hand van recente incidenten, zoals de hack van de Tesla Model X, onderstrepen we het belang van zowel digitale als fysieke veiligheidsmaatregelen. Dit artikel biedt praktische tips en strategieën om de cyberveiligheid van uw voertuig te verhogen, van het updaten van de software tot het versterken van de fysieke beveiliging. Bezoek CyberCrimeInfo.nl voor het volledige artikel en meer inzichten in cyberveiligheid.

Lees verder



ccinfo.nl

Rotterdam Noord - Bankhelpdesk fraude

In Rotterdam-Noord is een 76-jarige man het slachtoffer geworden van een doortrapte vorm van bankhelpdeskfraude. Deze specifieke vorm van criminaliteit houdt in dat oplichters zich voordoen als bankmedewerkers om zo toegang te krijgen tot pinpassen en pincodes van nietsvermoedende burgers. In dit geval werd de man telefonisch benaderd door iemand die zich voordeed als medewerker van de Rabobank, met het valse verhaal dat er fraude met zijn bankrekening was gepleegd. Na het overtuigen van het slachtoffer om zijn bankpas door te knippen, werd deze door een 'koerier' opgehaald, inclusief de mobiele telefoon van de man. De politie heeft beelden vrijgegeven van de dader en roept getuigen op om zich te melden. Dit incident benadrukt het belang van waakzaamheid tegenover telefonische benaderingen door vermeende bankmedewerkers. Lees het volledige artikel op onze website voor meer informatie en tips over hoe u zich kunt beschermen tegen dergelijke vormen van fraude.

Lees verder

AI Gids CyberWijzer

De AI Gids CyberWijzer is een geavanceerde AI Chatbot, aangeboden door Cybercrimeinfo. Deze chatbot gebruikt een aangepaste versie van ChatGPT-4 om betrouwbare en actuele informatie te verstrekken over cybercriminaliteit, het darkweb en cybersecurity. CyberWijzer is exclusief verbonden met de Cybercrimeinfo-database, waardoor het een veelzijdige bron is voor een breed scala aan doelgroepen. Deze omvatten beginners, gevorderden, cybercrime experts, CISO's, ondernemers, burgers, kinderen, IT professionals, studenten, juridische professionals, beleidsmakers, ontwikkelaars, malware analisten, en ICS en OT beheerders. Het biedt informatie over onderwerpen zoals cyberveiligheid, financiële fraude, ransomware, netwerkbeveiliging, en meer.

CyberWijzer is ontworpen om intuïtief en veilig te zijn, met eenvoudige navigatie en heldere uitleg. Het waarborgt privacy en veiligheid door geavanceerde encryptie en naleving van privacyregelgeving.

CyberWijzer

AI Gids RechtRaadgever

De AI Gids RechtRaadgever is een chatbot ontwikkeld voor gebruik in het gebied van strafrecht en strafvordering. Het is ontworpen om efficiënte, snelle en nauwkeurige antwoorden te bieden in het steeds veranderende digitale landschap. Deze chatbot dient als een essentiële bron voor opsporingsambtenaren, hulpofficieren en iedereen die geïnteresseerd is in strafrecht. De expertisegebieden van RechtRaadgever omvatten:

- **Strafrecht en Strafvordering**: Het biedt diepgaande informatie over een breed scala aan onderwerpen binnen deze gebieden.
- **Proces-verbaal en Bewijsrecht**: De chatbot geeft duidelijke en accurate antwoorden met betrekking tot proces-verbaal en bewijsrecht.
- **Wetteksten**: RechtRaadgever helpt gebruikers om eenvoudig door complexe juridische materie te navigeren.

RechtRaadgever is 24/7 beschikbaar en maakt gebruik van AI-technologie die continu leert en verbetert. Het biedt gebruikstips zoals het formuleren van duidelijke, specifieke vragen en het vertrouwen op exclusieve, betrouwbare bronnen. De chatbot garandeert een vertrouwelijke omgeving met privacybescherming, en moedigt gebruikers aan om te experimenteren met verschillende vragen om de capaciteiten van de chatbot te leren kennen.

De chatbot is gebruiksvriendelijk en veilig, met gemakkelijke navigatie, duidelijke antwoorden, geavanceerde encryptie en privacybescherming.

RechtRaadgever

Waarom jouw donatie aan Cybercrimeinfo.nl essentieel is

Beste lezer,
In een wereld waar digitale dreigingen steeds geavanceerder en talrijker worden, speelt Cybercrimeinfo.nl 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.nl 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 WhyDonate pagina of via onderstaande QR code.

Met vriendelijke groet,
Het team van Cybercrimeinfo.nl

Doneer | Cybercrimeinfo.nl (ccinfo.nl)

Share Tweet Share Pinterest