Nieuwsbrief 267 - Week 25-2023

Identiteitsfraude in Nederland: Een groeiend probleem

Identiteitsfraude is een ernstig en verontrustend probleem dat in Nederland in de afgelopen jaren dramatisch is toegenomen. Recentelijk meldde het Nationaal Cyber Security Centrum (NCSC) dat meer dan zesduizend Nederlanders het slachtoffer zijn geworden van identiteitsfraude. Deze alarmerende cijfers tonen de dringende behoefte aan effectievere strategieën en maatregelen ter bescherming tegen deze vorm van criminaliteit. Het aantal meldingen van identiteitsfraude is aanzienlijk gestegen en het daadwerkelijke aantal gevallen ligt vermoedelijk nog hoger. Fraudeurs maken vaak gebruik van persoonlijke informatie om contracten af te sluiten, wat verwoestende gevolgen kan hebben voor slachtoffers. Zowel individuen, bedrijven als overheidsinstanties moeten gezamenlijk actie ondernemen om identiteitsfraude aan te pakken en te voorkomen.

Lees verder

De Oekraïense IT Army: Een Blik op Cyberoorlogsvoering

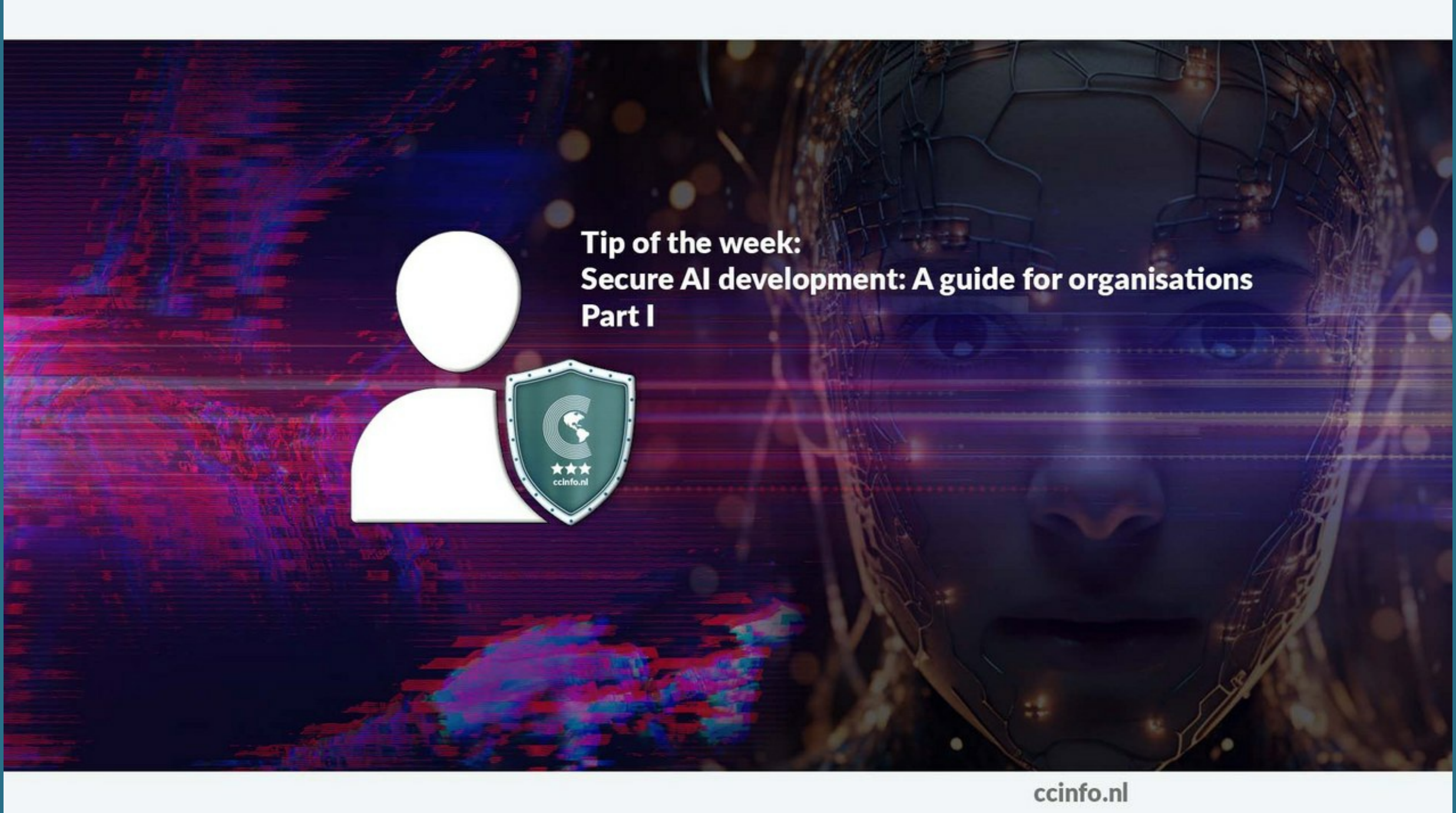
De Oekraïense IT Army heeft een aanzienlijke impact gehad op cyberoorlogsvoering, waardoor het digitale slagveld steeds relevanter is geworden in de 21e eeuw. Deze hacktivistische organisatie, vermoedelijk gelieerd aan de Oekraïense regering, biedt een zeldzaam inzicht in de aanvallende kant van cyberoorlogsvoering. De IT Army is ontstaan tijdens de Russische invasie van Oekraïne en maakt gebruik van een Telegram-kanaal om doelen te identificeren en tools te verstrekken aan gebruikers om aanvallen uit te voeren, waaronder gedistribueerde ontkenning van dienst (DDoS) aanvallen. In tegenstelling tot eerdere hacktivistische groepen is de IT Army opmerkelijk transparant en biedt het een grondig verslag van de aanvallende kant van cyberconflicten. Hoewel de Oekraïense regering beweert dat alleen civiele functionarissen betrokken zijn, wordt vermoed dat er samenwerking is met Oekraïense inlichtingenteams. Deze nieuwe vorm van oorlogsvoering roept echter ook nieuwe ethische en juridische vragen op die in de toekomst moeten worden aangepakt.

Lees verder

De grote uittocht naar Telegram: Een verkenning van de nieuwe ondergrondse cybercriminaliteit

In de wereld van cybercriminaliteit heeft er de afgelopen jaren een opmerkelijke verschuiving plaatsgevonden. Traditionele darkweb-marktplaatsen worden steeds meer verlaten ten gunste van Telegram, een berichtenplatform dat bekend staat om zijn sterke encryptie en privacyfuncties. Telegram is uitgegroeid tot een soort "darkweb" binnen handbereik, waar cybercriminelen illegale activiteiten ontplooien. Dit varieert van de verkoop van gestolen gegevens en het uitvoeren van ransomware-aanvallen tot het organiseren van cybercriminele groepen. Ransomware-bendes maken bijvoorbeeld gebruik van Telegram om hun activiteiten te coördineren en nieuwe leden te rekruteren. Naast ransomware-aanvallen vinden er ook andere vormen van cybercriminaliteit plaats op Telegram, zoals carding, DDoS-aanvallen en het verhandelen van gebruikersdatalijsten. Het bestrijden van cybercriminaliteit op platforms zoals Telegram vereist een gecoördineerde aanpak, waarbij het implementeren en handhaven van wachtwoordbeleid, multi-factor authenticatie en bewustwordingstraining voor medewerkers essentieel zijn. Door proactieve maatregelen te nemen, kunnen organisaties zich beter beschermen tegen de toenemende dreiging van cybercriminaliteit.

Lees verder



Tip van de week: Veilige AI-ontwikkeling: Een gids voor organisaties - Deel I

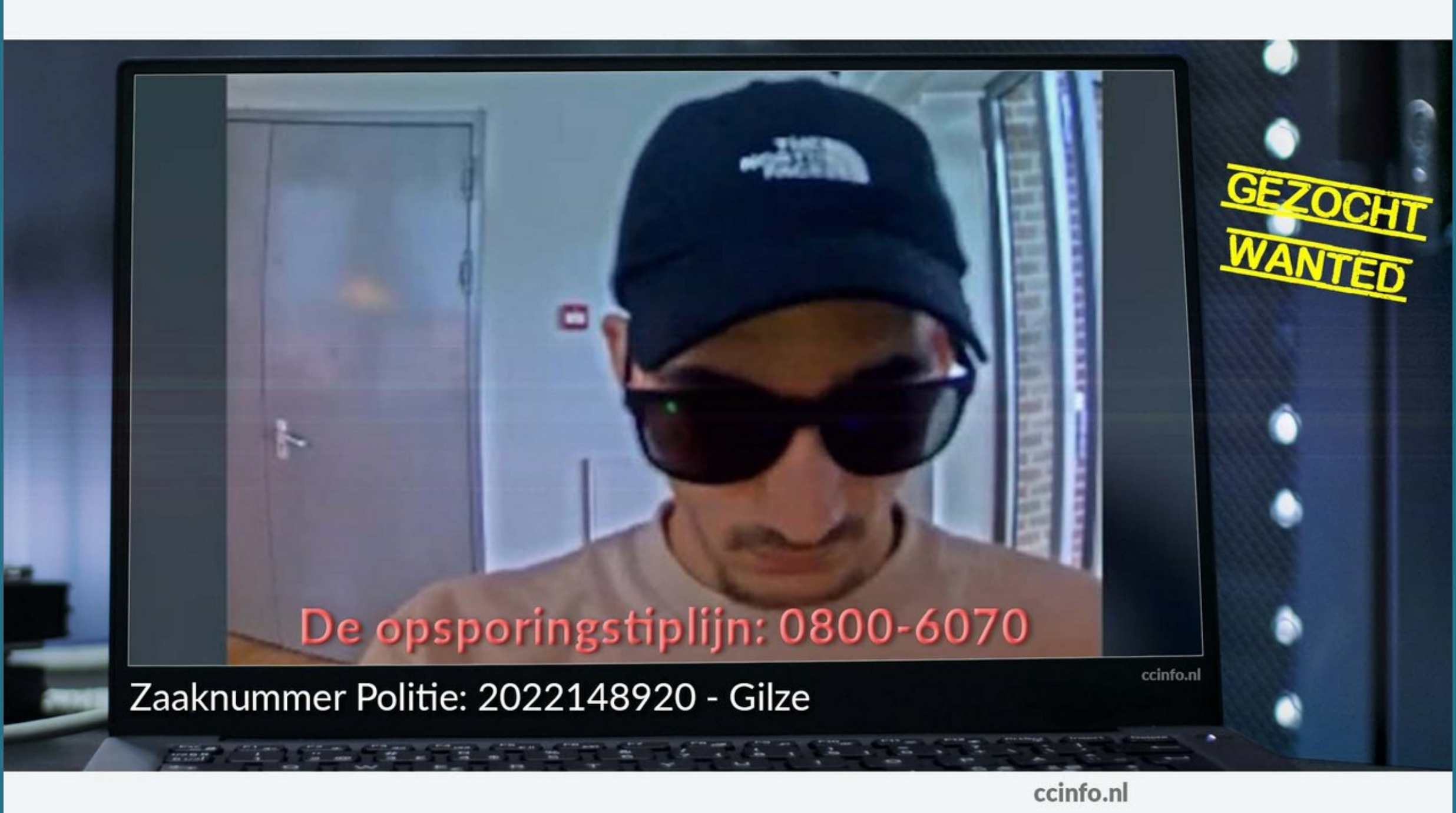
In de nieuwe serie "Veilige AI-ontwikkeling: Een gids voor organisaties" op Cybercrimeinfo kun je ontdekken hoe je veilige AI-systemen kunt ontwikkelen en implementeren. De serie behandelt de uitdagingen van AI-beveiliging en bespreekt hoe organisaties AI-systemen op een veilige, ethische en wettelijke manier kunnen ontwikkelen. Daarnaast wordt er aandacht besteed aan de rol van netwerken in AI. De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) heeft een vijfstappenplan ontwikkeld om organisaties te helpen bij het beveiligen van AI-systemen. De vijf stappen omvatten onder andere het begrijpen van de AI-technologie, het identificeren van potentiële bedreigingen, het ontwikkelen van verdedigingsstrategieën en het voortdurend monitoren en bijwerken van beveiligingsmaatregelen.

Lees verder

Overzicht cyberaanvallen week 24-2023

In de afgelopen week is er een golf van cyberaanvallen door heel Europa geweest, waarbij zowel Nederlandse als Belgische bedrijven en overheidsorganen getroffen zijn. De aanvallen zijn afkomstig van verschillende bronnen en er worden verschillende technieken gebruikt, waaronder ransomware, spyware en zero-day lekken. Onder andere het Nederlandse bedrijf Koper Automatisering en de Belgische bedrijven CHRN en Automatic Systems zijn slachtoffers geworden van deze aanvallen. Zelfs het wereldwijde energiebedrijf Shell is getroffen door een geavanceerde ransomware-aanval via een zero-day lek. Daarnaast heeft de Hengelose Scholengemeenschap OSG een deal gesloten met een ransomwaregroep na een aanval. De Clop ransomware bende lijkt nu de slachtoffers van de MOVEit data-diefstal in het vizier te hebben.

Bekijk het weekoverzicht



Gilze - Bankhelpdesk fraude

De politie is op zoek naar een verdachte in een cybercrimezaak in de Kerkstraat in Gilze. Op de website politie.nl is een foto van de verdachte geplaatst, en de politie roept het publiek op om tips over deze zaak door te geven. De verdachte wordt betrapt terwijl hij geld opneemt bij een pinautomaat met een gestolen pas, die eerder was buitgemaakt bij een 84-jarige man in Gilze. De politie vraagt mensen om contact op te nemen als ze de verdachte herkennen of weten waar hij zich bevindt. De zaaknummer is 2022148920 en de cybercrime vond plaats op 9 juni 2022 in Gilze.

Lees verder

Actuele cyberassistent die 24/7 beschikbaar is!

"De Cybercrimeinfo AI Chatbot - Elke dag getraind, elke dag beter in de strijd tegen digitale criminaliteit."

De Cybercrimeinfo AI Chatbot staat altijd paraat om uw vragen te beantwoorden over cybercriminaliteit, het darkweb en cybersecurity. Deze chatbot is exclusief verbonden met de Cybercrimeinfo-database en vertrouwt alleen op zorgvuldig gecontroleerde informatie uit deze bronnen. Alle informatie die de bot biedt, is grondig gecontroleerd en betrouwbaar. Hoewel de chatbot gespecialiseerd is in cybercriminaliteit, cybersecurity en het darkweb, kan hij voor vragen buiten dit domein toegang hebben tot internetbronnen om u van relevante en actuele informatie te voorzien. Wat de chatbot echt uniek maakt, is de wekelijkse update van informatie over cyberaanvallen, kwetsbaarheden, opsporingsnieuws en betrouwbare artikelen over cybersecurity, cybercrime en het darkweb. Klik hieronder om het volledige artikel te lezen op onze website.

AI Chatbot

Steun Cybercrimeinfo zodat we kunnen blijven bestaan

Om deze website te runnen en iedereen te kunnen blijven voorzien van het laatste nieuws, tips en tricks over digitale criminaliteit, zijn wij op zoek naar donateurs. Hiervan kunnen we onder andere nieuwe apparatuur aanschaffen, want deze hele site draait op vrijwilligers. Kortom, wij kunnen niet zonder jouw steun! Help je mee in de strijd tegen cybercrime?
Iedere donatie, hoe klein ook, is van harte welkom. Alvast bedankt namens het hele team van Cybercrimeinfo.

Doneren kan al vanaf 5 euro!

Doneer

Share Tweet Share Pinterest