Nieuwsbrief 269 - Week 27-2023

De toekomst van cybersecurity in Nederland: Een analyse van de dreigingen en mogelijkheden

In een tijdperk van digitalisering worden we geconfronteerd met toenemende cyberdreigingen. Het recente Cybersecuritybeeld Nederland 2023 rapport van de NCTV belicht de belangrijke rol van AI in de strijd tegen cybercriminaliteit, maar waarschuwt ook voor de uitdagingen die het met zich meebrengt. Verder blijkt uit het rapport de groeiende dreiging van cyberaanvallen, geïnitieerd door zowel individuen als georganiseerde groepen en statelijke actoren, en de noodzaak voor verhoogde digitale weerbaarheid. Ransomware vormt een bijzondere zorg, aangezien aanvallen niet alleen ernstige schade kunnen veroorzaken, maar ook de potentie hebben om de maatschappij te verstoren. Lees het volledige artikel op onze website om te begrijpen hoe we de uitdagingen van de toekomst kunnen aangaan.

Lees verder

De alarmerende realiteit van online seksueel ongewenst gedrag onder jongeren

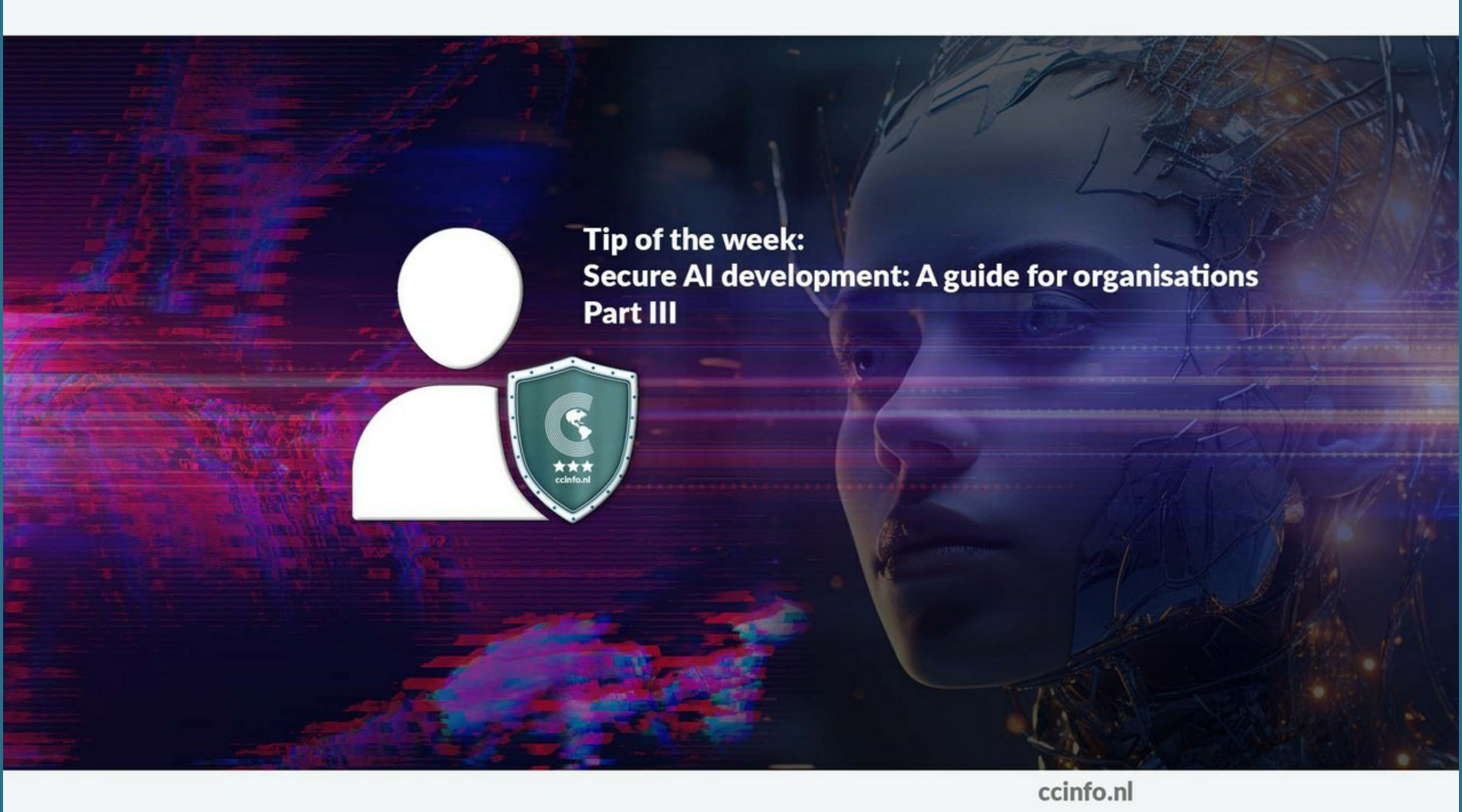
Het toenemend online seksueel ongewenst gedrag vormt een serieuze bedreiging voor de veiligheid van jongeren. Uit recent onderzoek blijkt dat 68% van de jongeren ten minste één keer in hun leven een vorm van online seksueel geweld heeft ervaren. Dit probleem, dat zich uitstrekt over Nederland, Duitsland, Frankrijk en Polen, onderstreept de dringende noodzaak voor gecoördineerde actie. Beleidsmakers, technologiebedrijven, ouders en de samenleving als geheel moeten samenwerken om onze kinderen en jongeren beter te beschermen en een veilige online omgeving te creëren. Educatie, bewustwording en effectieve bescherming zijn hierbij essentieel.

Lees verder

Hoe bedrijven reageren op datalekken op het darkweb

Het Kaspersky Digital Footprint Intelligence-team heeft een initiatief ontwikkeld om de reacties van bedrijven op datalekken op het darkweb te monitoren. Ze hebben posts op het darkweb opgespoord waarin toegang tot bedrijven, databases of gelekte accounts en andere kritieke incidenten te koop werden aangeboden. Het Kaspersky-team informeerde vervolgens de getroffen bedrijven. De resultaten tonen aan dat Europese bedrijven het meest getroffen zijn, met meer dan 25% van alle meldingen. Het initiatief onthulde tevens de alarmerende onvoorbereidheid, ontkenning en nalatigheid van veel bedrijven bij het omgaan met datalek-incidenten, wat de noodzaak onderstreept voor bedrijven om hun systemen en gegevens beter te beveiligen.

Lees verder



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

In dit deel van de serie over veilige AI-ontwikkeling zullen we de cruciale rol van de AVG (Algemene Verordening Gegevensbescherming) verkennen bij het waarborgen van gegevensbeveiliging. Organisaties die AI-technologieën ontwikkelen en implementeren, moeten zich houden aan de strenge AVG-eisen voor het verzamelen, opslaan en gebruiken van persoonlijke gegevens. In deze context is het essentieel dat organisaties juridisch advies inwinnen om ervoor te zorgen dat ze voldoen aan alle toepasselijke wetten en voorschriften, en zo juridische problemen en mogelijke boetes te vermijden. Bovendien moet rekening worden gehouden met specifieke sectorale regelgeving, zoals die welke van toepassing kan zijn op AI-systemen die worden gebruikt in de gezondheidszorg.

Lees verder

Overzicht cyberaanvallen week 26-2023

In week 26 van 2023 werden opvallende cyberaanvallen gemeld die wereldwijd een significante impact hebben gehad. Landal Greenparks was een doelwit van een ransomwaregroep die de gegevens van duizenden gasten publiceerde. TSMC, daarentegen, ontkende een cyberaanval ondanks een claim van een ransomwarebende die $70 miljoen eist. Tegelijkertijd werd een nieuwe malwarevariant genaamd EarlyRAT ontdekt, vermoedelijk afkomstig van Noord-Koreaanse cybercriminelen. In het Verenigd Koninkrijk vond een grootschalige ransomware-aanval plaats op een universiteit, met de diefstal van data van 1,1 miljoen patiënten. Ook Pepsi Bottling Ventures viel ten prooi aan malware, resulterend in een datalek dat 28.000 werknemers trof. Bij de KNMP werden bovendien persoonsgegevens van apothekers gestolen. Lees verder voor een gedetailleerd overzicht van deze cyberaanvallen.

Bekijk het weekoverzicht

Riel - Bankhelpdesk fraude

In Riel is een 84-jarige vrouw het slachtoffer geworden van bankpasfraude. Een fraudeur deed zich voor als een bankmedewerker en overtuigde de vrouw dat haar bankpas opgehaald moest worden om fraude te voorkomen. Hierbij werd er €1200 gepind van haar rekening bij een bankautomaat aan de Blokakkerstraat. De politie zoekt naar de identiteit van de persoon die deze transactie heeft uitgevoerd. Beschikt u over informatie die kan bijdragen aan dit onderzoek? Geef dit dan door via het tipformulier op de website van de politie. Uw hulp is essentieel in de strijd tegen digitale criminaliteit.

Lees verder

Winnaar! Luxe wellness-overnachting

Cybercrimeinfo.nl heeft Gerard van der Heijden bekroond als winnaar van een luxe wellness-overnachting bij B&B Arendsnest in Renswoude. Dankzij zijn doordachte antwoorden en zijn nauwkeurige oplossing voor de schiftingsvraag, heeft Gerard deze geweldige prijs verdiend. We willen iedereen die heeft deelgenomen aan deze competitie bedanken. Uw inzichten waren zeer waardevol en zullen ons helpen de functionaliteit en efficiëntie van onze nieuwe Cybercrimeinfo AI Chatbot-assistent te verbeteren. Blijf op de hoogte van onze initiatieven tegen cybercriminaliteit en bedankt voor uw continue steun!

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