DEELSESSIES FESTIVAL CYBERSECURITY IN DE ZORG 18 JUNI 2024

BLOK 1: VAN 15:30 TOT 16:15 UUR

Het Spook van de Spreekkamer | Don Eijndhoven

In de openende keynote lezing zet Don Eijndhoven het verband uiteen tussen geopolitieke gebeurtenissen in Oost-Europa en de Nederlandse Zorgsector. In deze opvolgende lezing gaat hij dieper in op de aankomende NIS2 wetgeving. Je hebt hier wellicht al de nodige angstaanjagende verhalen over gehoord. Don neemt in deze lezing de tijd om de zin van de onzin te scheiden en uit te leggen wat er straks van je wordt verwacht. Hierbij zal ook wat contextuele informatie worden gedeeld zodat je weet waar bepaalde uitspraken vandaan komen en hoe die opgevat dienen te worden. Kamp je met een onduidelijkheid over dit onderwerp, of heb je concrete vragen? Schuif aan en stel ze hier!

AI Act en CAICO Opleiding | Marit Blom | Sigra

We hebben te maken met een enorme groei aan AI-toepassingen. Europese AI-regelgeving gaat al in 2026 van kracht om gedegen te kunnen adviseren m.b.t. de compliance-aspecten van AI. Een AI Compliance Officer moet in deze behoefte kunnen voorzien. Sigra heeft in samenwerking met ICTRecht de CAICO-praktijkopleiding tot AI Compliance Officer inCompany georganiseerd voor Welzijn en Zorgaanbieders. Deze opleiding biedt de noodzakelijke kennis en vaardigheden op het snijvlak van AI, ethiek en compliance, met een scherpe focus op real-world toepassingen. Marit Blom neemt je mee in de highlights van de AI Act en de CAICO opleiding.

Demonstratie ethical hacking | Twente Hacking Squad | Universiteit Twente

Het ene beveiligingslek is nog niet gedicht en het nieuws schrijft alweer over het volgende kritieke beveiligingslek dat zo snel mogelijk moet worden opgelost voordat je systemen gehackt worden. Het lijkt alsof software inherent onveilig is en het niet een vraag is of je gehackt wordt, maar een vraag is wanneer je gehackt wordt. Tijdens deze sessie gaat de Twente Hacking Squad, het CTF-team van de Universiteit Twente, laten zien hoe makkelijk het fout kan gaan aan de hand van een live demonstratie en voorbeelden uit de praktijk.

Van keuze naar noodzaak: de evolutie van de bewustwordingstraining informatiebeveiliging | Wim Olijslager | Universiteit Twente

Privacy- en Security awareness trainingen zijn van cruciaal belang om medewerkers voor te lichten over de potentiële risico's en best practices voor het beschermen van kostbare data en informatie. Het helpt werknemers beveiligingsbedreigingen effectief te herkennen en erop te reageren, waardoor de kans op beveiligingsinbreuken als gevolg van menselijke fouten of onoplettendheid wordt verkleind. Door het bewustzijn te vergroten en voortdurend onderwijs te bieden, kunnen organisaties hun gegevens, systemen en bedrijfsmiddelen beter beschermen tegen cyberdreigingen. Wim neemt de deelnemers mee in de transitie van vrijwillige naar verplichte trainingen bij de Universiteit Twente.

Een cyberaanval? De zorg moet geleverd blijven worden! | Lucinda Sterk & Lisa de Wilde | Cyber Radiant

Het leveren van zorg aan patiënten is prioriteit nummer 1 binnen de zorgsector. Maar wat als dat heel moeilijk gemaakt wordt door een aanval van cybercriminelen? Tijdens deze interactieve presentatie nemen Lisa de Wilde (Cybersecurity Expert) en Lucinda Sterk (Crisiscommunicatie Expert) de deelnemers mee in de wereld van cyber-aanvallen. Ze bespreken de gevolgen van deze aanvallen op de zorgsector. Aan de hand van praktijkvoorbeelden geven ze je handvatten om de impact op jouw organisatie te verkleinen.
Lisa de Wilde heeft tientallen organisaties in binnen- en buitenland geholpen met het oplossen van complexe cyberaanvallen, waaronder een ziekenhuis. Lucinda Sterk heeft voor verschillende organisaties de crisiscommunicatiestrategie opgezet en de communicatie uitgevoerd tijdens verschillende crisissen.

BLOK 2: VAN 16:30 TOT 17:15 UUR

Aan de slag met de NIS2: wat kan ik nu al doen? | | Liesbeth Holterman | Cyberveilig Nederland

Met de NIS2 wordt aan de zorgsector straks verschillende cybersecurity maatregelen opgelegd. Om goed voorbereid te zijn op de NIS 2, is het verstandig om nu al de slag te gaan. Maar wat kan je nu al doen? En waar begin je? En wat moet je aanvullend nog regelen, als je als organisatie ook al voldoet aan den NEN7510, de norm voor informatiebeveiliging in de zorg? Liesbeth Holterman bespreekt dit in een praktische sessie. En natuurlijk zullen de highlight uit de internetconsultatie van de NIS 2 niet ontbreken. Na deze praktische sessie kan je aan de slag met de voorbereidingen voor de NIS 2.

ChatGPT, een goedkope security expert? | Thijs van Ede | Universiteit Twente

Recente ontwikkelingen in kunstmatige intelligentie hebben geleid tot slimme applicaties, van het bewerken van foto's tot het schrijven en redigeren van teksten. Chatbots zoals ChatGPT worden dagelijks gebruikt om te assisteren bij moeilijke taken en ze grotendeels over te nemen. Kan kunstmatige intelligentie, zoals ChatGPT, ook assisteren bij beveiligingsvraagstukken? Vertrouwen wij zulke programma's? En kan het helpen de werkdruk te verlichten? In deze deelsessie kijken we hoe ChatGPT werkt, of de output van deze programma's te vertrouwen is en welke recente ontwikkelingen deze technologieën beter inzetbaar maken.

Capture the flag: werken en denken als een hacker | Stichting Cyberbreinen |

Zelf ontdekken hoe het Twitteraccount van Donald Trump ooit gehackt is? Of een lek in de website van een snackbar vinden waardoor je bestellingen van andere klanten kunt zien? Je gaat het allemaal meemaken tijdens deze hands-on workshop. Je hoeft absoluut geen kennis van ICT te hebben, deskundige jonge cyberbreinen vanuit de Stichting Cyberbrein.nl helpen je waar nodig!

Kansen en risico's van gedrag op informatiebeveiliging | Sietske Rozie | Informatieveilig gedrag in de zorg

74% van alle datalekken en cybersecurityproblemen worden veroorzaakt door ons eigen gedrag. Patiënten en cliënten moeten erop kunnen vertrouwen dat hun persoonsgegevens veilig zijn bij hun zorgverleners. Toch gaan medewerkers, ondanks goede intentie en dus veelal onbewust, regelmatig onveilig met gevoelige informatie om. Zorgorganisaties zijn daardoor erg kwetsbaar voor cyberaanvallen en datalekken. Dat niet alleen, risico's op datalekken, identiteitsfraude en andere incidenten rondom informatieveiligheid en privacy worden steeds groter.

Sietske Rozie van het programma 'Informatieveilig gedrag in de zorg' deelt haar ervaring uit de praktijk als radioloog en geeft als gedragsdeskundige handvatten en tips voor jouw organisatie. Naast Sietske zal ook Martzen van het Ministerie van VWS, haar bijdragen doen en inzicht geven in hoe het Ministerie aankijkt tegen deze actuele onderwerpen.

De verborgen wereld achter cybercrime en gedigitaliseerde criminaliteit | Hanko van Giessen | Politie Eenheid Oost-Nederland

Een inkijk in de wereld van cybercrime en gedigitaliseerde criminaliteit met behulp van een aantal casussen uit de praktijk. In deze deelsessie wordt uitgebreid ingegaan op cybercrime delicten zoals ransomware en phising, en gedigitaliseerde criminaliteit in de vorm van bank helpdeskfraude en beleggingsfraude.

Hoe ziet de modus operandi van deze delicten eruit, wie zijn de slachtoffers en welke dadergroepen zijn verantwoordelijk voor deze nieuwe vorm van criminaliteit? En misschien nog wel het belangrijkste, hoe voorkom je dat je zelf slachtoffer wordt!

BLOK 3: VAN 18:15 TOT 19:00 UUR

NIS-2 staat niet alleen: welke andere cyber-wetgeving komt eraan? | Liesbeth Holterman | Cyberveilig Nederland

Met de NIS2 wordt aan de zorgsector straks verschillende cybersecurity maatregelen opgelegd. Maar naast de NIS2 zijn er ook nog andere wetten en regels op het gebied van cybersecurity die de komende jaren op ons af komen. Voorbeelden hiervan zijn de RED, de CRA en de Cyber Solidarity Act. Wat houden ze in en wat wordt de impact op de zorgsector? Deze sessie is met name interessant voor de doelgroep: inkoop, FG, CISO/security officer, management.

Zinvoller werken in de zorg met data en AI | Jelle Scholten | Little Rocket

De workshop "Zinvoller werken in de zorg met data en AI" zal zich specifiek richten op de toepassing van kunstmatige intelligentie en data-analyse om de zorgverlening te verbeteren. Jelle zal praktische tools en technieken presenteren die deelnemers kunnen inzetten om hun werkprocessen efficiënter en effectiever te maken. Dit biedt directe voordelen voor zowel de zorgverleners als de patiënten in verschillende zorginstellingen, waaronder ziekenhuizen, huisartsenpraktijken, ambulancediensten en de VVT-sector.

Hoe ga jij om met een cybercrisis? | Charlie van Genuchten | SURF

Het is ondertussen een standaard riedeltje: het is niet de vraag of, maar de vraag wanneer jouw instelling geraakt wordt door een cyberincident. Om je op dat moment voor te bereiden, is het handig om één keer in de zoveel tijd te oefenen hoe jouw organisatie (en jijzelf) zou reageren op zo'n crisis. In deze sessie gaan we daarom precies dat doen: een kleine cybercrisisoefening om je aan het denken te zetten. Je komt in een team te zitten met mensen van andere organisaties, zodat je kennis, tips en eventuele vraagstukken over cybercrisisprocedures kan uitwisselen met elkaar. En nu zien hoe iedereen door de crisis komt...

Cyber Escapebox: Verhoog je bewustwording op een spannende manier! | Bjorn van der Kerkhof en Tom Pearce | Game-effect

Stap in de wereld van informatiebeveiliging met onze spannende escapebox-sessie! Een organisatie is gehackt en jouw hulp is onmisbaar. Laat je meenemen in dit meeslepende avontuur en ontdek hoe jij kunt bijdragen aan een veiligere digitale omgeving.
Tijdens deze interactieve sessie leer je spelenderwijs alles over het belang van sterke wachtwoorden, hoe je phishingmails herkent, de basis van cryptografie en waarom het melden van incidenten cruciaal is. Daarnaast ontdek je hoe je een escapebox kunt inzetten om de bewustwording in jouw eigen organisatie te vergroten.

Starten met Cyber Trainen en oefenen | Auke Nicolai & Jeroen Brouwer | Z-CERT

In de eerste sessie zal je als deelnemer uitleg krijgen over de waarde van oefenen, de diverse vormen, de bijbehorende volwassenheid en hoe dit te organiseren. In een interactieve sessie worden de deelnemers uitgedaagd om mee te denken hoe ze oefenen, trainen en opleiden kunnen introduceren in de eigen organisatie. Auke en Jeroen geven hierbij een aantal praktijkvoorbeelden en praktische tips waarmee laagdrempelig kan worden gestart. Tevens geven ze inzicht in een ontwikkelplan voor de organisaties om in volwassenheid op het gebied van oefen, trainen & opleiden te groeien.

BLOK 4: VAN 19:15 TOT 20:00 UUR

Ontdek de NIS2 implicaties voor zorgorganisaties | Bruno Verweijen | Saxion Hogeschool

Ben je klaar om je organisatie naar een hoger niveau van digitale weerbaarheid te tillen? Samen met Bruno Verweijen, een vooraanstaand expert op het gebied van digitaal weerbare organisaties, duiken we in de wereld van NIS2 en verkennen we de implicaties voor jouw organisatie. Ontdek welke trends zich aftekenen in de weerbaarheid en leer hoe je de continuïteit van je organisatie kunt waarborgen.
In deze boeiende interactieve sessie gaan we in gesprek om o.a. concreet te maken wat NIS2 betekent en krijg je een voorproefje van de masterclass NIS2 voor bestuurders. Bruno Verweijen deelt met een positieve insteek zijn inzichten en beste tips tips om je organisatie klaar te stomen voor de toekomst.

GPT-4 en andere large language models beveiligen, dit is wat je moet weten| Willem Meints | Aigency

Steeds meer mensen maken gebruik van large language models voor uiteenlopende toepassingen. Met alle mooie nieuwe use cases die ontstaan komen we helaas ook steeds vaker uitdagingen tegen op het gebied van beveiliging.

In deze sessie laat Willem zien waar je risico loopt bij het gebruik van large language models zoals GPT-4 en hoe je in een aantal stappen die risico's kan verkleinen door je bestaande kennis op beveiligingsgebied toe te passen op AI en large language models.

Workshop cybersecurity: de basis op orde? | Saxion studenten | Saxion Hogeschool

In deze workshop gaan de deelnemers zelf aan de slag met een aantal praktische scans om te kijken in hoeverre ze de basis op orde hebben op het gebied van cybersecurity. Je kunt bijvoorbeeld zelf checken of je e-maildomein goed is ingesteld zodat cybercriminelen niet vanuit je e-mail-naam een phishingmail kunnen versturen. En in hoeverre heb je de basismaatregelen genomen die geadviseerd worden vanuit het Digital Trust Center? Je krijgt vervolgens praktische tips om mee aan de slag te gaan. En geen nood: je wordt hierbij begeleid door studenten van Hogeschool Saxion.

Cyber Escapebox: Verhoog je bewustwording op een spannende manier! | Bjorn van der Kerkhof en Tom Pearce | Game-effect

Stap in de wereld van informatiebeveiliging met onze spannende escapebox-sessie! Een organisatie is gehackt en jouw hulp is onmisbaar. Laat je meenemen in dit meeslepende avontuur en ontdek hoe jij kunt bijdragen aan een veiligere digitale omgeving.
Tijdens deze interactieve sessie leer je spelenderwijs alles over het belang van sterke wachtwoorden, hoe je phishingmails herkent, de basis van cryptografie en waarom het melden van incidenten cruciaal is. Daarnaast ontdek je hoe je een escapebox kunt inzetten om de bewustwording in jouw eigen organisatie te vergroten.

Geavanceerd Cyber Trainen en oefenen | Auke Nicolai & Jeroen Brouwer | Z-CERT

Introductie van de volwassenheidsniveaus en bijbehorende randvoorwaarden voor geavanceerd oefen, trainen & opleiden. Hoe kun je je eigen cyberweerbaarheid en incident respons verhogen en hoe komen we tot een betere regionale en landelijke cyberweerbaarheid. Wat is er al geregeld en beschikbaar op het gebied van instelling overstijgende oefenprogramma's, wat kan je hier als instelling zelf mee en hoe kunnen we als regio hierop aansluiten?