DEELSESSIES FESTIVAL CYBERSECURITY IN DE ZORG 20 JUNI 2023

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

Hoe hackt een hacker: de menskant | Sophie Jellema | Secura

In deze interactieve sessie legt psycholoog en sociaal engineer (mensenhacker) Sophie Jellema uit hoe social engineers werken. Bijvoorbeeld, hoe zorgen social engineers dat de kans zo groot mogelijk wordt dat jij in een phishingmailtje trapt of hoe kraken ze wachtwoorden? En misschien nog wel belangrijker: in de sessie wordt ook uitgelegd wat jij kan doen om jezelf (beter) te beschermen tegen hackers.

De mens als zwakste schakel? No way! | Remco Spithoven | Lectoraat Maatschappelijke Veiligheid Saxion

Na deze workshop ga je naar buiten met een andere kijk op cyberweerbaarheid. We kijken veel te negatief naar de rol van de mens in cybersecurity en het is hoog tijd om dat aan te pakken! We verkennen waar dit perspectief vandaan komt, wat we dan missen en hoe we ons handelingsperspectief kunnen verrijken.

Een kijkje in de keuken van een (ethische) hacker | Mats Dekker | Ethische hacker

Tijdens deze workshop moeten de deelnemers de handen uit de mouwen steken. De deelnemers gaan namelijk zelf bezig met de tools die hackers gebruiken om te hacken. Voorbeelden hiervan zijn phising en OSINT. Daarnaast worden de deelnemers meegenomen in de wereld van Artificial Intelligence en welke veiligheidsvraagstukken het met zich meebrengt.

Ransomware: real-life impact en de preventieve waarde van criminologie | Jeroen Brouwer | Veiligheidsregio Twente

Vanuit ervaringsdeskundigheid wordt aan de hand van casuïstiek een inkijk gegeven in de impact van een ransomware aanval. Uiteraard zijn er technische consequenties, maar een ransomware aanval vraagt ook het een en ander van je organisatie; daar wordt in deze deelsessie op ingezoomd. Nadat in beeld is gebracht hoe groot de impact van een ransomware aanval kan zijn, wordt er stilgestaan bij preventie. Ook hier voeren technische aspecten vaak de boventoon, gevolgd door ‘leuke bewustwordingscampagnes’. Zelden zijn deze maatregelen voldoende om een gemotiveerde aanvaller te stoppen. Ontdek hoe theorieën uit de criminologie kunnen bijdragen om weerbaarder te zijn tegen ransomware aanvallen!

Social engineering: de menselijke factor | Rik Sentveld | Z-CERT

Rik Sentveld werkt als Senior Cybersecurity Support Specialist bij Z-CERT. Daarvoor was hij 24 jaar werkzaam bij het Ministerie van Defensie als netwerk- en incidentmanager en als cybersecurity specialist en docent bij het Cyber Warfare & Training Centre. Zijn opgedane kennis van social engineering, OSINT en gedragsanalyse gebruikt hij tegenwoordig om de zorgsector te beveiligen. Deze deelsessie zal voornamelijk gaan over wat je kunt doen met de lessen die zijn geleerd naar aanleiding van een cybercrisis (bij je eigen organisatie of die van een ander) om zowel jezelf, collega’s en de organisatie te wapenen tegen social-engineering aanvallen in de toekomst.

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

Klaar voor Quantum | Roland van Rijswijk-Deij | Universiteit Twente

In deze deelsessie wordt stilgestaan bij quantum computing. Wat is quantum computing: Quantumcomputers zijn intelligente en krachtige computers. Computers die informatie op een nieuwe manier verwerken en op deze wijze grote en belangrijke doorbraken kunnen forceren. Er wordt verwacht dat quantumcomputers deuren opent naar mogelijkheden die nu nog ondenkbaar zijn. Hoewel quantum computers voor velen nog science fiction lijken, moeten we ons nu al voorbereiden op de komst ervan. In deze presentatie legt Roland uit waarom.

Interactief ervaringen uitwisselen: Security-incidenten en datalekken | Erik van den Beld | Audittrail & Liberein

Ieder datalek is een beveiligingsincident, maar andersom niet. Tijdens deze sessie bespreken we hoe je omgaat met afwegingen met betrekking tot informatiebeveiligingsincidenten en datalekken. Tijdens deze interactieve sessie bespreken we zowel de procedurele kant als de juiste mensen en expertise die je in een dergelijke situatie nodig hebt. Deelnemers worden van harte uitgenodigd om eigen casuïstiek in te brengen om van elkaar te leren.

Dilemma's bij crisiscommunicatie | Lucinda Sterk | Communicatie expert

Aan de hand van voorbeelden uit de zorgpraktijk en enkele prikkelende stellingen wordt in deze deelsessie de discussie op gang gebracht in de groep over communicatie bij een hack. Wanneer ga je extern communiceren? Hoe ga je om met technisch deskundigen die liever niet willen dat je communiceert maar Twitter al ontploft van de wilde geruchten? Hoe ga je om met interne critici die vinden dat je communicatie sneller/beter/anders moet?

Thoughts on prevention of cybercrime and online fraud: Wat kunnen we leren van de medische wetenschappen? | Jan-Willem Bullee | Universiteit Twente

Het voorkomen van cybercrime en online fraude is een complexe uitdaging die vraagt om innovatieve benaderingen. In vergelijking met gevestigde vakgebieden zoals accounting, geneeskunde en logistiek, is cybercrime relatief nieuw en nog steeds in ontwikkeling. Om deze groeiende dreiging aan te pakken, kunnen technieken uit andere disciplines, zoals de geneeskunde, worden toegepast. Door de parallellen tussen cyberaanvallen en gezondheidsaandoeningen te onderzoeken, kunnen preventieve maatregelen worden ontwikkeld om de cyberbeveiliging te versterken. Kunnen de principes van het screenen op ziekten worden toegepast om cybercrime en online fraude terug te dringen?

Mijn organisatie gaat op zwart, wat nu? | Luuk Stadhouders | Berenschot

Cyberincidenten hebben de laatste jaren een vlucht genomen, ook in de zorg. Het is niet meer de vraag óf, maar wanneer een organisatie wordt geraakt door een cyberaanval. Goed voorbereid zijn en weten wat te doen bij een cyberincident is de enige manier om de toenemende digitale dreigingen en daaruit voortkomende (mogelijke) risico's een stap voor te blijven. Leren van incidenten - in je eigen organisatie, maar ook bij andere - is minstens zo belangrijk. Wat ging goed? Wat kan beter? Luuk deelt de belangrijkste lessen uit zijn praktijkervaring en geeft concrete inzichten hoe je je organisatie goed voorbereid.

Sinds 2020 werkt Luuk Stadhouders als managing consultant bij Berenschot op het gebied van cybersecurity en informatiebeveiliging. Luuk richt zich op vraagstukken op het gebied van incident- en crisismanagement (OTO), strategie en beleid, en inrichting en samenwerkingsvraagstukken binnen en tussen organisaties.

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

Een cyberaanval? Laat je niet verassen! | Lucinda Sterk | Communicatie expert

In deze deelsessie zal Lucinda het gaan hebben over de diverse manieren waarop je jezelf kan voorbereiden op een cyberaanval en hoe je de kans op een cyberaanval zo klein mogelijk maakt. Hierbij worden ook 'de open deuren' besproken die iedereen kent, maar waar zoveel organisaties nog over struikelen. Het is geen raket wetenschap, maar een kwestie van doen.

NIS-2: Wat komt er op ons af? | Auke Nicolai | Z-CERT

De NIS2, of in het Nederlands de NIB2 is onontkoombaar, ook voor de Nederlandse zorgsector. Hoewel nog niet alles volledig is uitgewerkt weten we nu een aantal zaken wel. Het is goed om deze kennis met u te delen zodat we de tijd die we hebben voor de daadwerkelijk implementatie, goed en efficiënt kunnen besteden.

Auke is sinds vier jaar Business Consultant bij Z-CERT en verantwoordelijk voor een van de deelnemers voor bestaande dienstverlening. Daarnaast is Auke betrokken bij de diverse projecten binnen Z-CERT om in samenwerking met de deelnemers de diensten te verbeteren en uit te breiden. Auke is al ruim 30 jaar werkzaam in de ICT in verschillende rollen en aandachtsgebieden.

Keep it simple!| Werner Zuurbier | Meander Medisch Centrum

In deze deelsessie zal Werner de waarde van risico-assessments en security frameworks benadrukken. Hoe kan je als relatief 'kleine' zorginstelling toch voldoen aan steeds strengere eisen rondom security (NEN7510) en de komende regelgeving? Het gevaar bestaat dat uit angst voor cyberdreigingen er veel redenen worden gezocht om vooral iets niet te doen! Wil je meer te weten komen over het benutten van kansen van digitalisering, dan ben je in deze deelsessie aan het juiste adres!

Hoe pas je technologie op een ethisch verantwoorde manier toe? | Marit Blom | Sigra

In deze sessie ga je ervaren wat je aan de aanpak beleidingsethiek (ABE) kunt hebben. Dit is een innovatieve methode die concrete handvatten biedt om technologie op een ethisch verantwoorde manier toe te passen. Tijdens de workshop zetten we één zorgtechnologie centraal en gaan de aanpak verkort ervaren.

Zo simpel kan het zijn: gehackt in seconden | Thijs van Ede & Jerre Starrink | Twente Hacking Squad

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.

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

Cyberbreinen | Henk van Ee | Stichting Cyberbreinen

Henk van Ee en twee jonge cyberbreinen geven een demonstratie over:
Open Wifi: wat kan een hacker eigenlijk meelezen als je verbindt met een Open Wifi netwerk? “USB”-stick: hoe werkt het nu als je een tooltje van een hacker installeert omdat je denkt dat het een gewone USB-stick is? Wat kan dan allemaal? En bluetooth: wat zijn daar de risico’s van?

Samen Sterker: regionale samenwerking in informatiebeveiliging en privacy regio Noord-Holland | Marit Blom | Sigra

Marit Blom, manager Sigra expertisecentrum privacy & Informatieveiligheid voor zorg en welzijn deelt haar ervaringen (na 5 jaar AVG) over de regionale samenwerking rondom privacy en informatieveiligheid in de regio Noord- Holland. Hoe zorg je voor kennisdeling, kennisversnelling en een pragmatische werkwijze? Hoe creëer je draagvlak? En hoe ga je om met ethische dilemma’s?

Ransomware: de grootste (cyber)dreiging voor (zorg)ondernemend Nederland | Liesbeth Holterman | Cyberveilig Nederland

Bijna elke week zijn er wel nieuwsberichten waarbij organisaties worden geraakt door een ransomware-aanval. Criminelen blokkeren of versleutelen hierbij je computers, bestanden, of soms zelfs hele netwerken, en geven die pas weer vrij als je losgeld betaalt. Ook zorginstellingen zijn een interessante doelgroep voor criminelen: immers er gaan veel (bijzondere) persoonsgegevens in om en de dienstverlening mag niet stil komen te liggen. Tijdens de presentatie van Liesbeth Holterman, strategisch adviseur van Cyberveilig Nederland, zal ze ingaan op ransomware: wat is het, hoe gaan criminelen te werk en met welke maatregelen kan je een aanval voorkomen? Meer specifiek zal ze ingaan op het fenomeen data-exfiltratie bij een ransomware aanval, aangezien het wegsluizen van data steeds meer als effectief middel wordt ingezet door criminelen om slachtoffers alsnog te dwingen tot betalen. Tenslotte zal ze enkele ransomware voorbeelden in de zorg delen.

Best practices in cybersecurity | Robert Weedage | Cybersecurity specialist

Met meer dan 20 jaar ervaring, opgedaan binnen de politie en de (private)cybersecurity wereld, zal Robert Weedage vanuit meerdere perspectieven antwoord geven op de volgende vragen: Wat kun je doen om jouw bedrijf/organisatie weerbaarder te maken, welke verschuivingen vinden er momenteel plaats en wat is de impact als jij slachtoffer wordt?

Zo simpel kan het zijn: gehackt in seconden | Thijs van Ede & Jerre Starrink | Twente Hacking Squad

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.