



Technical Safety;

Tools, Wetten en Tips

Cybersecurity in OT

Donderdag 26 september 2024

16.00-19.00 uur

Inclusief interactief diner

Railcenter Amersfoort

Tijdens de tweede bijeenkomst in het Drieluik Technical Safety hebben we het over; Cybersecurity in OT. Een belangrijk thema tijdens het gebruik, het ontwerp én het onderhouden van assets. Want, hoewel digitalisering kan bijdragen aan efficiency- en productiviteitsverbetering, moet het wel veilig blijven.

Vershil IT en OT

Operationele Techniek (OT) omvat het sturen en beheren van industriële processen middels hard- en software-systemen. Terwijl IT zich voornamelijk richt op het waarborgen van de vertrouwelijkheid van informatie, richt OT zich voornamelijk op de beschikbaarheid en integriteit van systemen. Bovendien is continuïteit van de processen in het OT-domein van groot belang. Deze processen kunnen vaak niet zomaar worden gestopt of onderbroken zonder grote gevolgen.

Deelname is gratis en we kunnen 50 professionals een deelnameplek geven

**Indien je niet aanwezig bent zonder afmelding vooraf, brengen wij no-show kosten van €75,- in rekening*



Programma

Ontvangst en Welkom

Cyberweerbaarheid waarborgen

Carolien van der Vliet-Hameeteman, Cybersecurity Consultant bij TNO

Thomas Rooijackers, Cybersecurity Onderzoeker bij TNO

Als gevolg van de digitalisering ontwikkelen, bouwen, onderhouden en exploiteren we systemen die steeds meer ICT-technologie bevatten en verbonden zijn. Veel van deze cybersystemen worden gedurende vele jaren ontwikkeld, met als bijgevolg dat deze systemen kwetsbaarheden kunnen bevatten. Om de cyberweerbaarheid van deze systemen te waarborgen, is het essentieel om anders te ontwerpen en te ontwikkelen zodanig dat cybersecurity in alle fases van de levenscyclus wordt meegenomen.

Invloed van de EU-NIS2

Mark Bakker, Sales Director Service Line Industrial (OT) Cyber Security bij Applied Risk BV

De ingevoerde EU-regels voor cyberbeveiliging zijn geactualiseerd met de NIS2-richtlijn. Hierdoor is het bestaande rechtskader gemoderniseerd om bij te blijven met de toenemende digitalisering en de evoluerende cyber-dreigingen. Wat betekent dat voor je organisatie en hoe zorg je voor veilige remote access?

De effecten van de Cyber Resilience Act

Ruud Scholten, Accountmanager Cyber Security for Control Systems bij Croonwolter&dros

Vanuit Europa komt veel nieuwe security gerelateerde wetgeving op ons af de komende jaren. De NIS2 is hiervan het bekendste voorbeeld en is derhalve veel besproken vanwege haar impact op ondernemend Nederland. De komst van de CRA (Cyber Resilience Act) zal echter ook een enorme impact hebben. Wat betekent de CRA voor jou? Hoe bereid je hier op voor?

Cybersecurity; cruciaal voor de veiligheid

Sjors Both, Business Development Manager bij Soltegro

Het hanteren van een integrale ontwerp aanpak is cruciaal om complexe multidisciplinaire projecten binnen de gestelde kaders tot een goed einde te brengen. Ook aspecten zoals machineveiligheid en cybersecurity dienen integraal te worden meegenomen om de veiligheid te blijven borgen.

Afsluitend Interactief Diner

AANMELDEN