Hudson Cybertec biedt meerwaarde dankzij hands-on ervaring in cybersecurity

Trainingen in cybersecurity vergroten weerbaarheid

De wereld van cybersecurity staat voor diverse uitdagingen: AI, een oorlog op het Europese continent en nieuwe wet- en regelgeving. De zwakste schakel in de keten van cyberveiligheid is nog altijd de mens en daarom zijn trainingen in cybersecurity belangrijker dan ooit.

Er gebeurt veel op het gebied van cybersecurity, weten lead consultant Michael Theuerzeit en managing director Marcel Jutte, beiden werkzaam voor Hudson Cybertec. Jutte: "Er komt nieuwe wet- en regelgeving aan die belangrijk is voor industriële cybersecurity. De NIS2 volgt de huidige wetgeving op en dat betekent onder andere dat er nu vele duizenden bedrijven zijn die wettelijke verplichtingen krijgen met betrekking tot cybersecurity. Met de huidige wetgeving waren dat er enkele tientallen. Het zal dus een stuk drukker worden in de branche, omdat we ineens veel meer klanten zullen bedienen."

RED en CRA

Naast de NIS2 komt er ook een nieuwe RED (Radio Equipment Directive) aan die cybervoorschriften bevat voor alle apparaten waar een antenne op zit, of anderszins draadloos informatie uitwisselen. Jutte: "Binnen de OT hebben we steeds meer apparatuur die draadloos functioneert: voor die apparatuur wordt de RED ook relevant."
Ook de CRA (Cyber Resilience Act) komt eraan en zal verplichtingen stellen aan bedrijven om hun cybersecurity door de keten heen te managen. "Kortom, een hoop nieuwe, belangrijke wetten en regels", concludeert Jutte.

AI vergroot aanvalsvlak

Een andere belangrijke ontwikkeling heeft te maken met kunstmatige intelligentie. Theuerzeit,: "Artificial Intelligence wordt nu nog niet of nauwelijks ingezet om processen te managen, maar ik verwacht dat we op termijn hier zeker een enorme groei zullen zien. Wat AI nu al heel relevant maakt voor cybersecurity is

dat aanvallers AI kunnen inzetten om een aanval voor te bereiden. Als je op dit moment aan ChatGPT vraagt om de code van bijvoorbeeld malware te schrijven, zal je dat niet direct krijgen, maar als je middels een omweg vraagt naar hoe een bepaalde kwetsbaarheid uitgebuit kan worden, zal je middels AI toch wel degelijk code kunnen krijgen die je eventueel zou kunnen inzetten bij cyberaanvallen. ChatGPT is nu nog een beetje spielerei, maar AI wordt in hoog tempo steeds geavanceerder en zal dus ook cybersecurity voor steeds grotere uitdagingen stellen. Je moet er ook rekening mee houden dat AI een rol zal gaan spelen in social engineering. Je kunt nu al 'deep fake' filmpjes vinden van een minister-president die een raar dansje uitvoert, of een staatshoofd of andere kopstukken die uitspraken doen die ze in werkelijkheid nooit zouden doen. Deze filmpjes zijn nu soms al bijna niet van echt te onderscheiden. Vertaal dat naar een fabriek en dan kan het zijn dat je een videocall krijgt van je leidinggevende die je vraagt een bepaalde handeling uit te voeren. Dat blijkt dan compleet fake te zijn. We staan eigenlijk nog maar aan het begin van deze revolutie. Je zou kunnen concluderen dat door AI het aanvalsvlak exponentieel toeneemt."

Target, ja of nee?

"Vergeet ook vooral niet dat de oorlog in Oekraïne invloed heeft op de manier waarop we tegen cybersecurity aankijken", vult Jutte aan. "Je merkt dan meteen dat er allerlei bedrijven om advies vragen. Ben je nu wel of geen target of het moment dat er niet zo gek veel naar het oosten toe een oorlog uitbreekt?"

"Personeel dat onbewust onbekwaam is en veel toegang heeft tot digitale omgevingen, is de achilleshiel van je cybersecurity

Ook de energietransitie heeft invloed op cybersecurity. Theuerzeit: "Zonnepanelen leveren ook cyberkwetsbaarheden op. Op het moment dat je zonnepanelen thuis op het elektriciteitsnet aansluit en die ook met een app kunt laten uitlezen, moet je je afvragen hoe veilig dat is."

Trainingen

Cybersecurity wordt steeds belangrijker, niet alleen omdat het aanvalsvlak groter wordt, maar ook omdat er steeds meer regelgeving komt. En daarom worden trainingen in cybersecurity steeds belangrijker, weet Jutte: "Het zit hem voor een groot deel in de nieuwe wet- en regelgeving, zoals de reeds genoemde NIS2, de CRA en de RED. Er is een steeds grotere behoefte aan cybersecurity kennis in de markt, zowel in Nederland als daarbuiten. Dat laatste is voor internationaal opererende bedrijven belangrijk."
Bedrijven zullen zich steeds vaker moeten oriënteren op hun eigen cybersecurity, meent Theuerzeit: "De eerste vraag die dan vaak gesteld wordt is: wat moet daar aan worden verbeterd zodat ik 'in control' ben? Vaak komen die bedrijven uit bij de IEC62443. Maar wat moeten ze dan met die norm, hoe werkt dat? En daar komen onze trainingen dan boven drijven."

Managing director Marcel Jutte: "Binnen de OT hebben we steeds meer apparatuur die draadloos functioneert: voor die apparatuur wordt de RED ook relevant."

"ChatGPT is nu nog een beetje spielerei, maar AI wordt in hoog tempo steeds geavanceerder en zal dus ook cybersecurity voor steeds grotere uitdagingen stellen"

Aantoonbaar in control

Hudson Cybertec verzorgt al meer dan tien jaar trainingen in cybersecurity. Twee jaar geleden schaarde Hudson Cybertec zich onder de Kiwa vlag en dat zorgde er voor dat die trainingen uitgebreid werden naar meer klanten en meer sectoren. Bovendien is Kiwa de aangewezen partij om certificeringen op de norm uit te schrijven. "Dat maakt onze trainingen nog waardevoller", meent Jutte."Op dit moment wordt het trainingsportfolio internationaal uitgerold met Kiwa. Die certificering wordt steeds belangrijker. Bedrijven moeten aantoonbaar in control zijn: ook daar komen nieuwe normdelen voor. Je moet weten wat voor bewijslast je moet kunnen leveren om aan die nieuwe normdelen te voldoen. Hoe maak je aannemelijk als organisatie dat je echt in control bent? Dat soort zaken leren mensen tijdens onze trainingen." Theuerzeit: "Onze trainingen zijn daarnaast ook flexibel: die gaan met de ontwikkelingen mee. Zo komt nu de rol van IoT vaker aan bod: hoe zorg je er voor dat je binnen je OT-omgeving op een veilige manier met IoT devices omgaat? Daar komt binnenkort weer een nieuw normdeel voor."

Bepalende factor

Bij cybersecurity trainingen wordt altijd gekeken naar de klassieke mens-organisatie-techniek driehoek. Jutte: "De IEC62443 is ook op die manier ingericht.

Lead consultant Michael Theuerzeit: "Onze trainingen zijn flexibel: die gaan met de ontwikkelingen mee."

Men denkt vaak dat de techniek de bepalende factor is in de totale cybersecurity, maar het is toch echt de mens die de bepalende factor is. Personeel dat onbewust onbekwaam is en veel toegang heeft tot digitale omgevingen, is de achilleshiel van je cybersecurity."

De bewustwording met betrekking tot cybersecurity is de afgelopen jaren fors toegenomen, weet Jutte. "Inmiddels weet men overal wel dat je cybersecurity serieus moet nemen. Je komt soms nog wel kleine bedrijven tegen die er nog te weinig mee bezig zijn." Bedrijven die grote, kritische processen hebben draaien, zijn zich doorgaans bewust van de risico's die ze lopen. Toeleveranciers worstelen hier soms nog mee, weet Theuerzeit. "Er wordt nog wel gestoeid met de vraag in hoeverre een toeleverancier verantwoordelijk is voor de cybersecurity rondom zijn product, wanneer dat product een aantal stappen verder in de keten pas ergens wordt gebruikt. De RED en CRA en de NIS2 zullen die vraag vergemakkelijken, want deze regelgeving kijkt naar de hele keten. De IEC62443 kijkt ook naar de keten, maar de verantwoordelijkheid houdt op bij jouw stukje van die keten. Daarom is het goed dat er regels komen die over die grenzen heen kijken."

Te vroeg of te laat?

Theuerzeit benadrukt dat het niet zo is dat toeleveranciers hun eigen cybersecurity helemaal niet op orde hebben: "Het gaat echt over de verantwoordelijkheid in de hele keten. Er is vrijwel geen enkele industriële toeleverancier meer die cybersecurity niet serieus neemt. Kijk, heel praktisch: sommige toeleveranciers hebben nu de mogelijkheid om extra features in hun product te bouwen waardoor het product een hogere mate van cyberveiligheid krijgt. Doe je dat als bedrijf

als die vraag of verplichting er nog niet is en maak je daarmee je product duurder dan de concurrent, of wacht je tot er een wettelijke verplichting is om die features in te bouwen, maar ben je er dan misschien te laat mee?"

CSIR

En soms gaan partijen nog verder dan het toepassen van de voorgeschreven richtlijnen. Jutte: "Kijk naar een partij als Rijkswaterstaat: die heeft zelfs z'n eigen cybersecurity richtlijn opgesteld (de CSIR), die bestaat inmiddels tien jaar. Afgelopen jaren hebben wij een bijdrage geleverd aan het actualiseren van die richtlijn. In de CSIR zit de IEC62443 ingebouwd, maar het gaat verder dan dat. Ook waterschappen gaan deze richtlijn gebruiken en er is interesse vanuit provincies en gemeentes."

Bijhouden

De trainingen die door Hudson worden verzorgd, vinden plaats bij allerlei soorten bedrijven.
Theuerzeit: "Denk aan toeleveranciers die industriële sensoren bouwen, tot aan system integrators die vaak vanuit hun klanten te maken krijgen met vragen over cybersecurity. Maar ook asset owners die zelf aan de slag willen met cybersecurity of aan de slag blijven met cybersecurity. Het is namelijk echt een proces: als je je cybersecurity op orde hebt, ben je er niet vanaf. Je moet het bijhouden."

OT en IT

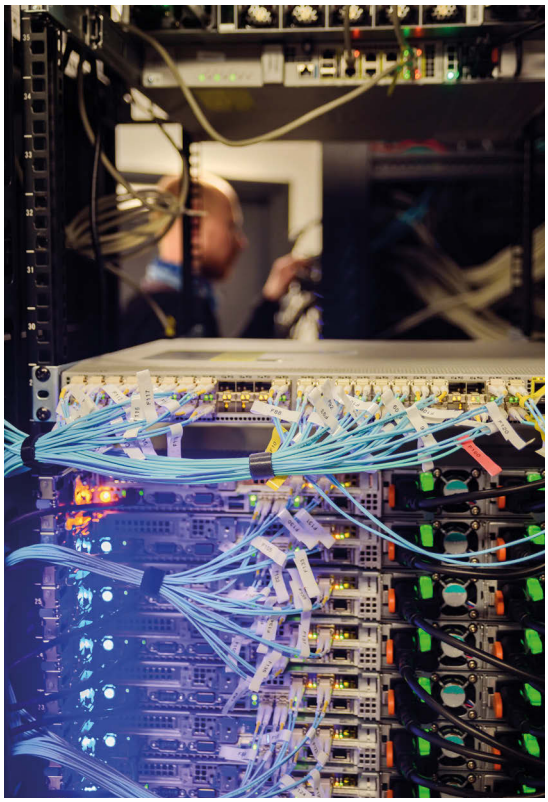
Hoewel Hudson Cybertec gespecialiseerd is in OT cybersecurity, wil dat niet zeggen dat IT-cybersecurity daar helemaal los van staat. Theuerzeit: "Er zijn situaties waar we bij een bedrijf komen dat z'n IT cybersecurity helemaal op orde heeft, maar waarbij er aan de OT-kant heel wat aan schort. Maar het komt ook voor dat we het kantoor meenemen in de OT-cybersecurity."

Toen cybersecurity een punt van aandacht werd, schoten bedrijven die 'iets met cybersecurity' deden als paddenstoelen uit de grond. Anno 2023 is dat eigenlijk nog steeds zo. Jutte: "Cybersecuritybedrijven die de IT beveiliging bij een klant op orde hebben gebracht en in de vergaderkamer de vraag krijgen of ze ook de OT kunnen regelen, zeggen vaak ja. Maar OT cybersecurity is echt een apart specialisme. We komen helaas nog steeds bij bedrijven over de vloer waar men geprobeerd heeft de OT cybersecurity op orde te krijgen, maar waarbij het niet echt geslaagd is vanwege de IT-bril waarmee dit is gedaan. Voor zo'n bedrijf is het duurder om door ons de rommel te laten opruimen, dan dat wij het in één keer goed zouden hebben kunnen doen."

Zelf in de praktijk

Die OT hands-on ervaring van Hudson onderscheidt het bedrijf van andere bedrijven, waar niet dagelijks in de praktijk wordt gewerkt aan cybersecurity uitdagingen in de OT.
Theuerzeit: "Eigenlijk is het wel opmerkelijk dat in een branche die van certificeringen en normen aan elkaar hangt, in principe elk bedrijf trainingen en advies mag geven in (OT) cybersecurity. Er valt best wat voor te zeggen om daar ook gecertificeerd voor te moeten worden. Je zou daar het prutswerk dat wij in de praktijk soms tegenkomen, gemakkelijk mee kunnen besparen."

Kennis over cybersecurity haal je niet uit een boekje, vindt ook Jutte: "Je moet echt in de praktijk zitten om bij te blijven. Alleen dan hoor je de verhalen over hoe een hack toch geslaagd is, of een incident juist is voorkomen. Dat is wat mij betreft ook dé reden om een cybersecurity ondersteuning in te winnen of training te volgen bij een bedrijf dat zelf diep in die praktijk zit."
Over kennis gesproken, ook de cyberspecialisten van Hudson moeten hun kennis up to date houden. Jutte: "Enerzijds halen we die uit de alledaagse praktijk waarin we werken, anderzijds zitten we in werkgroepen, in constellaties waarin we met elkaar discussiëren, maar we doen zelf uiteraard ook mee aan trainingen en seminars."



"We komen helaas nog steeds bij bedrijven over de vloer waar men geprobeerd heeft de OT cybersecurity op orde te krijgen, maar waarbij het niet echt geslaagd is vanwege de IT-bril waarmee dit is gedaan"