Hudson Cybertec biedt meerwaarde dankzij hands-on ervaring

Trainingen in cybersecurity vergroten weerbaarheid

Door Joeri van der Kloet

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 cybersecurity in de watersector en de industrie. De Europese NIS2-richtlijn (Second Network and Information Security directive, red.) leidt tot aanscherping van de huidige Wbni-wetgeving (Wet beveiliging netwerk- en informatiesystemen, red.) 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.”

Drinkwaterbedrijven moeten nu al voldoen aan de NIS2 en de Wbni, omdat ze onderdeel uitmaken van de vitale infrastructuur. “Maar daar komen nu ook de waterschappen en andere bedrijven bij”, verduidelijkt Jutte.

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 omgeving van de operationele technologie (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 die zal verplichtingen stellen aan bedrijven om hun cybersecurity door de keten heen te managen. “Kortom, een hoop nieuwe, belangrijke wetten en regels”, concludeert Jutte.

Drinkwaterbedrijven hebben hun OT-cybersecurity volgens Hudson Cybertec meestal goed op orde. Zij worden daar op geauditeerd en de Vewin faciliteert controles. Op de foto de regelkamer van drinkwaterbedrijf Vitens in Zwolle (foto: Vitens).

AI vergroot aanvalsvlak

Een andere belangrijke ontwikkeling heeft te maken met de snelle opkomst van 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

Cybersecurity voor een breder publiek

Om de cybersecurityrichtlijn van Rijkswaterstaat (CSIR) gebruiksklaar te maken voor een breder publiek, heeft het Waterschapshuis Hudson Cybertec gevraagd de CSIR (versie 2.0) te veralgemeniseren tot een versie 3.0. Hierbij zijn alle RWS-specifieke zaken vervangen door in bredere context bruikbare teksten. Deze veralgemenisering maakt de CSIR bruikbaar voor alle partners in het Bestuursakkoord Water, ongeacht of zij ontwikkelingen van de IA-omgeving in eigen beheer uitvoeren, of uitbesteden aan een externe partij.

De BIACS (Basismaatregelen voor cybersecurity van Industriële Automatisering & Controle Systemen) gebruikt de structuur van de CSIR en biedt basisvereisten voor het verbeteren van de digitale weerbaarheid. Hierdoor is een set met no-regret maatregelen ontstaan en biedt de BIACS vanwege de gelijke structuur bedrijven de mogelijkheid later door te stappen naar de CSIR. De BIACS is veel simpeler van opzet, zodat ook organisaties met een gemiddeld volwassenheidsniveau ermee uit de voeten kunnen.

schrijven, zal je dat niet direct krijgen, maar als je middels een omweg vraagt naar hoe een bepaalde kwetsbaarheid uitgebuit kan worden, zal je via AI toch wel degelijk code kunnen krijgen die je kan inzetten bij cyberaanvallen. Je kunt concluderen dat door AI het aanvalsvlak exponentieel toeneemt."

"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 aan de rand van Europa een oorlog uitbreekt?" Het is ook niet gek dat de NIS2 en daarmee de Wbni ook al een verplichting is voor drinkwaterbedrijven, meent Jutte: "Die bedrijven behoren tot de vitale infrastructuur. Bij een geslaagde aanval op een drinkwaterbedrijf heb je echt een probleem."

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

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, Wbni, de CRA en de RED. Er is een steeds grotere behoefte aan cybersecuritykennis in de markt, zowel in Nederland als daarbuiten."

Hudson Cybertec verzorgt al meer dan tien jaar trainingen in cybersecurity. Twee jaar geleden schaarde het zich onder de Kiwavlag en dat zorgde ervoor dat die trainingen werden uitgebreid 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. 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 Internet of Things vaker aan bod: hoe zorg je ervoor dat je binnen je OT-omgeving op een veilige manier met IoT-devices omgaat? Daar komt binnenkort weer een nieuw normdeel voor."

Bij cybersecurity trainingen wordt altijd gekeken naar de klassieke driehoek mens-organisatie-techniek. Jutte: "Men denkt vaak dat de techniek de bepalende factor is in de totale cybersecurity, maar het is toch echt de mens. Personeel dat onbewust onbekwaam is en veel toegang heeft tot digitale omgevingen, is de achilleshiel van je cybersecurity."

CSIR en BIACS

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 cybersecurityrichtlijn opgesteld: de Cybersecurity Implementatierichtlijn objecten RWS (CSIR). Die bestaat inmiddels tien jaar. Afgelopen jaren hebben wij een belangrijke bijdrage geleverd aan het actualiseren van die richtlijn. Ook waterschappen gaan

deze richtlijn gebruiken en er is interesse vanuit provincies en gemeentes. Daarnaast heeft Hudson Cybertec voor het ministerie van IenW de BIACS ontwikkeld. Dit kader beschrijft de Basismaatregelen voor de cybersecurity van Industrial Automation & Control Systems. Organisaties krijgen hiermee een handreiking om de basisweerbaarheid van hun OT omgeving op orde te brengen. De BIACS is bedoeld voor organisaties met een gemiddeld volwassenheidsniveau die de CSIR te uitgebreid vinden en een eenvoudiger securitykader willen gebruiken."

OT en IT

Hudson verzorgt trainingen bij allerlei soorten bedrijven. Hoewel het gespecialiseerd is in OT-cybersecurity, wil dat niet zeggen dat IT-cybersecurity daar helemaal los van staat. Theuerzeit: "Soms komen we bij een bedrijf 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. Drinkwaterbedrijven hebben hun OT-cybersecurity veelal goed op orde. Zij worden daar op geauditeerd door externe partijen en ook de Vewin faciliteert dergelijke controles."

Marcel Jutte:
"Binnen de OT hebben we steeds meer apparatuur die draadloos functioneert: voor die apparatuur wordt de Radio Equipment Directive ook relevant."

Onder de waterschappen is er meer variatie als het gaat om OT-cybersecurity, weet Jutte: "Er zijn waterschappen die hun OT-cyberveiligheid volledig uitbesteden. Dan moet je zeker weten dat die partij echt goed weet wat hij doet. Door die OT-veiligheid uit te besteden, verlies je voor een deel de grip op je cybersecurity. Zo kan het zijn dat je externe partner wat laks is met het verlenen van toegang tot je systeem. Dan loop je als waterschap dus meer risico dan je zou willen."

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 cybersecurityuitdagingen 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 daarvoor ook gecertificeerd te moeten worden. Je zou daar het prutswerk dat wij in de praktijk soms tegenkomen, gemakkelijk mee kunnen vermijden."