Hudson Cybertec

'ORGANISATIES MOETEN AANTOONBAAR IN CONTROLE ZIJN ÉN BLIJVEN'

Tekst: Mels Dees

Waar berichten in de media over hackers en virussen duidelijk maken hoe belangrijk het beveiligen van IT-omgevingen is, daar krijgt cybersecurity bij Operationele Technologie veel minder aandacht. Ten onrechte, want de gevolgen van een incident kunnen groot zijn.

De verschillen tussen OT en generieke IT worden vaak onvoldoende onderkend, weet Michael Theuerzeit, lead consultant bij Hudson Cybertec. "Operationele Technologie is een ander domein met andere consequenties als er verstoringen optreden. Als met de IT iets fout gaat, dan kost dat in het slechtste geval de kop van de ceo of van de cfo, maar er vallen geen doden of gewonden."
Bij cybersecurityproblemen binnen de OT kunnen ongewenste emissies van gassen, schadelijke lozingen van vloeistoffen of explosies het gevolg zijn. "Dat kan impact hebben op de natuur, of op het welzijn van mensen", geeft Theuerzeit aan. "Er is dan echt sprake van fysieke impact, en dat maakt OT zo anders dan IT."
Bedrijven automatiseren immers om iets in de fysieke wereld gedaan te krijgen. "Om een object te bewegen. Of om een product te maken. Of om een proces te kunnen begeleiden, zoals het doorlopen van een raffinageproces."
De impact van, bijvoorbeeld, een cyberaanval kan daarom groot zijn. "De kans is aanwezig dat de onderneming dan geen controle meer heeft op de primaire processen, met alle gevolgen van dien." Het is om die reden van groot belang dat ondernemingen aantoonbaar in control zijn - en blijven.
Om kwetsbaarheden op te sporen en adequaat beleid te kunnen opstellen, ontwikkelde Hudson Cybertec, een hard groeiende internationaal opererende Nederlandse onderneming, met OT Insight een monitoring-oplossing.


Marcel Jutte


Michael Theuerzeit

Nulmeting
Om in control te zijn en te blijven, begint het ermee dat een bedrijf exact moet weten welke processen er

Foto: Danny Cornelissen

Vaak zijn organisaties verrast als ze met de uitkomsten van de meting worden geconfronteerd

in de organisatie lopen, door welke mensen die worden verzorgd en met welke apparatuur. “Een nulmeting is van groot belang en de uitkomsten ervan bepalen de te nemen maatregelen”, geeft Marcel Jutte, oprichter en managing director van Hudson Cybertec aan. Daarbij komen de aspecten mens, organisatie en techniek nadrukkelijk aan de orde. “We halen alle voor OT relevante kwetsbaarheden in de organisatie boven water”, stelt Theuerzeit.

Vaak zijn organisaties verrast als ze met de uitkomsten van de meting worden geconfronteerd. Zo wordt binnen OT vaak apparatuur of software gebruikt die niet meer actueel is, wat zorgt voor kwetsbaarheden. Daar zijn de verantwoordelijken zich niet altijd van bewust.

“Aan de hand van de uitkomsten van de nulmeting stellen we aanpassingen voor en schrijven met de klant aan adequaat beleid. Gezamenlijk wordt dan naar de inrichting van de OT-omgeving en naar cybersecurity gekeken”, legt Theuerzeit uit. “Een bedrijf moet digitaal weerbaar zijn en blijven.”

Assetmanagement is van groot belang om tot een goede risico-inventarisatie te komen, weet de lead-consultant, net als monitoring, waarvoor dan OT Insight wordt ingezet. “Ook moet je de supply chain goed kennen waarvan de onderneming deel uitmaakt.”

Dit laatste is onder meer relevant om te kunnen bepalen waar gegevens (data) naartoe gaan. Blijven die in Nederland, of is ook sprake van verwerking of opslag in het buitenland, en zo ja, zelfs buiten Europa? “En wanneer processen worden uitbesteed, moet je weten hoe de system integrator omgaat met security.”

Aan de hand van de nulmeting kan een organisatie, in overleg met Hudson Cybertec, aan de hand van een plan de digitale weerbaarheid verhogen en zorgen dat relevante normen worden nageleefd, waarbij vooral de internationale norm IEC 62443 (‘Cybersecurity voor Industriële Automatisering & Controle Systemen’) leidend is.

Certificering

Veelvuldig helpt het bedrijf waarvoor Theuerzeit werkt de betreffende organisatie zich voor te bereiden op het proces van certificering. “We verzorgen daarbij een pre-audit en lopen met de onderneming het hele proces door. Daarbij kunnen we nauwkeurig aangeven waar afwijkingen optreden en hoe die opgelost moeten worden.”

Sinds kort maakt Hudson Cybertec onderdeel uit van de Kiwa groep, specialist in certificering. “Er is sprake van een zogeheten ‘Chinese Wall’ tussen onze activiteiten en die van Kiwa als het aankomt op de daadwerkelijke certificering waardoor onafhankelijkheid is gegarandeerd”, benadrukt Theuerzeit.

Certificering zorgt ervoor dat een onderneming kan aantonen in control te zijn. “Dat wordt steeds belangrijker”, weet Jutte. “Steeds vaker zien we strengere eisen aangaande cybersecurity van opdrachtgevers aan leveranciers. Maar ook voor het voldoen aan wet- en regelgeving, kunnen bedrijven aangeven dat ze in control zijn.”

INTERNET OF THINGS ALS NIEUWE UITDAGING

Internet of Things (IoT) wordt vaak gezien als iets nieuws, maar eigenlijk vormt het al langere tijd een onderdeel van OT. “Wat we wel zien is dat er steeds meer slimme devices in het OT-domein komen”, vertelt Michael Theuerzeit. “Vaak zit er zelfs een webserver in en veel apparaten, sensoren en dergelijke hebben verbinding met elkaar tot aan verschillende clouddiensten aan toe. Dat betekent dat we te maken hebben met hyperconnectivity.” De kans is groot dat niet goed beveiligde apparaten zich in het netwerk bevinden. “Vaak is cybersecurity een beetje een ondergeschoven kindje bij deze devices. Daar moeten organisaties zich van bewust zijn. Je moet de beveiliging en updates managen en meenemen in het kwetsbaarhedenmanagement.”