“Veel bedrijven zijn onbewust onbekwaam als het gaat om cybersecurity”

Te weinig aandacht voor cyberveiligheid in industrie

Cybersecurity is voor velen nog steeds abacadabra en moeilijk te herkennen. Waarom wordt bijvoorbeeld een vent met bivakmuts en koevoet direct opgepakt, terwijl een verzorgde vrouw met een USB met malware veel meer schade kan toebrengen? Marcel Jutte snapt heus wel het mechanisme erachter, maar is realistisch. De cybersecurity-specialist van Hudson Cybertec ziet dat er in de maakindustrie nog te weinig aandacht is voor cyberveiligheid van de hele fabriek.

Jutte wil het helemaal niet over IT hebben. De crux ligt volgens de directeur van Hudson Cybertec namelijk bij OT: Operationele Technologie. Je zou het verschil tussen IT en OT kunnen zien met hoe een fabriek werkt. IT is vooral op software berust, binnen de OT speelt het hardwarecomponent een belangrijke rol. Denk dan aan SCADA, Remote Terminal Units, Smart Meters/Sensors die de fabriek aansturen.

SCADA? OT? Het zijn termen die binnen de maakindustrie bekend zijn, maar nog lang niet altijd een belangrijke rol spelen. Ten onrechte, vindt Jutte. Zijn bedrijf Hudson Cybertec is een leveranciersonafhankelijke cybersecurity solution provider, die wereldwijd betrokken is bij cybersecurity-trajecten voor de operationele technologie. Hij introduceert na alle termen en afkortingen het volgens hem belangrijkste acroniem van alle automatiseringslingo: IACS, kort voor Industriële Automatisering & Controle Systemen.

ZWEEP

Jutte is niet de eerste de beste binnen de cyberveiligheid voor de industrie. Van origine is hij procesautomatiseerder en hij kent al dertig jaar de ins en outs van IACS en cybersecurity. Hij is docent en spreker op dit gebied en medeontwikkelaar van de standaard IEC 62443. Deze cybersecurity-standaard voor Industriële Automatisering & Controle Systemen is een wereldwijd erkende en ondersteunde standaard die specifiek ontwikkeld is voor dit domein. De standaard biedt een solide basis voor het managen van cybersecurity binnen het IACS-domein. Er zijn verschillende delen binnen de standaard die elk een apart gebied afdekken. Zo zijn er delen waarmee eindgebruikers hun voordeel kunnen doen, maar er zijn ook delen waaraan juist systeemintegratoren en leveranciers veel hebben. Door het omarmen van de standaard kunnen allen binnen hun eigen discipline bijdragen aan het verhogen van de veiligheidsniveaus, waarbij de standaard een uniforme communicatie tussen de verschillende partijen faciliteert.

Hudson Cybertec is een zogenoemde cybersecurity solution provider voor de operationele technologie (OT). “Wij helpen bedrijven met het op orde krijgen en houden van cybersecurity voor de primaire processen. We hebben speciaal aandacht voor IACS. Dat houdt onder andere in dat we waken over de veiligheid bij bijvoorbeeld een DCS. Dat is een distributed control system en die worden gebruikt in industriële en civieltechnische toepassingen om een proces te volgen, te sturen en te controleren. Ook PLC’s (programmable logic controller, een ‘pc’ waarmee je machines aanstuurt), HMI’s (mens-machine-interface), SCADA-systemen, industriële netwerken en instrumentatie pakken we aan. We zijn daar waar de technische installaties essentieel zijn voor de primaire bedrijfsvoering.”

OLIFANT

Jutte vervolgt: “We werken onafhankelijk van leveranciers en onderscheiden ons dankzij onze ervaring en expertise. Daarnaast kom ik zelf uit de procesindustrie; ik spreek de taal van de industrie. Ik ken de cultuur.”

Veel partijen in de productietechnologie zijn toeleveranciers. “Je kan als eindklant volledig cybersecure zijn, maar zijn de toeleveranciers dat ook? Dan hebben we het over system integrators, installateurs, ingenieursbureaus, contractors en fabrikanten. Vaak zijn het mkb’ers. Als voorbeeld noem ik een leverancier van lasrobots. Zo’n partij heeft alle verstand van lassen en hoe de robot daarbij in te zetten. Maar van cybersecurity hebben ze bij zo’n onderneming geen kaas gegeten. Als kleiner bedrijf denk je bij processen bijvoorbeeld aan salarisadministratie, personeelsplanning, enzovoort. Maar niet aan cybersecurity. Bedrijven investeren wel in efficiëntere machines en het snoeien in kosten, maar OT-beveiliging is bij sommige bedrijven een olifant in de kamer.”

Hij ziet dat met name bij de vitale infrastructurele bedrijven (drinkwater en chemie bijvoorbeeld), de eisen strenger worden. “Daar komen geen vreemde ICT-producten binnen. Dat een leverancier met een eigen server of pc aankomt, is onmogelijk. Als je niet compliant bent aan de bestaande ICT en de bijbehorende beveiliging, mag je niet eens meedoen aan een aanbesteding. In de procurement-fase wordt die eis al gesteld.”

Wat is dan de taak van Hudson Cybertec binnen de maakindustrie? “We willen de maakindustrie ontzorgen. Vaak is het een familiebedrijf, waar vader bijvoorbeeld de directeur is, moeder zorgt voor de personeelsplanning en dochter op de administratie zit. Van daaruit zijn ze verder gegroeid. De systeembeheerder is iemand uit het dorp. Dat werkt prima, tot een bepaald punt. Tegenwoordig zijn machines IT-systemen geworden, vaak onbedoeld en ongewenst direct gekoppeld aan het internet. Dit soort bedrijven is zeer kwetsbaar voor cybercriminaliteit.”

Hudson Cybertec heeft een specifieke aanpak voor het mkb, waarbij deze ontzorgd worden op het gebied van cybersecurity. “We maken een quick scan van een onderneming. Daar kijken we hoe het is gesteld met de internetveiligheid van een bedrijf. Hebben de mensen het juiste opleidingsniveau? Wie heeft toegang tot wat? En hoe? Kan ik via de machine bij de pc van de administratie binnenkomen?”

Hudson Cybertec voert daarnaast een zogenoemde pentest (binnendringingstest) uit. Dit is een toets van een of meer computersystemen op kwetsbaarheden, waarbij deze kwetsbaarheden ook werkelijk gebruikt worden om in deze systemen in te breken. De resultaten komen in een rapport, dat helpt om voldoende maatregelen te treffen. Hudson Cybertec kan helpen met de implementatie van deze maatregelen en periodieke scans uitvoeren zodat het cybersecurity-niveau optimaal blijft.

> **“HET IS MAKKELIJKER OM TE INVESTEREN IN HET TE PAKKEN KRIJGEN VAN DE BLUEPRINTS VAN EEN CONCURRENT DAN HET ZELF TE ONTWIKKELEN”**

De nieuwe Cybersecuritywet (NIB)

De Europese Netwerk- en InformatieBeveiliging (NIB)-richtlijn heeft als doel om in de gehele EU alle belangrijke voorzieningen zoals energie, zorg en drinkwater voldoende te beschermen tegen cyberaanvallen. Deze NIB-richtlijn is nu in Nederlandse wetgeving via de Wet beveiliging netwerk- en informatiesystemen (Wbni) omgezet.

Alle organisaties die door de Minister van J&V als ‘vitaal’ worden aangewezen moeten aan de nieuwe wet voldoen. Welke organisaties zullen dat zijn? Dit zal uiterlijk per 9 november 2018 duidelijk zijn. Logischerwijs in ieder geval de organisaties die nu reeds als vitaal zijn aangewezen onder de WGMC. De NIB-richtlijn heeft echter een veel bredere scope en andere definities. Bijvoorbeeld: centraal bij een cyberincident staat dat het niet alleen gaat om de gevolgen voor de continuïteit, maar ook om integriteit, authenticiteit en vertrouwelijkheid. Het ligt daarom voor de hand dat aan de lijst van ‘vitaal’ ook andere organisaties worden toegevoegd en daarmee onder de scope van de cybersecurity-wet komen te vallen.

Organisaties moeten ervoor zorgen dat hun informatiebeveiliging op orde is; door ‘passende technische en organisatorische maatregelen’. Daarnaast geldt er, in het geval van een ernstig cyberincident, voor alle organisaties een meldplicht. Voor aanbieders van essentiële diensten (AED’s) en digitale service providers (DSP’s) geldt een dubbele meldplicht: zowel bij het NCSC als bij de toezichthouder.

Foto: Shutterstock.com

SPIONAGE

Hoe groot is het probleem? “Veel groter dan mensen denken”, zegt Jutte. “Het gaat er namelijk niet alleen om hoe vaak een systeem wordt aangevallen. Ddos-aanvallen kan je als kwaadwillende gewoon kopen. Ransomware? Er zijn genoeg voorbeelden van. Maar stel je voor dat je een toeleverancier bent voor vitale infrastructuren, bijvoorbeeld een kerncentrale. Je wilt niet dat het fout gaat. En neem cyberspionage, dat is een nog lang niet voldoende onderkend probleem. Het is makkelijker om te investeren in het te pakken krijgen van de blueprints van een concurrent dan het zelf te ontwikkelen. Een voorbeeld: de Range Rover Evoque reed eerder in China dan in Groot-Brittannië. Maar dan niet onder de naam van Range Rover, maar wel met de blueprints van Range Rover.”

Ja, er is meer bewustwording in de markt, ook in de maakindustrie. Maar dat ebt volgens Jutte ook weer weg. “Dat gebeurt met alles. Veel bedrijven zijn onbewust onbekwaam als het gaat om cybersecurity. Men gaat er van uit: onze IT-man is een goede vent. Hij doet altijd zijn best. Maar vergeet niet dat hij de deur van de serverruimte in de zomer open laat staan om het te laten ventileren. Dat is de eerste stap in cyberveiligheid: een slot van 17,50 euro op je serverruimte.”