“Cybersecurity is een proces, het is nooit af”

Josephine van Luik (CWM) en Marcel Jutte (IPCS) over cyberweerbaarheid van de maakindustrie

Bij cybersecurity gaat het meestal over IT, zeg maar kantoorautomatisering. Aandacht voor de fabrieksautomatisering, of operationele technologie (OT), is er veel minder, zeker bij de kleinere mkb-bedrijven. Als spelers in een industriële keten moeten ze echter wel werk maken van hun digitale beveiliging. Het Cyberweerbaarheidscentrum Maakindustrie Zuid-Holland (CWM) is dan een goed aanspreekpunt. “Dat kan helpen om de basishygiëne voor OT-cybersecurity op orde te krijgen.”

35 jaar ervaring in OT

Marcel Jutte is al 35 jaar actief in de wereld van industriële automatisering en operationele technologie (OT) en heeft zich gaandeweg toegelegd op cybersecurity. Zo is hij voorzitter van het Industrieel Platform Cyber Security (IPCS), dat meer dan vijftig specialisten in OT-cybersecurity bundelt. “Wij organiseren werkbezoeken aan kritische infrastructuur, zoals energiecentrales, en hebben werkgroepen die actuele onderwerpen oppakken en daar whitepapers over schrijven. Ook zijn we betrokken bij diverse overheidsinitiatieven. Ik zit bijvoorbeeld in de stuurgroep van de OT Coalitie voor digitale weerbaarheid van industrial automation and control systems.”

www.cwmaakindustrie.nl

www.securitydelta.nl/ipcs

Digitale beveiliging van OT is een ondergeschoven kindje in de maakindustrie. Dat geldt in ieder geval voor de doelgroep van het CWM, zegt Josephine van Luik. “Bij de kleinere mkb-bedrijven is er nog onvoldoende bekendheid met cybersecurity en weinig zicht op de risico’s.” Marcel Jutte vult aan: “Bij het platform IPCS zien we dat de beheerders van de vitale infrastructuur het voor zichzelf wel op orde hebben, maar zij zijn weer afhankelijk van mkb’ers. Die houden zich bezig met hun primaire proces en voor hen is cybersecurity een noodzakelijk kwaad. Ze moeten er wel wat aan doen omdat hun opdrachtgevers ernaar vragen vanwege nieuwe regelgeving.”Van Luik: “Maar ze missen de kennis en maken ook geen budget vrij om met het onderwerp aan de slag te gaan, omdat er veel andere prioriteiten spelen. Ze komen nu wel met vragen over de nieuwe NIS2-richtlijn (de Network and Information Security directive, gericht op grote en middelgrote organisaties in een breed scala aan sectoren die als essentieel of belangrijk worden beschouwd voor de samenleving en economie) en de Cyber Resilience Act, die echt ingaat op de veiligheid van producten met digitale componenten en vijfjarige levenscyclus. Wij ondersteunen bedrijven door cybersecurity onder de aandacht te brengen en de awareness rond digitale risico’s te vergroten. Dat doen we onder meer met kennissessies en workshops, waarbij we organisaties ook een concreet handelingsperspectief bieden. Wanneer bedrijven zich bij ons aansluiten, starten we met een nulmeting. Daarbij kijken we naar de stand van zaken rond IT- en OT-beveiliging en welke eerste stappen zij kunnen zetten om hun digitale weerbaarheid te versterken.”

IT en OT gescheiden werelden

Een belangrijke uitdaging is dat IT en OT binnen veel kleinere bedrijven nog altijd twee gescheiden werelden zijn, met ieder hun eigen kenmerken, systemen en verantwoordelijkheden, vertelt van Luik. Waar IT vooral draait om kantoorautomatisering, data en digitale processen, ligt de focus binnen OT op continuïteit van productie en operationele systemen. Daardoor wordt cybersecurity in de praktijk



Marcel Jutte: "Heel veel bedrijven weten niet waar ze moeten beginnen met cybersecurity. Dan is het CWM, waar je met gelijkgestemden zit, een mooi begin."

Communities voor cyberweerbaarheid

Josephine van Luik heeft een achtergrond in crisis- en securitymanagement en werkt voor het Cyber-weerbaarheidscentrum Maakindustrie (CWM) Zuid-Holland. "Wij zijn een publiek-private samenwerking tussen bedrijven uit de maakindustrie, de overheid en het onderwijs. Voor bedrijven zijn we een expertisecentrum en een hulploket op het gebied van digitale veiligheid. Als communitymanager kom ik bij veel bedrijven over de vloer om te kijken waar zij tegen-aan lopen en hoe wij ons programma daar zo goed mogelijk op kunnen laten aansluiten. Er zijn meerdere cyberweerbaarheidscentra actief in verschillende secto-ren, en we werken daar nauw mee samen. Zo is er voor de tuinbouwsector Cyberweerbaarheidscentrum Greenport, dat zich richt op het versterken van de digi-tale weerbaarheid van telers, ketenpartners en andere organisaties binnen de tuinbouwketen." Jutte: "Het CWM zit meer aan de kant van de bedrijven die nog moeten beginnen met cybersecurity. Het IPCS zit precies aan de andere kant, met allemaal topspecialisten. Zo vullen we elkaar aan."

nog vaak benaderd vanuit de IT-kant alleen. Volgens Jutte vraagt het om specialistische kennis en een goed begrip van beide domeinen. "Je ziet dat sommige organisaties erkennen dat zij die expertise niet zelf in huis hebben en daarom bewust externe specialisten inschakelen. Dat is een gezonde benadering. Tegelijkertijd zijn er ook situaties waarin cybersecurity erbij wordt gedaan, terwijl de complexiteit van IT- én OT-omgevingen juist vraagt om specifieke kennis en ervaring."

"Eerst moet je de basishygiëne voor OT-cybersecurity op orde krijgen"

Ideaal is het als IT- en OT-managers samen optrekken. Bij grotere organisaties gebeurt dat meestal wel, ziet Jutte. "Die hebben een CISO, chief information security officer, die zorgt dat in zijn team ook mensen zitten die verstand hebben van OT. Want er zijn daadwerkelijk grote verschillen in de aanpak. Ik geef een simpel voorbeeld. Als je drie keer een fout wachtwoord intoetst, word je vaak tijdelijk geblokkeerd. Op kantoor is dat lastig, maar geen ramp. In de fabriek soms wel. Want dan kun je niet meer bij de productiebesturing, kun je geen motoren meer uitzetten of zien wat er gebeurt. Dat slimme IT-mannetje kan dan een workaround bedenken voor de OT-manager die de hete adem van de productiechef in zijn nek voelt: 'Joh, je moet zorgen dat het zo snel mogelijk weer gaat draaien.' Maar soms is er echt iets aan de hand met de beveiliging en dan wil je dat juist niet. Veel slimmer is het als die kleinere ondernemers zich bewust worden van de problematiek en zich voor hulp wenden tot het CWM om eerst hun basishygiëne voor OT-cybersecurity op orde te krijgen."

Risico-inventarisatie

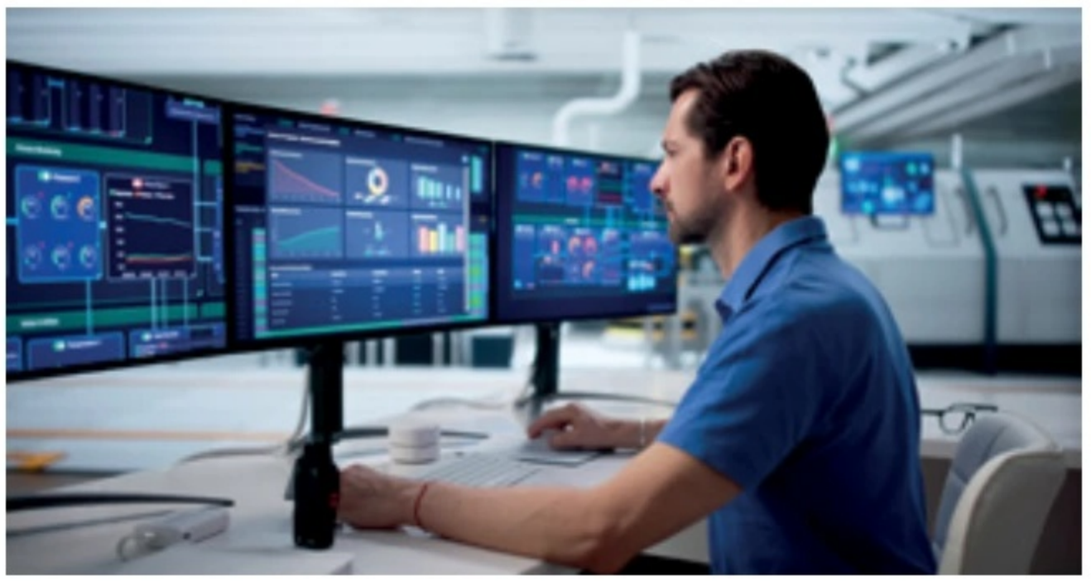
Gaat het over cybersecurity, dan moet het zeker ook gaan over gebruik van de cloud. Jutte is daar huiverig voor. "Met name voor OT, zeker als je kijkt naar de vitale infrastructuur. Het gaat dan natuurlijk over data, maar je hebt ook besturingen die via de cloud gaan. Daar ben ik absoluut geen voorstander van, omdat je het aanvalsoppervlak

Josephine van Luik: "Werken in de cloud heeft natuurlijk voordelen voor bedrijven, maar ze moeten er wel bewust mee omgaan en op de hoogte zijn van de risico's."



“Cybersecurity is een proces, het is nooit af”

voor cybercriminelen vergroot. Wat je juist moet doen is ‘hardening’ van je systemen. Dat betekent dat je alle zaken die je niet gebruikt, weghaalt of uitschakelt. Als je bijvoorbeeld een USB-poort niet nodig hebt, zorg je dat die niet meer werkt. Hardening kan ook zijn: als je niet echt in de cloud hoeft te zijn, probeer dat te voorkomen. Moet je toch over het internet, gebruik dan een VPN (virtual private network, red.).” Van Luik: “Werken in de cloud heeft natuurlijk ook voordelen voor bedrijven, maar ze moeten er wel bewust mee omgaan en op de hoogte zijn van de risico’s.”



“Wat zijn jouw ‘kroonjuwelen’, de applicaties die zeker niet mogen niet uitvallen?”

De cloud zal in ieder geval onderdeel moeten zijn van een risico-inventarisatie, zegt Van Luik. “Die kan meteen in het verlengde liggen van onze nulmeting: van welke externe partijen ben je afhankelijk, welke software heb je in huis, welke apparaten hangen aan het internet? Tweede stap is dan dat je kijkt wat jouw ‘kroon-juwelen’ zijn, de applicaties die zeker niet mogen uitvallen. Vervolgens ga je kijken hoe je die beveiligt. Dat is de driestaps-aanpak die je in ieder geval moet volgen.” Jutte: “In de vitale infrastructuur zijn ze hier al tien, vijftien jaar mee bezig. Voor de mkb’ers in de maakindustrie is zo’n risico-inventarisatie met hulp van het CWM een goed startpunt, een eyeopener: welke assets heb ik, welke zaken hebben aandacht nodig, wat zijn de kritische machines, waar zitten de grote risico’s?”

Gezamenlijke zorg voor de keten

Voor bedrijven in de maakindustrie komt daar nog bij dat ze altijd onderdeel zijn van een keten, als afnemer dan wel leverancier. Ze zijn afhankelijk van elkaar en dus moet cybersecurity een gezamenlijke zorg zijn, aldus Van Luik. “Die keten is zo sterk als de zwakste schakel – ik weet dat het een standaardquote is –, maar voor cybersecurity geldt dat echt. Daarom vind ik dat de grotere spelers een voorbeeldrol op zich moeten nemen.”

“De grotere spelers moeten een voorbeeldrol op zich nemen”

Technische dienstverleners zoals itsme nemen als spin in het web van de toeleveringsketen een cruciale positie in; zij kunnen niet stil komen te liggen door een hack. Daar komt bij dat ze componenten leveren voor industriële automatisering, zoals PLC’s, die zelf cyberveilig moeten zijn. Daarom hebben zij een speciale rol, aldus Jutte. “Ze bieden vaak eerstelijnssupport waar hun klanten, de mkb’ers, als eerste naar bellen bij problemen, ook als het om cybersecurity gaat. Die partijen moeten dan wel een goed verhaal hebben. Ze moeten op de hoogte zijn van de nieuwste ontwikkelingen en hun klanten daarover informeren, ook over de noodzakelijke maatregelen voor cybersecurity.”

Borgen binnen de organisatie

Voor veel bedrijven in de keten is het CWM een mooi ‘entry point’ voor het thema cybersecurity, stelt Jutte. “Heel veel bedrijven weten niet waar ze moeten beginnen. Dan is het CWM, waar je met gelijkgestemden zit, een mooi begin. Vraag hun advies, laat een nulmeting doen, pak de belangrijkste punten op en blijf eraan werken. Het zijn soms heel simpele dingen, zoals het opstellen van een procedure voor het wachtwoordbeleid. Vaak is men te goed van vertrouwen en gebruikt men elkaars wachtwoorden, maar dat kan een keer misgaan. Maak ieders verantwoordelijkheid duidelijk, zodat niemand die zomaar kan afschuiven.” Het begint met het stellen van de juiste vragen, vult Van Luik aan. “Zijn er bijvoorbeeld standaardregels voor wachtwoordgebruik, worden de toegangs-rechten goed beheerd, is de multifactor-authenticatie voor inloggen goed geregeld, staan er geen achterdeurtjes open omdat bijvoorbeeld leveranciers van machines nog toegang hebben?” Zo kan het CWM helpen bij het begin, maar een einde is er niet, waarschuwt ze tot slot. “Cybersecurity is eigenlijk nooit echt af. Dreigingen blijven veranderen, systemen veranderen en mensen blijven de grootste risicofactor waar het fout kan gaan. Daar moet je je prioriteiten leggen. Het blijft een proces dat je continu moet borgen binnen je organisatie.”

IPCS

Cyber Weerbaarheidscentrum Maakindustrie Zuid-Holland