Een totaalaanpak voor cybersecurity

DOOR REDACTIE AUTOMATIE PMA - VEILIGHEID EN CERTIFICERING · 21 SEPTEMBER 2018

We kennen allemaal de nieuwsberichten. Hacks in binnen- en buitenland leggen bedrijven, banken en instellingen plat, met steeds groter wordende gevolgen.

Ook in de primaire processen. Voorheen was IT (Information Technology) een gescheiden wereld van OT (Operation Technology). Die twee werelden komen steeds dichter bij elkaar. Rianne Boek van NEN en Marcel Jutte van Hudson Cybertec werken samen binnen NEN om cybersecurity een prominente plaats te geven in de industrie.
“Wij zijn er voor alle organisaties waar techniek een essentieel onderdeel is van de bedrijfsvoering”, legt Marcel uit. “Het is belangrijk om een bewustzijn te creëren op het gebied van cybersecurity – met name voor industriële automatisering en controlesystemen. Het verkeer op de weg, productielijnen in fabrieken, de klimaatbeheersing in een operatiekamer, de besturing van de deltawerken; het zijn allemaal geautomatiseerde processen.”

Vitale processen

“Als je deze processen niet goed beschermt, loop je enorme risico’s”, vervolgt Marcel. “Economisch, milieutechnisch, procesmatig en op het gebied van veiligheid. Vooral in de industrie. We hebben het over elektriciteitscentrales en chemische fabrieken maar ook het drinkwaterbedrijf. Een virus of een hack kan ervoor zorgen dat er geen water meer uit de kraan komt.”

Een eigen norm

“Iedereen weet dat ze er wat mee moeten”, beaamt Rianne. “En de normering – IEC 62443 – biedt een uitstekende basis. NEN biedt in samenwerking Hudson Cybertec de training hierin. We zorgen ervoor dat cybersecurity een vast onderdeel wordt van de bedrijfsvoering en dat bedrijven hun essentiële processen goed beschermen. Voor iedere deelnemer in de procesketen – leverancier,

eindgebruiker, engineer, procesontwikkelaar – hebben we een eigen set normen. Iedereen spreekt zo elkaars taal en is binnen de eigen specialisatie op de hoogte van risico's en een gedegen aanpak."

Techniek, organisatie en mens

Marcel benadrukt in de training het samenspel tussen bewustzijn en handelen. "Cybersecurity rust op drie onderdelen: techniek, organisatie en de mens. Software moet beschermd zijn, maar veiligheid moet ook onderdeel zijn van de doelen van het bedrijf. En als laatste mogen we de menselijke factor nooit over het hoofd zien. Een voorbeeld: een bedrijf besluit dat het kantoorpand geautomatiseerde toegangscontrole nodig heeft – organisatie. Maar als pasjes makkelijk te kopiëren zijn – techniek – of het personeel pasjes uitleent of laat slingeren – mens – wat heeft het dan voor een zin?"

Risico's signaleren

Zowel Rianne als Marcel vinden het zorgwekkend dat het bewustzijn in de mens-zijde van de driehoek onderbelicht blijft. "Neem een goed wachtwoord serieus, en plak het niet onder je muismat. Voer updates bewust en op tijd uit. Als je een usb-stick op straat vindt, stop die dan niet zomaar in je pc. Het is belangrijk dat deze manier van denken vanuit de IT ook doorwerkt op OT-gebied. Die usb-stick met virus kan complete productielijnen stil laten vallen. En een aangesloten laptop van buitenaf kan ook een zwakke plek in jouw beveiliging toevoegen."

Industrieel Platform Cyber Security

De training is een groot succes. Maar sommige deelnemers willen meer. Rianne: "Normalisering is absoluut noodzakelijk. Maar hoe je die toepast, ermee aan de slag blíjft in de snelle veranderingen binnen de OT en IT en ook de wetgeving; dat is niet eenvoudig om bij te benen als cybersecurity niet je vak is. Mede door die signalen, waar bedrijven en instellingen op vastliepen, is het Industrieel Platform Cyber Security (IPCS) ontstaan."

Actief bijhouden

"De leden van het platform komen twee keer per jaar samen en bespreken ontwikkelingen in binnen- en buitenland", gaat Rianne verder. "Deelnemers vertellen over hun problemen en over gevonden oplossingen. Er ontstaan discussies en er worden tips uitgewisseld. De normen bieden hierbij houvast, en dit platform volgt de verdere ontwikkeling. Zo laat je de deur ook niet op een kier staan."

Internet of things

Rianne schetst een voorbeeld van de veranderingen van nu: "We leven steeds meer in een wereld met het *internet of things* (IoT) en het daaraan gerelateerde *industrial internet of things* (IIoT). Lampen, speakers, temperatuursensoren, de deurbel; allemaal aangesloten op het web, op afstand uitleesbaar en/of bestuurbaar en met een eigen IP-adres. Ze wisselen informatie onderling uit, en met de mens. Alles is meetbaar en kan afzonderlijk of samen bestuurd worden. Het is de toekomst van de industrie, zeker, maar wat betekent dit voor de beveiliging? Ook hierover wisselt het platform informatie met elkaar uit."

Wetgeving bijbenen

Ook Marcel is blij met het platform. "We hoeven het wiel niet steeds opnieuw uit te vinden", zegt hij. "Er is veel kennis en probleemverkenning voor handen. Wij maken dat benaderbaar. Daarnaast maakt het platform het mogelijk om te kijken of de normen blijven voldoen en belichten we de wetgeving. Er komt een grote verandering aan: de Wbni (Wet beveiliging netwerk- en informatiesystemen). Naast de wettelijke meldplicht van digitale incidenten is er dan ook de zorgplicht. Bedrijven moet aantonen dat ze er alles aan hebben gedaan om digitale incidenten te voorkomen. Cybersecurity, dus."

Iets voor u?

Als u twijfelt of de training of het platform iets is voor uw bedrijf, kunt u de elevator pitch van het IPCS downloaden. Het korte document maakt direct duidelijk wat de noodzaak van cybersecurity is voor industrieel-technische bedrijven. Daarnaast heeft u direct een checklist welke medewerkers de training zouden moeten volgen.