Cybersecurity in de productie- en procesautomatisering

Sebastiaan Koning van Hudson Cybertec neemt de gelegenheid om over het belang van een goede cybersecurity te spreken. Processen in fabrieken zijn in rap tempo complexer geworden en steeds verder geautomatiseerd. "Daarbij wordt er ook vaker gebruik gemaakt van draadloze verbindingen. En dat brengt risico's met zich mee, zeker als die data uit alle sensoren richting een cloudoplossing gaat."

Cybercriminaliteit neemt toe, onder andere vanwege het feit dat je tegenwoordig geen 'nerd' meer hoeft te zijn om een cyberaanval uit te voeren. Je koopt ze gewoon online. "Dat leidt ertoe dat de overheid ook in actie is gekomen", vertelt Koning. "Zo hebben bedrijven een zorg- en meldplicht. De sancties die volgen op overtreding van die wetten, zijn niet mals."

Koning licht zijn betoog toe met een aantal casussen. Zo weet iedereen nog wel dat de terminal van Maersk in Rotterdam geruime tijd plat lag door een geslaagde cyberaanval. En in het voorjaar van 2019 werd de Noorse aluminium producent Norsk Hydro getroffen door een cyberaanval die alleen al in de eerste week 40 miljoen euro kostte. "Drie jaar geleden toonde een onderzoek aan dat jaarlijks zo'n 3000 industriële installaties door cyberaanvallen werden getroffen. Reken maar dat dit anno 2020 nog veel meer is."

Maar de dreiging komt ook vaak van binnen. Rancuneuze medewerkers die de beschikking hebben over wachtwoorden, kunnen voor de grootste problemen zorgen bij bedrijven. En waar cyberaanvallen zich tot enige jaren geleden beperkten tot de IT-kant van een bedrijf, worden er steeds vaker aanvallen op de OT-kant ingezet. "Denk maar aan de Triton malware, wat de Tritonex safety applicatie aanvalt en daarmee de failsafes in de PLC's omzeilt."

Sebastiaan Koning van Hudson Cybertec: "Er moet budget worden vrijgemaakt om die security sluitend te krijgen."

Verouderde besturingssystemen vormen ook een risico. "Systemen mogen niet down in de OT en om die reden zie ik nog regelmatig Windows 2000 en XP voorbij komen. De OT loopt vaak nog ver achter op IT als het over cybersecurity gaat."
En dan zijn er steeds vaker externe leveranciers die op afstand kunnen inloggen op hun applicaties. "Begrijpelijk", vindt Koning. "Maar wat als er een cyberincident bij die toeleverancier ontstaat. Kunnen cybercriminelen dan ook op die applicatie inloggen en kunnen ze dan ook verder in je fabriek kijken?"

> Maar wat als er een cyberincident bij die toeleverancier ontstaat: kunnen cybercriminelen dan ook op die applicatie inloggen en kunnen ze dan ook verder in je fabriek kijken?

Wat kunnen we er aan doen? "Redden we het met een firewall alleen?", vraagt Koning. "Tuurlijk draagt dat bij, maar dat alleen is niet genoeg. Cybersecurity berust op drie pijlers: organisatie, mens en techniek. Die moet je alledrie aanpakken en in balans houden. Er zijn heel veel oplossingen voor cybersecurity, maar veel van die oplossingen zijn afkomstig uit de IT. Let daarom op dat de maatregelen die je treft voldoen aan de ISO 62443, een cybersecurity norm, specifiek voor industriële toepassingen."

Maar het belangrijkste is draagvlak binnen de organisatie. "Vooral vanuit het management. Als daar niet het besef is dat cybersecurity zeer relevant is, moet je daar dus beginnen. Er moet budget worden vrijgemaakt om die security sluitend te krijgen."