Hoe kwetsbaar is de procesindustie?

Hack het lek: de frequentieregelaar

Kunnen hackers makkelijk op afstand schade aanrichten aan vitale industriële installaties of kritische infrastructuur van water- en energievoorziening? Niet als een bedrijf de cybersecurity op orde heeft. Maar een indringer die binnen is, komt makkelijk bij een kwetsbare schakel: de frequentieregelaar.

Arie Mol

Bij veel industriële roterende machines, zoals procespompen, wordt het toerental geregeld met frequentiegeregelde elektromotoren. Een communicatieprotocol verbindt de software van een frequentieregelaar met het procesbesturingssysteem. Fabrikanten van frequentieregelaars voorzien hun product van talloze instelmogelijkheden. De eindgebruiker kan de regelaar configureren voor zijn specifieke toepassing. Deze openheid en veelzijdigheid van de regelaar is tevens een kwetsbaarheid: settings kunnen eenvoudig via een netwerkprotocol worden gelezen, en veranderd, door ongeautoriseerd personeel. Een beveiligingsfunctie als 'skip' vertelt iedereen, dus ook een kwaadwillende indringer, wat een verboden toerentalgebied is. Deze nuttige functie voorkomt immers dat motor en pomp worden bedreven in hun kritisch toerental. De indringer stuurt motor en pomp vervolgens naar een verboden bedrijfstoerental. De gevolgen laten zich raden: te lang in een kritisch toerental draaien, ruïneert snel vitale onderdelen als mechanical seals, lageringen en ATEX labyrinten door onbeheerste resonantietrillingen. Bedieningspersoneel kan niet ingrijpen, want de noodstop functie is natuurlijk ook softwarematig gemanipuleerd.

KWETSBARE INSTALLATIES

Het meest kwetsbaar zijn motoren en pompen met een kritisch toerental onder maximum bedrijfstoerental. Het gaat dan meestal om hoog-toerental toepassingen (> 3000 rpm) en grote vermogens (> 0,5 MW), zoals een frequentiegeregelde ketelvoedingspomp in een elektriciteitscentrale.
Een proces met een groot aantal parallel draaiende, al dan niet synchrone, motoren is een ander voorbeeld. Deze toepassing is te vinden in de garenindustrie en bij centrifuges voor uraniumverrijking. Stuxnet, het schadelijke computerprogramma dat in 2009

zou zijn ontwikkeld om Iraanse ultracentrifuges te saboteren, is een klassiek voorbeeld.
Bij installaties met een kritisch toerental boven maximum bedrijfstoerental kan de gevolgschade beperkt blijven. Bij toenemend toerental neemt het pompvermogen toe met de derde macht van het toerental en de motorstroomtoename zorgt ervoor dat snel de maximale stroombeveiliging of het autonome thermisch blok vóór de frequentieregelaar wordt aangesproken. Maar ook een ongecoördineerde productiestop is een zeer ongewenste situatie. Een 'root cause analysis' kent een paar heikele punten. De dader is tevens de enige getuige. Een verwoesting door een cyberattack hang je niet aan de grote klok. Logboeken met configuratie-aanpassingen worden niet altijd bijgehouden.

CYBERSECURITY WAARBORGEN

Wanneer het gaat om persoonsgegevens krijgt beveiliging een hoge prioriteit. Een bedrijf is op grond van de Wet Bescherming Persoonsgegevens (WBP) sinds 1 januari 2016 verplicht om een ernstig datalek meteen te melden aan de Autoriteit Persoonsgegevens. Deze Autoriteit kan een fikse boete opleggen. Wanneer het gaat om de ICT-beveiliging van de rotating equipment, de moneymakers, speelt er geen externe druk zoals meldplicht en boete. Het initiatief tot adequate beveiliging moet van binnenuit komen.
Het is doorgaans lastig om in een bedrijfsnetwerk binnen te dringen. Vervolgens is het ook lastig om data te stelen, maar het is kinderlijk eenvoudig om ernstige schade aan te richten aan productiemiddelen. Een adequate beveiliging vraagt om een deskundige afstemming tussen eindgebruiker, dienstverleners en leveranciers. Netwerktoegang-autorisatie, databeheer, software-specificaties en updating moeten goed doordacht worden. Firewalls tussen het proces (fabriek) en de administratie (kantoor) zijn nuttig maar onvoldoende. Het 'Internet of Things' biedt de mogelijkheid aan de hacker om via met internet verbonden (Wi-Fi) sensortechnologie in te breken via een achterdeur. De kwetsbaarheid voor inbraak neemt snel toe. De grootste bedreiging is niet altijd de 12-jarige whizzkid op zijn zolderkamer of de crimineel in Verweggistan. De zwakste schakel zit intern, in een chantabele of ontevreden werknemer. Management en personeel dienen zich bewust te zijn van de risico's van hun gedrag. Bezuinigen op training is geen optie. Hoeveel is er in het budget opgenomen voor de post cybersecurity?

CONDITIEBEWAKING UITBESTEDEN

Datzelfde internet der dingen biedt bedrijven de mogelijkheid om conditiebewaking, service en onderhoud en slimme data-analyse uit te besteden aan externe deskundigen of de Original Equipment Manufacturers (OEM's). Maar er doemt een 'data dilemma' op. ICT-managers en verzekeringsmaatschappijen zijn niet blij met welke koppeling naar de buitenwereld dan ook. Een 'data diode' – wel data van binnen naar buiten, niet andersom – stelt hen niet gerust. Welke datasets gaan er nog meer mee, welke gevoelige productiedata? Is een hacker onder de indruk van een data diode? Te veel uitbesteden heeft het nadeel van toenemende kwetsbaarheid. De kans is groot dat bij een crash of calamiteit met een essentieel productiemiddel de eindgebruiker een informatieachterstand heeft op de OEM. Een eventuele (garantie) claim succesvol onderbouwen, wordt dan lastig.

Conditiebewaking, welke datasets gaan er naar buiten?

Hoe kwetsbaar is de infrastructuur?