Norsk Hydro kreeg in 2019 te maken met een grote cyberaanval. Wereldwijd gingen de schermen op zwart en moesten operators werken met papier in plaats van het bedrijfsnetwerk. Binnen een week had het bedrijf een schadepost van zo'n 40 miljoen euro

'Als de schermen op **zwart** gaan'

Cyberaanvallen halen tegenwoordig vaker het nieuws dan ons lief is. Maar wat kun je eraan doen? Als productielijnen, waternetwerken, machineparken of energiecentrales stilvallen kost dit kapitalen en het geeft een hoop gedoe. Dus maak machines weerbaar tegen cyberaanvallen. Dat is de boodschap die Sebastiaan Koning, senior cybersecurity-consultant bij **HUDSON CYBERTEC**, afgelopen najaar gaf tijdens de Nationale Aandrijftechniekdag. In dit artikel gaan we dieper in op zijn presentatie 'Hoe maak ik mijn machine cybersecure door gebruik te maken van de IEC 62443 norm'.

"De wereld om ons heen verandert razendsnel. Niet alleen evolueren slimme apparaten in de privésfeer zoals intelligente thermostaten, smart watches, slimme verlichting,... Er is eveneens een evolutie gaande in industriële automatisering. Wat ooit eenvoudig begon met een lopende band die werknemers bedienden, werd door de jaren heen steeds complexer. Die complexiteit groeit bovendien steeds sneller. Inmiddels is alles met elkaar verbonden op een slimme manier, zijn we aanbeland bij Industrie 4.0 en zien we een toenemende automatiseringsgraad en complexiteit van machines en installaties. Ook draadloze systemen, interne en externe koppelingen, aansturen op afstand en cloudtoepassingen nemen toe. Bedrijven worden hierdoor steeds afhankelijker van systemen en van specialisten die de systemen kunnen bedienen," zegt

TEKST / Evi Husson
FOTO'S / Norsk Hydro

Sebastiaan Koning van Hudson Cybertec: "Focus op mens, techniek en organisatie"

Sebastiaan Koning, senior cybersecurity-consultant bij Hudson Cybertec. Het bedrijf is expert met betrekking tot de IEC 62443, de wereldwijde standaard voor cybersecurity voor Industriële Automatisering en Controle Systemen (IACS). Hudson Cybertec ondersteunt bedrijven met het op orde krijgen van cybersecurity voor hun primaire proces op het gebied van mens, organisatie en technologie.

Groei aan cybercriminaliteit

Cybercrime lift mee op nieuwe ontwikkelingen in de digitale wereld. "Cyberaanvallen zijn tegenwoordig zelfs te koop. Je kunt ze zonder al te veel moeite aanschaffen of er zelfs een abonnement op nemen. En kom je er niet uit, dan ondersteunen helpdesks je bij een aanval. Mede hierdoor is er een immense groei aan cybercriminaliteit."

Niet alleen IT-omgevingen zijn kop van jut. "Steeds vaker zie je dat ook de industrie doelwit is van cyberaanvallen. Het gaat dan onder meer over malware. In 2017 werden jaarlijks drieduizend locaties besmet met doorsnee malware. Dit leidt niet noodzakelijk tot incidenten, maar het geeft wel aan dat onbevoegden ongevraagd systemen binnendringen. Inmiddels zijn we vier jaar verder en is het aantal besmettingen met malware aanzienlijk toegenomen. Daarnaast zien we ook dat sommige malware specifiek is ontwikkeld om de industriële automatisering te infecteren. Een bekend voorbeeld is de Triton-malware. Doel ervan was om de safety systemen in een petrochemische installatie in Saoedi-Arabië te overbruggen om zo een explosie te veroorzaken. Gelukkig is dit hen niet gelukt, maar het had heel anders kunnen aflopen."

Gerichte of niet gerichte aanval

Een tweede type aanval gebeurt met ransomware, ook wel gijzelsoftware genoemd. "Bestanden en systemen worden 'gegij-

Na een cyberaanval is het zaak de boel weer op de rit te krijgen. Dit was de 'war room' van Norsk Hydro na de aanval in 2019. De herstartplannen werden op papier gemaakt

Als een complexe installatie plotseling stil komt te liggen, kan dat gevaar opleveren voor de operators

zeld' waarna losgeld wordt gevraagd om ze weer vrij te geven. Ongeveer twee derde van deze systeemaanvallen is bewust en gericht op organisaties. Dat betekent dat een derde ervan niet gericht is, wat wellicht nog veel enger is. Zo heeft ook Maersk ervaren. Wereldwijd legde ransomware al hun systemen plat waardoor ongeveer vierduizend servers en 45.000 computers opnieuw moesten worden geïnstalleerd, inclusief alle applicaties. De totale schade werd geschat op 300 miljoen euro."

In 2019 ging het mis bij aluminiumreus Norsk Hydro. "Ook hier kwam hun wereldwijde operatie stil te liggen met als gevolg dat ze na een week ongeveer 40 miljoen euro aan schade hadden. Dichter bij huis was in 2020 weefgetouwenbouwer Piconol in België het slachtoffer. Zij hadden de zaken wat beter op orde waardoor de schade beperkt bleef tot een miljoen euro. Kortom, aanvallen zijn niet langer alleen gericht op IT. Ook het OT (Operationele Technologie)-domein moet cybersecure worden ingericht om aanvallen te voorkomen."

Alles valt of staat met het inrichten van de juiste processen en de 'awareness' bij de gebruikers (FOTO: RON DE HAER)

Zwakke plekken

De opkomst van meer, geavanceerde en doelgerichte aanvallen is een risico. "Daarnaast draagt een aantal andere aspecten binnen de organisatie bij tot een hoger risico op aanvallen. Denk aan verouderde besturingssystemen, IT-advies dat zonder nadenken in OT-systemen wordt toegepast, een slechte regulering van de koppeling tussen IT en OT,..."

Met externe koppelingen moet eveneens voorzichtig worden omgesprongen. Koning geeft een voorbeeld: "Een fabriek werd door de jaren heen voorzien van een datanetwerk om alle systemen aan elkaar te koppelen. Werknemers konden de productie vanaf een centraal systeem bedienen en beheren. Het bedrijf legde bewust geen internetverbinding aan aangezien het niet zomaar de installaties met de buitenwereld wilde verbinden. Dit zou extra risico's met zich mee kunnen brengen. Echter, enige tijd later schafte het bedrijf een nieuwe machine aan met een dermate grote complexiteit dat regelmatig ondersteuning van de leverancier nodig was. De machine, voorzien van een 4G-modem, maakte daarom regelmatig verbinding met de leverancier. Deze kon eenvoudig meekijken en op afstand ondersteuning bieden waar nodig. Maar door een kwetsbaarheid bij de leverancier kon een aanvaller toegang krijgen tot zijn systemen en via deze weg ook de OT-systemen van het producerende bedrijf aanvallen. Dit

scenario ben ik in de praktijk al een aantal keer tegenkomen. Eventuele gevolgen zijn een verstoring van het productieproces en cyberspionage. Ook schade aan materieel, milieu en in het ergste geval mensen is mogelijk omdat beveiliging het bijvoorbeeld niet langer doet."

Techniek, mens en organisatie

Hoe je je tegen aanvallen kunt beschermen? "'Laten we een firewall plaatsen, dan zijn we veilig' wordt wel eens geroepen," zegt Koning. "Maar een firewall is een technische maatregel en technische maatregelen hebben slechts 20 tot 30 procent impact. Wil je cybersecurity echt goed organiseren, dan zal je de focus moeten leggen op drie pijlers: mens, techniek en organisatie. Alleen als je deze drie op orde hebt, ben je veilig. Richt bijvoorbeeld procedures in op menselijk en organisatorisch niveau zodat iedereen weet wat kan en mag zodat onregelmatigheden snel worden opgemerkt. Kies daarnaast niet voor IT-advies maar bepaal een industriële aanpak voor je cybersecurity waarbij de IEC 62443 de leidraad is."

Pragmatisch

De theorie omzetten in de praktijk is niet altijd even gemakkelijk. "Mijn advies is om heel pragmatisch aan de slag te gaan en te beginnen met een analyse. Welke assets heb je? Hoe communiceren deze met elkaar? Wat zijn de kwetsbaarheden? Wat zijn de risico's en wat is de impact als er iets misgaat? Wat is het huidige niveau van cybersecurity? Wat voor maatregelen zijn er al toegepast? Ga vervolgens aan de slag met het opstellen van een beleid en procedures. Kies voor beveiligingsoplossingen, implementeer deze en onderhoud ze. Stimuleer daarbij ook de bewustwording bij medewerkers. Dit kun je onder meer doen door verantwoordelijkheden goed af te stemmen, te informeren wat je wil bereiken en hoe je dit wil aanpakken. Deel kennis over cybersecurity als die aanwezig is en help elkaar."

Zero trust

Ook voor het werken met externe partijen zijn procedures nodig. "Mijn advies is om uit te gaan van het zero trust-principe. Vertrouwen is goed, maar controle is beter. Zo kun je zowel technische als organisatorische eisen opstellen, zodat niet alleen het product an sich cybersecure is (security by design), maar ook de leveranciersketen is geborgd. Het toetsen van de werkzaamheden die worden uitgevoerd door externe partijen is belangrijk."

Ga in gesprek

Werk je zelf als toeleverancier met klanten, dan is het belangrijk dat je ook met jouw klant in gesprek gaat over cybersecurity, gaat Koning verder. "Je moet weten wat zijn eisen zijn op het gebied van cybersecurity, welke netwerkverbindingen beschikbaar zijn en welke werkwijze zij hanteren om cybersecure te werken. Als toeleverancier zul je ook altijd bewust moeten blijven van potentiële risico's. Het zomaar even een computer in hun netwerk pluggen, is uit den boze. Ook jouw klant kan jou besmetten waarna jij vervolgens weer naar een andere klant gaat. Kortom, neem je verantwoordelijkheid en ga altijd cybersecure te werk."

Hoe verder?

Als eenmaal je organisatie cybersecure is ingericht, stopt het niet. "Je bent nooit klaar met cybersecurity. Technologie blijft evolueren maar de dreigingen evolueren evenzeer en wellicht nog veel sneller dan de techniek. Beoordeel daarom continu risico's, vooral wanneer er sprake is van mutaties. Verander je iets in de bedrijfsvoering – denk aan een update, de aanschaf van een nieuwe machine, het inpluggen van een externe pc,... – beoordeel steeds wat de risico's kunnen zijn voor jou, je klant of je samenwerking. Wil je sneller onregelmatigheden kunnen detecteren, dan is OT cybersecurity monitoring een goede oplossing. Deze leggen aan de hand van gegenereerde data een basis vast van normaal gedrag en detecteren met behulp van machine learning en anomaliedetectie snel afwijkend netwerkverkeer waardoor je sneller maatregelen kunt nemen." <

www.hudsoncybertec.com

Stilstand of storing van energiecentrales (hier een waterkrachtcentrale) of grote pompaandrijvingen in waternetwerken kunnen de maatschappij flink verstoren

/// DE CLOUD

Het is altijd even extra opletten wanneer je werkt in de cloud. Sebastiaan Koning: "Cloudverbindingen kunnen naast de primaire verbinding die je maakt met je installatie, veel meer verborgen virtuele verbindingen hebben. Daarom is het aan te bevelen om je goed te informeren over clouddiensten. Een cloudoplossing kan een groot risico zijn als dit niet goed is gereguleerd."