Hoe voorkom je een cyberaanval op je machines?

Cyberaanvallen speelden zich in het verleden vooral af in IT-omgevingen. De laatste tijd groeit ook het aantal dreigingen in het OT-domein (operational technology): malware en bewuste aanvallen die gericht zijn op de besturingssystemen of de procesautomatisering van producerende bedrijven. Hoe kun je je hiertegen beschermen?

Tekst **Evi Husson**

"Cybercrime, specifiek ontwikkeld om PLC's in productieomgevingen aan te vallen, neemt toe", stelt Sebastiaan Koning, cybersecurity-consultant bij Hudson Cybertec. "Denk bijvoorbeeld aan de Triton-malware. Via deze malware kregen aanvallers toegang tot de safety-systemen (Triconex Safety Instrumented System, ofwel SIS-werkstation, red.) van een chemische fabriek in Saoedi-Arabië, met het doel deze te herprogrammeren zodat ze een explosie konden veroorzaken. De aanval mislukte aangezien twee controllers in een zogenoemde "Fail-safe"-modus terechtkwamen waardoor de operationele processen automatisch werden stilgelegd."
Recentelijk zijn er meer zulke aanvallen geweest. Bij scheepvaart- en transportgigant Maersk bleken de computers vergrendeld door malware (2017). Ransomware trof de Noorse aluminiumgigant en energieconcern Norsk Hydro in 2019 terwijl dit ook Honda is overkomen afgelopen juni. Op meerdere vestigingen was de productie onderbroken. Dichter bij huis, en ook recent, was het alle hens aan dek bij Piconal in België, fabrikant van weefmachines. Een deel van het bedrijf lag begin dit jaar door ransomware volledig plat.
"Het gaat niet langer om malware die naast het platleggen van het IT-systeem per toeval ook het OT-systeem bereikt. Toevalligheden zijn veranderd in doelgerichte aanvallen."

Andere aanpak

"Gelukkig krijgt het beveiligen van OT nu – uit noodzaak – ook de aandacht die het eigenlijk al jaren eerder had moeten krijgen", stelt Koning.
Dit beveiligen van OT-systemen vergt een andere aanpak. "IT-systemen krijgen regelmatig een update waardoor mogelijke kwetsbaarheden in het systeem worden verminderd. Bij OT-systemen is dit veel complexer. Je hebt hier vaak te maken met legacy-apparatuur, die kwetsbaar is en niet altijd geüpdatet kan of mag worden. Bovendien moet er zorgvuldig met veiligheidsupdates worden omgegaan. De systemen voor de aansturing van de procesautomatisering moeten altijd blijven werken. Alle updates binnen OT-systemen moeten daarom eerst worden gevalideerd. Leveranciers van de software moeten gescreend en de updates moeten door de eigenaars van de installaties zelf worden getest, voor een productieomgeving deze in bedrijf mag nemen. Dit kost dus veel meer tijd dan een relatief eenvoudige software-update bij IT. Deze IT-updates zijn zodanig generiek en wereldwijd al uitvoerig getest dat je ze vrijwel zonder risico voor de continuïteit van een proces kunt uitrollen. Heel anders dan in een OT-omgeving."

Ken je netwerk

Een strategie om de cyberweerbaarheid van OT-systemen te verhogen, begint bij het kennen van je netwerk. "Vanuit IT wordt vaak voor een blokkeer-aanpak gekozen. Zodra men vaststelt dat een IP-domein geïnfecteerd lijkt, wordt dit geïsoleerd en afzonderlijk aangepakt om de schade te minimaliseren. Bij OT-systemen werkt dit niet aangezien de systemen veel complexer zijn en met elkaar zijn verbonden. Bepaalde mogelijk geïnfecteerde systemen isoleren kan leiden tot grote schadelijke gevolgen voor het bedrijf. Daarom is het noodzakelijk om in een heel vroeg stadium mogelijke aanvallen te detecteren zodat snel en zonder grote gevolgen kan worden ingegrepen. Dit is mogelijk door je netwerk goed te kennen en te bepalen wat normaal is. We roepen continu: *Know your network*, ken je apparaten en je systemen en weet hoe deze syste-

men met elkaar communiceren. Dat is de basis."

OT-monitoring

In de praktijk gebeurt dit vaak met monitoring. "OT-monitoringsoplossingen leggen een *baseline* vast van het normale gedrag. Welke assets zitten in het netwerk en hoe communiceren die met elkaar? OT-systemen produceren doorgaans veel voorspelbare data, aangezien alle gegenereerde data een specifiek doel dienen. Je kunt dus heel goed bepalen wat het normale gedrag is. Met anomaliedetectie op basis van machine learning wordt vervolgens op een snelle en intelligente manier gedetecteerd of er afwijkend gedrag wordt vertoond. Wordt bijvoorbeeld een onbekende asset op het netwerk aangesloten of wordt een asset vervangen door een malafide asset dan merkt het systeem dit meteen op en kan adequaat worden gereageerd."

Monitoring op basis van anomaliedetectie is van dermate grote meerwaarde voor de OT-omgeving, dat dit in Duitsland onderdeel wordt van aanstaande wet- en regelgeving voor kritieke infrastructuren. Steeds meer organisaties moeten aantonen dat voldaan wordt aan wet- en regelgeving. "Een aanpassing van wet- en regelgeving is er nog niet in Nederland, maar eens een lid van de Europese Unie een eerst stap zet, volgen de andere Europese landen wellicht vrij snel. Het Hudson Cybertec OT-monitoringsysteem geeft inzicht in de *compliance* met verschillende normen, wet- en regelgeving zoals de BIO, CSIR, IEC 62443 of ISO 27k."

False positives

Het is belangrijk om monitoringssystemen te kiezen die specifiek zijn gericht op OT-systemen. Een tweede aspect dat de nodige aandacht verdient, is het op een juiste manier inleren van het systeem. "Het goed inleren van machine learning technologie is van belang om zogenoemde *false positives* te voorkomen. Deze kunnen het productieproces verstoren aangezien alarmmeldingen vaak manueel moet worden bekeken en uitgeschakeld. Een goede voorbereiding voor implementatie is van belang."

"Met anomaliedetectie op basis van machine learning wordt op een snelle en intelligente manier gedetecteerd of er afwijkend gedrag wordt vertoond."

Remote access en cybersecurity

Productiesystemen in OT-afdelingen worden alsmaar complexer. De productie moet voortdurend de aandacht verdelen tussen verschillende vakgebieden waar ze mee te maken hebben. Hierdoor wordt steeds vaker bewust beroep gedaan op externe expertise. "Het komt regelmatig voor dat leveranciers hun klanten bij de aanschaf van nieuwe machines service- of onderhoudscontracten aanbieden. Ze vragen daarbij mogelijk om toestemming om op afstand bij de machine te kunnen. Mogelijk gaat data via het OT- en IT -systeem alleen naar buiten, maar in andere gevallen heeft de leverancier een 4G- ▷

modem ingebouwd zodat ze *remote*, indien nodig, in de machine kunnen om problemen te verhelpen. Hoe is de veiligheid in deze gevallen geborgd? Hoe voorkom je dat een aanvaller via een leverancier toegang krijgt tot jouw machine in de productieomgeving? Daar zit een potentieel risico."

Scenario's

"Als er *remote* toegang is ingericht of wordt gevraagd, is de eerste vraag die je je als productie-omgeving altijd moet stellen: Is *remote* toegang echt nodig? Is het antwoord op deze vraag JA, dan zal vervolgens op basis van de risico-inventarisatie moeten worden nagegaan wat is toegestaan, hoe dit op een veilige manier mogelijk is en hoe dit zal worden geborgd. Is er een mogelijke backdoor, dan zal moeten worden nagegaan hoe je kunt voorkomen dat dit impact heeft op de rest van de productie. Aan te bevelen is om voor alle mogelijke scenario's te onderzoeken wat wanneer welke impact op welke systemen kan hebben. Door de situatie te inventariseren en in kaart te hebben hoe je datastromen eruit zien en hoe je dataflow eruit ziet, kun je vooraf al de nodige maatregelen nemen en meteen inspringen als er iets afwijkend gebeurt."

"Wat we constateren is dat de organische groei van bedrijven en hun systemen niet altijd goed is gedocumenteerd waardoor er blinde vlekken in het systeem ontstaan."

Techniek – mens - organisatie

Voor een fabriekseigenaar is het verstandig om specifieke eisen rond cybersecurity op te stellen waaraan opdrachtnemers of toeleveranciers moeten voldoen. "Je moet daarbij niet alleen bepalen waaraan systemen die ze leveren moeten voldoen. Ook randvoorwaarden opstellen voor medewerkers die mogelijk op bezoek komen is van belang."
Cybersecurity beperkt zich niet alleen tot technische oplossingen. "Zowel voor de eigen werknemers als samenwerking met *third parties* geldt dat er een balans moet zijn tussen mens, organisatie en techniek. Het is aan te bevelen procedures op menselijk en organisatorisch niveau in te richten zodat de kans dat iemand iets mee naar binnen brengt en in het OT-systeem terechtkomt kleiner wordt. Houdt de mensen ook periodiek bewust zodat ze altijd alert blijven en onregelmatigheden opmerken. Daarnaast blijven technische maatregelen om de risico's te beperken, voortdurend aan de orde."

Geen eenmalige exercitie

De theorie is eenvoudiger dan de praktijk. "Wat we constateren is dat de organische groei van bedrijven en hun systemen niet altijd goed is gedocumenteerd waardoor er blinde vlekken in het systeem ontstaan. Is er bijvoorbeeld een machine aan het machinepark toegevoegd, met een 4G-verbinding naar buiten om op afstand service te laten meekijken, en dit is niet goed gedocumenteerd, dan is dit mogelijk een zwakke plek. Cybersecurity is met andere woorden geen eenmalige exercitie, maar iets om altijd bij te houden en periodiek te toetsen. Stel jezelf voortdurend de vragen: Waar staan we nu op security-gebied met betrekking tot mens, organisatie en techniek? Heb ik alle maatregelen genomen of moet ik weer nieuwe maatregelen nemen? Pas je dit systematisch toe, dan is het risico op onaangename verrassingen veel kleiner."

IT versus OT

Informatietechnologie (IT) en operationele technologie (OT) zijn op fundamenteel andere uitgangspunten gebaseerd. Operationele Technologie is primair ontworpen om zo betrouwbaar mogelijk te opereren met een zo hoog mogelijke beschikbaarheid. Als het besturingssysteem uitvalt of er zijn andere calamiteiten, dan zou het proces moeten kunnen blijven draaien, no matter what. Installaties zijn vaak al jaren geleden ontworpen, zijn erg robuust en zodanig ingericht dat risico's zoveel mogelijk worden beheerst. Bij IT is daarentegen snelheid, connectiviteit, rekenkracht en communicatie veel belangrijker. Bedrijven die menen dat een IT-afdeling ook de beveiliging van de industriële automatisering en control systems erbij kan nemen, komen er daarom al snel achter dat die combinatie niet zo goed is te maken is. Het gaat om twee totaal andere werelden die op een hele andere manier zijn opgebouwd.