Eerste SOC voor permanent monitoren OT-installaties op cyberincidenten

Hudson Cybertec uit Den Haag gaat als een van de eerste beveiligingsspecialisten in operationele technologie (OT) een voorziening inrichten voor het 24 x 7 monitoren van industriële systemen en netwerken van bedrijven vanuit een centraal punt. In de IT-wereld zijn deze zogeheten Security Operating Centers (SOC's) al veel langer in gebruik. Hoewel onder invloed van de digitale transformatie de IT- en OT-omgevingen naar elkaar toe groeien, vraagt het beveiligen tegen cyberrisico's in het industriële segment om andere functionaliteit. Een in IT-beveiliging gespecialiseerd bedrijf kan de OT er niet even bijdoen. Daarvoor is de denk- en handelswijze van de in beide omgevingen werkzame mensen te verschillend. ▷ Fred Franssen

Het vinden van de balans tussen mens, organisatie en techniek vormt de rode draad in de ondernemingsmissie van Marcel Jutte, een veteraan met meer dan 30 jaar werkervaring in de OT binnen de industriële wereld en aanverwante sectoren.

Met zijn kennis en ervaring maakt hij deel uit van talloze werkgroepen, adviescommissies en andere overlegorganen waarin de participanten zich buigen over de normen en richtlijnen rondom het thema cybersecurity. Vanuit zijn bedrijf Hudson Cybertec adviseert, inspecteert en implementeert Jutte samen met een vijftiental medewerkers cyberbeveiligingsoplossingen bij een brede groep klanten in binnen- en buitenland. Volgens Jutte is het succes van de onderneming voor een belangrijk deel toe te schrijven aan het onafhankelijk opereren van de toeleveranciers van beveiligingstechnologie.

Appels met peren vergelijken

"Wij krijgen steeds vaker de vraag van organisaties om voor hen de specificaties te definiëren op basis waarvan zij hun toeleveranciers en systeem integratoren kunnen laten offreren. Op die manier voorkomen ze het vergelijken van appels met peren in de selectiefase. Uiteindelijk hebben ook de toeleveranciers daar baat bij. Zo vervullen we een adviserende en tevens controlerende rol bij bijvoorbeeld de beveiliging

van de operationele systemen in een omvangrijk project voor de winning van olie en gas in Noorwegen met een looptijd van enkele decennia. We zitten daarnaast bij grote projecten in eigen land, zowel in de vitale infrastructuur als bij overheden en internationaal opererende organisaties. Ook zien we de vraag vanuit het mkb voor ondersteuning op het gebied van cybersecurity toenemen."

Mindset compleet anders

Volgens Jutte staat cybersecurity in relatie met operations bij veel bedrijven nog niet hoog genoeg op de agenda. Zo ontbreekt het vaak nog aan een cybersecuritybeleid op het gebied van de OT. Volgens hem is er meestal wel sprake van beleid voor de kantoorautomatisering en de overige IT-onderdelen van een onderneming. "Vanuit de historie draagt veelal de financiële man in het directieteam de verantwoordelijkheid voor de IT-gerelateerde zaken. De OT kent vaak geen aparte vertegenwoordiger op directieniveau. De 'blauwe boorden' wenden zich niet zo snel tot de baas. Daarnaast is hun 'mindset' compleet anders dan die van IT'ers. OT'ers zijn vaak pure techneuten die denken en handelen vanuit de continuïteit van de operationele processen. Ze zijn in de regel 'selfsupporting'. De dreigingscriteria en risico's in hun werkomgeving zijn ook compleet anders. Een operator is niet altijd in de gelegenheid een systeem uit te zetten voor het doorvoeren van een patch. Een mailserver in de kantooromgeving kan rustig vijf minuten uit de lucht zijn zonder dat het bedrijf direct schade oploopt. En daar waar de IT-systemen wel de continuïteit beïnvloeden, is het proces van patchen en updaten geregeld via al langer bestaande voorzieningen met onder meer back-up- en herstelprocedures."

Om een goed beeld te krijgen van hoe de cybersecurity is geregeld, begint Hudson Cybertec in de regel met een 'nulmeting'. Die moet antwoord geven op vragen als: zijn de OT-faciliteiten essentieel voor de bedrijfsvoering; welk risico loopt het bedrijf na een incident bij de digitale voorzieningen; zijn de medewerkers en directie zich daarvan bewust en wat is hun kennisniveau als het gaat om het implementeren van cybersecuritymaatregelen?

Kijkje in kantoor

Jutte komt terug op zijn motto: "Het draait allemaal om de balans tussen mens, organisatie en techniek. Is er een beleidsplan en hoe zijn de verantwoordelijkheden geregeld? Zijn er gescheiden netwerken voor IT en voor OT? Veelal zijn er wel maatregelen genomen, waardoor men niet zomaar ongeautoriseerd vanuit de kantooromgeving op het netwerk van de industriële automatisering kan komen.

Andersom kan ook. Recent bleken we bij een assessment in een industrieel productiebedrijf vanuit het fabrieksnetwerk in de loon- en salarisadministratie te kunnen kijken. Daar stond ook informatie in over uitgekeerde bonussen. De IT-manager werd erbij geroepen. Die had net een inspectie laten uitvoeren waarin het lek niet boven water kwam. De zwakke schakel betrof een verkeerd ingestelde firewall die zich bevond op het scheidsvlak tussen de OT en IT."

Met de specifieke OT-SOC wil Marcel Jutte ook deze tussen wal en schip geraakte beveiligingsoplossingen kunnen monitoren. Hij verwacht nog dit jaar de eerste grotere partijen te kunnen aansluiten op de centrale bewakingsvoorziening. Die past geheel in de huidige trend in het securitywezen van permanente controle op het ongewenst binnendringen van netwerken, inclusief de pogingen daartoe - intrusion detection - en het uitvoeren van penetratietesten of het als 'mystery guest' de werkvloer opgaan. In de SOC combineert Hudson Cybertec de kennis van de vele, uiteenlopende protocollen in de OT-sector met de totaal verschillende werkomgevingen van de klantenkring, die kan variëren van oliebooringstallaties, infra en chemische productieplants tot aan installaties voor waterbeheer en waterzuivering.

Marcel Jutte.

Normontwikkeling

Alle ervaringen opgedaan met OT-cybersecurity in de uiteenlopende sectoren vloeien weer samen in de dienstverlening op het vlak van forensisch onderzoek. Met het verzamelen en analyseren van data uit incidenten zijn de specialisten van Hudson Cybertec ook in staat om een lijst van tegenmaatregelen op te stellen. Die bieden uitkomst bij het herstellen van de eventuele schade, opgelopen na een incident en het opstarten, dan wel voortzetten van de reguliere procesgang. In bijna alle sectoren waarin het bedrijf actief is, gelden aparte normen voor beveiliging. De cybersecuritynorm IEC 62443 voor Industrial Automation & Control Systems (IACS) is echter leidend. Het bedrijf beschikt ook over een eigen 'Academy' en verzorgt in nauwe samenwerking met NEN IEC 62443 trainingen.

"Wij zijn al langer betroken bij de normontwikkeling", vervolgtBijsch Marcel Jutte. "Wij weten hoe die norm is opgebouwd uit diverse onderdelen en ook hoe je die modulen voor de verschillende bedrijfsomgevingen moet gebruiken. Wij leveren een handvat bij het toepassen van de norm voor het inrichten van cybersecurity in je eigen organisatie volgens de richtlijnen van de Wet Beveiliging Netwerk- en Informatiediensten, afgekort Wbni. Bedrijven die onder deze wet vallen, zijn verplicht aan de toezichthouder aan te tonen dat ze adequate maatregelen hebben genomen om cyberincidenten zoveel mogelijk te voorkomen." ■