De IT-nachtmerrie van Process Control Security

Als ict-manager, CIO of CISO bent u verantwoordelijk voor de beveiliging van het bedrijfsnetwerk. U doet er alles aan om het beveiligingsniveau zo hoog mogelijk te houden, binnen de gestelde budgetten. Er wordt een standaard gevolgd om security te stroomlijnen en te managen. Uw team werkt elke dag hard om systemen up-to-date te houden. Kortom, alles loopt naar wens. Dan wordt u, naast uw huidige taken, ineens ook verantwoordelijk voor de security van de Process Control omgeving, de fabrieksautomatisering, ofwel de Operational Technology binnen de organisatie.

U organiseert een eerste meeting met zowel uw it-mensen, als de collega's uit de fabriek. Naast enkele operators nemen onder andere de control engineers en system engineers, die verantwoordelijk zijn voor de Operational Technology (OT), plaats aan tafel. Terwijl de eerste discussies losbarsten, realiseert u zich dat de verschillen tussen IT en OT nog groter zijn dan gedacht. De computers binnen de Process Control omgeving draaien allemaal op Windows XP of Windows 2000 en worden dus niet meer ondersteund door Microsoft. Mooi, die krijgen allemaal een update naar Windows 7 en de eerste problemen zijn opgelost.

Verdeeldheid tussen IT en OT

Nadat de rust aan tafel enigszins is teruggekeerd, wordt u fijntjes te kennen gegeven dat u upgraden naar een ander Operating System, of zelfs maar het installeren van de laatste beschikbare security patches, wel uit uw hoofd kunt zetten. Want dan werkt de besturingssoftware misschien niet meer, of de garantie van de fabrikant vervalt. Zelfs een simpele reboot van het systeem is al uit den boze. In welke it-nachtmerrie bent u verzeild geraakt? De eerste visioenen van slapeloze nachten schieten al door uw hoofd.

"Dit is een heel herkenbaar scenario," legt Marcel Jutte, Managing Director bij Hudson Cybertec, uit. "IT en OT zijn twee compleet verschillende werelden. Om de security daarvan samen te brengen, is specifieke kennis, ervaring en samenwerking nodig." Jutte geeft twee voorbeelden: "Steeds meer apparatuur in de instrumentatielaag is IP-gebaseerd. Wie is verantwoordelijk voor het uitgeven van de IP-adressen voor die systemen? Hetzelfde geldt voor de firewall in het fabrieksdomein. Hoort deze bij IT of bij de Process Control omgeving en wie doet het beheer? Hiervoor is vanwege de specifieke kennis intensieve samenwerking nodig tussen beide domeinen. Hudson Cybertec treedt regelmatig op als intermediair tussen IT en OT en helpt als specialist bedrijven met het op orde krijgen van het beveiligingsniveau." Daarnaast is het belangrijk te weten wat er op het Process Control netwerk gebeurt. Een verkeerde waarde sturen naar een PLC kan al voor problemen zorgen. Monitoring van het dataverkeer is in deze omgevingen dan ook vaak cruciaal.

Verschillende security belangen

De belangen van IT en OT staan vaak lijnrecht tegenover elkaar. Dit is terug te voeren op de primaire doelstelling van security binnen beide domeinen. In de IT staat het bewaken van de confidentialiteit van informatie bovenaan de prioriteitenlijst. Integriteit en beschikbaarheid van systemen zijn daaraan vaak onderschikt. Met het terugzetten van een back-up zijn de meeste problemen eenvoudig op te lossen, terwijl een herstart van een server meestal alleen zorgt voor tijdelijke drukte bij de koffiemachine.

Binnen het OT domein zijn de belangen meestal omgekeerd. Er moet controle blijven over de processen, die soms niet gestopt kunnen worden zonder grote gevolgen. Security is hierdoor vaak inherent aan safety. Beschikbaarheid en zo ook integriteit worden dan belangrijker dan confidentialiteit. In Process Control omgevingen worden accounts regelmatig gedeeld door meerdere personen en belangrijke systemen staan vaak continu ingelogd. Operators moeten er niet aan denken dat zij te maken krijgen met 'loss of view' of 'loss of control' over het proces, waardoor zij in een noodsituatie niet onmiddellijk kunnen ingrijpen.

Weet waar de organisatie staat

Een van de eerste stappen is te onderzoeken waar de organisatie staat qua security in de Process Control omgeving. Dit gebeurt middels een assessment. Deze beschouwt alle relevante gebieden van de drie security pijlers: mens, organisatie en techniek. Het is als het ware een nulmeting, een ijkpunt waaraan effecten van veranderingen kunnen worden gemeten. Met een assessment kan worden bepaald wat de huidige status van security is in de procesomgeving, waar de kwetsbaarheden zitten en welke cybersecurityrisico´s de organisatie loopt. "Voordat tot een assessment kan worden overgegaan, is vaak nog werk te verrichten op het gebied van awareness," is de ervaring van Marcel Jutte. "Als security awareness ontbreekt bij het senior management, is budget voor verbeteren van de cyber security soms niet beschikbaar. Met het geven van awareness-sessies aan het senior management helpt Hudson Cybertec de ict-managers budget te verkrijgen voor cybersecurity van de Operational Technology."

Op weg naar meetbare resultaten

De resultaten van een security assessment geven een organisatie handvatten voor het verbeteren van de security binnen de Proces Control omgeving. Hudson Cybertec ondersteunt klanten gedurende het hele proces. "We helpen onze relaties vanaf de eerste awareness, via assessments, tot volledige implementatie en uitvoering van Cyber Security Management, als integraal deel van de bedrijfsvoering," zegt Jutte. "Cybersecurity is een continu groeiproces. Dreigingen veranderen en regelmatig worden er nieuwe kwetsbaarheden gevonden, of vinden er veranderingen plaats in de organisatie of gebruikte techniek. Goed Cyber Security Management verlangt dan ook dat periodiek gemeten wordt of de securitymaatregelen nog voldoen en welke aanpassingen nodig zijn."

Securitystandaard voor de industrie

Binnen IT geldt de ISO-27000 series standaard. Binnen OT wordt vaak de internationale ISA99/IEC 62443 standaard ingezet. De standaard, die een framework voor securitymaatregelen omvat, is volledig toegespitst op het gebruik binnen Process Control en technische omgevingen zoals DCS, ICS, SCADA en PLC omgevingen en gebouwgebonden installaties. In het security framework komen alle cybersecurityaspecten aan bod, van risico assessments en personele security, tot security management en evaluatie van de effectiviteit van veranderingen.

Klaar voor de toekomst

Met de implementatie van een Cyber Security Management methodologie in de organisatie volgens ISA99/IEC 62443, houdt u de controle over cybersecurity van de technische omgeving. U krijgt inzicht in de volgende stappen die uw organisatie moet nemen op gebied van cybersecurity en houdt op gestructureerde wijze het beveiligingsniveau op peil. Jutte besluit: "Security van de technische omgevingen is belangrijk en moet niet worden onderschat. Waak voor schijnveiligheid die ontstaat door het treffen van verkeerde maatregelen. Vraag advies bij een gespecialiseerde partij die een onafhankelijk advies kan geven. Zo kunt u security van OT ook in de toekomst met vertrouwen tegemoet zien."

Marcel Jutte,
Managing Director
bij Hudson Cybertec