Securitybeleid nodig, met oog voor menselijke factor en beheer

Techniek alléén is kansloos tegen cyberdreigingen

Het klinkt zo mooi: "Investeer flink in beveiligingsapparatuur voor uw technische infrastructuur en het komt allemaal goed." Helaas, zo komt het niet goed. Natuurlijk is het essentieel om voldoende technische maatregelen te treffen om de Industrial Control Systems (ICS) van het bedrijf te beveiligen tegen cyberdreigingen. Maar steeds blijken deze maatregelen slechts één van de puzzelstukjes te zijn in het geheel. Marcel Jutte, managing director van Hudson Cybertec, verklaart waarom.

Ron Teibeek

"Met techniek kan veel, maar niet alles", aldus Marcel Jutte. "Technische maatregelen kunnen slechts tot bepaalde hoogte bescherming bieden tegen menselijke fouten, onwetendheid of onvolledig beleid. Aanvullende maatregelen zijn daarom noodzakelijk. Security is gebouwd op drie pijlers die alle even belangrijk zijn. Deze pijlers zijn 'Mens', 'Organisatie' en 'Techniek'. Ze vullen elkaar aan en versterken elkaar."
De pijler 'Mens' beschouwt alle zaken die gerelateerd zijn aan awareness en menselijk gedrag op de werkvloer. Het spreekt voor zich dat ongetrainde werknemers fouten of verkeerde inschattingen kunnen maken omdat zij zich helemaal niet bewust zijn van dreigingen. Zij zijn niet in staat deze te herkennen, en weten niet hoe te handelen bij een mogelijke dreiging of hoe zij security-risico's tot een minimum kunnen beperken. 'Organisatie' richt zich op hoe het bedrijf omgaat met security. "Hierbij zijn het securitybeleid voor de technische omgeving, de aanwezige procedures binnen de organisatie en communicatie naar de betrokken werknemers belangrijke aandachtspunten", licht Jutte toe." Is Operations zich wel bewust van security? Industrial Control Systems, procesomgevingen of andere technische omgevingen stellen volledig andere eisen aan het securitybeleid dan een kantooromgeving. Terwijl op het gebied van safety de zaken vaak wel goed zijn uitgewerkt in het beleid, is dat op gebied van security veel minder vaak het geval."
Tot slot kijkt 'Techniek' naar alle technische maatregelen die getroffen kunnen worden om het securityniveau te verhogen. Dit betreft niet alleen apparatuur, maar ook zaken als scheiding van netwerken, antivirussoftware, technische infrastructuur, het op orde hebben van netwerktekeningen, enzovoort. Hoewel naar 'Techniek' vaak de meeste aandacht uitgaat, mag inmiddels duidelijk zijn dat dit onterecht is. De pijlers 'Mens' en 'Organisatie' zijn zeker even belangrijk.

Meten is weten

"Het is essentieel om een solide cybersecuritybeleid te voeren, waarin de drie securitypijlers geborgd zijn", vervolgt Marcel Jutte. "Het is daarom belangrijk te weten waar uw organisatie staat qua security. Daarvoor dient u het huidige niveau van cybersecurity binnen de technische omgeving van uw organisatie te kennen. Maar hoe bepaalt u dit huidige securityniveau en hoe ontwikkelt en implementeert u een solide cybersecuritybeleid voor uw technische infrastructuur?"
Jutte ziet veel van de bedrijven die met deze vragen worstelen, uiteindelijk terechtkomen bij Hudson Cybertec. "Door een security-assessment te laten uitvoeren door een onafhankelijke partij zoals wij, krijgen bedrijven een duidelijk en objectief beeld van de huidige staat van de security. Met het resultaat van een assessment kunnen bedrijven acties nemen om de juiste maatregelen te nemen voor beperking van de digitale risico's. Dit heeft een positieve uitwerking op de bedrijfscontinuïteit. Een security-assessment fungeert als nulmeting en maakt verbeteringen meetbaar. Meten is weten."

Assessments kunnen plaatsvinden op procedureel, organisatorisch of technisch niveau. Hudson Cybertec volgt bij assessments vaak de internationale securitystandaard ISA99/IEC 62443 (cybersecuritystandaard voor Industrial Control Systems), omdat hierin de drie securitypijlers goed worden afgedekt. Hierdoor ontstaat een volledig beeld van de situatie. Bedrijven kunnen er echter ook voor kiezen een assessment uit te laten voeren volgens sector- of eigen bedrijfsstandaarden, of deze te laten spiegelen aan de ISA99-IEC 62443 of een andere standaard. "Een van onze opdrachtgevers in de vitale infrastructuur wilde weten waar zij als organisatie staan op het gebied van cybersecurity voor de procesomgeving", geeft Jutte als voorbeeld. "We hebben de actuele situatie geaudit tegen het interne securitybeleid. Daarnaast hebben we het beleid zelf gespiegeld aan de ISA99/IEC 62443 standaard. Hieruit bleek een beperkte compliancy aan een onvolledige securitystandaard, een onwenselijke situatie. We hebben een geheel nieuw securitybeleid geschreven voor deze klant, waardoor zij over een eenduidig securitybeleid beschikken dat is toegespitst op de procesomgeving. Door dit beleid integraal op te nemen in de organisatie en te managen, hebben zij nu controle over hun security."

Management

Security is een continu proces dat verankerd moet worden in de bedrijfsvoering; het moet als het ware bij iedereen tussen de oren zitten. Security moet dan ook worden gemanaged, weet Marcel Jutte: "Door invloeden van binnenuit en buitenaf veranderen de securityrisico´s na verloop van tijd. Aanpassingen in de infrastructuur door bijvoorbeeld verplaatsen van apparatuur kunnen nieuwe risico's introduceren. En nieuwe manieren van werken, zoals BYOD, stellen de organisatie voor volledig nieuwe security-uitdagingen. Ook de dreigingen veranderen. Door de ontwikkelingen het afgelopen jaar, weten we dat andere landen grote interesse hebben in onze vitale infrastructuur. Het is daarom belangrijk periodiek inzicht te verkrijgen in de huidige risico's en het actuele dreigingsbeeld. Middels een security-audit ontstaat inzicht in welke mate de actuele situatie nog voldoet aan het beleid. De resultaten kunnen een opstap zijn naar aanpassingen."

Er zijn verschillende internationale standaarden en best practices voor cybersecurity en cybersecuritymanagement. "Sommige zijn gericht op de kantooromgeving en daardoor eigenlijk onbruikbaar binnen technische omgevingen", legt Jutte uit. "Andere zijn toegespitst op een bepaalde industriesector en daarom weer niet goed te gebruiken binnen andere sectoren. De ISA99/IEC 62443 cybersecuritystandaard biedt alle noodzakelijke elementen voor het opzetten van cybersecuritymanagement, specifiek voor technische omgevingen. Door security in een managementproces te gieten, zijn bedrijven in staat de security van de technische omgevingen te managen en te waarborgen. Wij ontzorgen onze klanten op securitygebied, vanaf awareness tot een goed gefundeerd en gemanaged security-beleid. Hierdoor kunnen zij de focus houden op hun core business."

Investeren in goede security is dus noodzakelijk, maar wel op de juiste manier. Belangrijk is om te weten waar de organisatie staat en ervoor te zorgen dat de drie pijlers van security de organisatie stevig ondersteunen. 'Techniek' alléén is kansloos tegen cyberdreigingen, maar indien ondersteund door de juiste maatregelen op de gebieden 'Mens' en 'Organisatie' wordt een organisatie weerbaar en de technische omgeving cybersecure.