De grens tussen IT en OT vervaagt

Op weg naar cybersecuritymanagement

De grens tussen IT en OT (Operational Technology) vervaagt. In het OT domein van vandaag en morgen hebben we geen machines meer met een IT component, maar hebben we te maken met complexe IT systemen die acteren op veranderingen in de fysieke wereld. Deze systemen zijn vaak volledig geïntegreerd in het proces.

Dit cyber-fysieke grensvlak is uniek ten opzichte van de IT wereld. Complexe chemische processen en gevaarlijke handelingen die op dit grensvlak verlopen, kunnen bij fouten zorgen voor serieuze HSE-incidenten. Cyber-fysiek vormt daarmee een business risico voor organisaties. Het is dan ook van groot belang om deze risico's in kaart te brengen en cybersecurity te gaan managen.

Hoewel er dus meer bewustwording is voor cybersecurity worstelen veel bedrijven nog met een belangrijke vraag: Waar moet ik beginnen? Marcel Jutte, managing director van Hudson Cybertec: "Waar bedrijven enkele jaren geleden nog tegen een gebrek aan awareness opliepen, zien we nu veelal een roep om concrete hulp om een start te maken met cybersecurity."

Een business case

Een internationaal chemiebedrijf heeft, net als vele anderen, de weg gevonden naar Hudson Cybertec. Ze zijn zich terdege bewust van de HSE consequenties die het primaire proces kan veroorzaken indien er cybersecurity-incidenten optreden, en het proces hierdoor in een onveilige toestand zou komen. Ook safety-PLC's kunnen het slachtoffer worden van een cyberaanval en daardoor niet meer, of anders werken dan verwacht. Dit kan grote (fysieke) gevolgen hebben. Het chemiebedrijf wilde cybersecurity gaan managen, maar had geen inzicht in de huidige securitystatus.

De nulmeting

Een security assessment heeft inzichtelijk gemaakt hoe het bedrijf er op dat moment voorstond. Deze nulmeting vormde een startpunt voor verbeteringen. Uit het assessment kwam duidelijk naar voren welke stappen de organisatie moest nemen om cybersecurity op het gewenste niveau te krijgen. Zo ontbrak een actueel securitybeleid en bijbehorende procedures. Daarnaast bleek het noodzakelijk om de securityorganisatie op een goede wijze in te richten. Om al deze zaken in goede banen te leiden, leverde Hudson Cybertec een interim-CISO die cybersecuritymanagement ingericht heeft en als klankbord voor het senior management van het chemiebedrijf fungeerde. Daarbij was aandacht voor zowel mens, organisatie en techniek.

Basis voor het cybersecuritymanagement vormt de IEC 62443, de internationale de facto norm voor cybersecurity van industriële automatisering & controle systemen. Hudson Cybertec wordt internationaal gezien als subject matter expert op dit gebied en is actief betrokken bij de normontwikkeling.

Prioriteiten stellen bij een beperkt securitybudget

Omdat de budgetten beperkt waren, zijn er prioriteiten gesteld voor het cybersecuritymanagement. Door het vastleggen van een scope heeft de organisatie richting gekregen voor security. Hierbij zijn keuzes gemaakt, waarbij het chemiebedrijf het meest profiteert van de verbeteringen. Zo werd er gekozen om duidelijke verantwoordelijkheden voor cybersecurity te beleggen in een compacte security organisatie en een securitybeleid met een basisset aan procedures op te stellen. Jutte zegt: "Er is daarbij slim gebruik gemaakt van zaken die er al waren en nog actueel waren, zoals een high-level risicoanalyse. Hierbij werd vooral gekeken naar de extra impact van cyber (en cyber-fysiek) op de high-level risico's voor de organisatie."

Duidelijkheid voor de organisatie

Door de securityorganisatie klein te houden, kan er snel worden geschakeld binnen de organisatie. Er is gekozen om vanuit verschillende disciplines input te geven in de organisatie. Hierdoor zijn zowel IT als OT vertegenwoordigd. Het nieuwe beleid en procedures zijn bewust beknopt gehouden. Het maakt voor alle medewerkers duidelijk wat van hen wordt verwacht op gebied van security, zowel op gebied van cyber als fysiek.

Goed getraind personeel vermindert de securityrisico's

De organisatie onderkent het belang van personeel om het niveau van cybersecurity omhoog te brengen. In samenwerking met het bedrijf heeft Hudson Cybertec een programma opgesteld voor het verbeteren van de security awareness bij de medewerkers. Het awareness programma zorgt ervoor dat de medewerkers van het chemiebedrijf zich beter bewust worden van de securityrisico's waarmee ze dagelijks te maken hebben. Hierdoor zijn de cybersecurityrisico's al afgenomen, terwijl het programma nog loopt. "Bij een security awareness programma is periodieke herhaling belangrijk." weet Jutte, "Na een tijdje worden medewerkers weer wat minder alert. Herhaling verankert de bewustwording bij de medewerkers."

Netwerksegmentatie

Op technisch vlak is besloten om de bestaande IT en OT infrastructuur te segmenteren. De bevindingen die gedaan waren tijdens de nulmeting gaven duidelijk aan hoe de segmentatie vorm gegeven kon worden. Het Zone & Conduit model uit de IEC 62443 fungeerde als leidraad bij het opstellen van een zonemodel. Met kleine investeringen was het mogelijk hier een grote verbetering in cybersecurity te bewerkstelligen.

Forensic readiness

Om de organisatie voor te bereiden voor als er toch een incident plaatsvindt, wordt er op dit moment gewerkt aan forensic readiness voor het chemiebedrijf. Hierbij worden zaken als logging en monitoring zodanig ingericht, dat in geval van een incident een juiste respons mogelijk is, terwijl het productieproces zo min mogelijk wordt verstoord. In aanloop naar de aankomende cybersecuritywet is het belangrijk dit soort zaken op orde te hebben.

Volgende stappen

Jutte: "Aan het einde van dit jaar gaan we wederom een meting doen van het cybersecurityniveau. We kunnen dan mooi inzichtelijk maken hoe effectief de verbeteringen zijn geweest die we hebben doorgevoerd in cyber security. We zien nu al hoe cybersecuritymanagement zijn vruchten afwerpt binnen de organisatie. Met een assessment kunnen we hetgeen we zien en voelen, ook kwantificeren." Hij sluit af: "Wij beschouwen al onze klanten als partners. Samen werken we aan het verbeteren van cybersecurity. We proberen onze partners daarbij zo veel mogelijk te ontzorgen."

Na een tijdje worden medewerkers weer wat minder alert. Herhaling verankert de bewustwording bij de medewerkers...