Beperken van cybersecurity risico's in productiefaciliteiten

Een compleet overzicht van kwetsbaarheden in haar productiefaciliteiten hielp een wereldwijd chemie concern om cybersecurityrisico's gericht te verkleinen. CGI onderzocht met een team van OT cybersecurity-experts de productie-faciliteiten.

Toen onze klant een cybersecurity-programma voor Operational Technology (OT) startte, was het doel van dit programma het voorkomen van:

- Onveilige situaties als gevolg van cybersecurity incidenten
- Verstoring van productie of fabrieksomgeving of ransomwareaanvallen
- Verlies van intellectueel eigendom, productkwaliteit en reputatieschade

De uitdaging

De meeste bedrijven hebben veelal niet alle expertise en capaciteit direct beschikbaar om cybersecurity dreigingen effectief aan te pakken. Een van onze klanten had behoefte aan specifieke expertise en een algeheel overzicht van alle cybersecurity risico's en maatregelen om de bedreigingen en kwetsbaarheden in de fabrieken te adresseren. Dit betrof alle computersystemen voor operationele technologie die worden gebruikt om de productie te sturen en te beheren. Deze industriële controlesystemen (ICS) omvatten doorgaans systemen zoals Manufacturing Execution Systems (MES), Supervisory Control and Data Acquisition (SCADA) -systemen, Distributed Control Systems (DCS) Programmable Logic Controllers (PLC's) en Safety Instrumented Systems (SIS). ICS'en zijn doorgaans bedrijfskritische applicaties met navenant hoge beschikbaarheidseisen.

De oplossing

CGI werd geselecteerd om deze assessments uit te voeren op basis van de langdurige en vertrouwde relatie op het gebied van security. Een team van OT cybersecurity experts van CGI beoordeelde de fabrieken op basis van de OT cybersecurity standards & practices van de klant, waarbij deze klant zelf aan elke locatie een eigen en specifiek complexiteitsniveau toewees, te weten: laag, gemiddeld of hoog. Deze classificatie was gebaseerd op het aantal te beoordelen systemen, de lokaal beschikbare expertise en het belang van de locatie voor de klant.

Voor elke classificatie is door CGI een uniforme, maar op maat gemaakte aanpak ontwikkeld om de assessments uit te voeren.

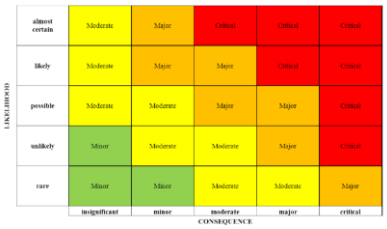
OT / ICS CYBERSECURITY ASSESSMENTS omvatten

- Planning
- Informatie verzamelen
- Site bezoeken en beoordelen
- Rapportage
- Aanbevelingen

Voorafgaand aan de locatiebezoeken werden de locaties ondersteund door een voorbereidingsteam van CGI om ervoor te zorgen dat alle vereiste informatie, zoals netwerkdiagrammen en asset informatie, tijdig beschikbaar was voor het assessment.

CGI voerde de assessments uit met meerdere on-site assessor-teams gespecialiseerd in OT cybersecurity. De assessments omvatten gestructureerde interviews, inspectie van de fysieke beveiliging, analyse en beoordeling van het OT / ICS-netwerk, de netwerkverbonden OT-systemen en de processen voor anti-malware, identiteits- en toegangsbeheer, firewalls en externe toegang.

De assessments gaven een duidelijk inzicht in de volwassenheid van het OT cybersecurity-beleid, de manier waarop dit beleid was geïmplementeerd en de maatregelen die genomen zouden moeten worden met betrekking tot eventuele bevindingen.



Het evaluatierapport omvatte een Business Impact Assessment voor elk systeem, een risico-beoordeling en een compliance-tracker, met specifiek advies ten aanzien van risicobeperking voor elk van de bevindingen.

De beoordeling met daarin de risico's, waarschijnlijkheid en bedrijfs-impact alsook aanbevolen risico beperkende maatregelen zijn voorzien van een prioriteit en hebben de klant geholpen haar OT / ICS-cybersecurityprogramma voor de verdere toekomst te bepalen.

Waarom CGI

Klanten kiezen voor CGI vanwege haar kennis en ervaring in missie-kritische omgevingen en OT Cybersecurity - als ook de benodigde capaciteit en het vermogen om fabrieken en de bedrijfsoperatie wereldwijd te kunnen beoordelen, met een uniforme aanpak en binnen de afgesproken planning. CGI kan daarbij verschillende cybersecurity-experts leveren met de benodigde diepgaande kennis op het gebied van industriële productie systemen en processen.

Over CGI in cybersecurity

CGI heeft ruim 40 jaar ervaring in het ontwikkelen en beveiligen van missie kritische systemen in complexe omgevingen over de gehele wereld, inclusief defensie- en veiligheidsdiensten. We investeren in het borgen van onze kennis en kunde, in nauwe samenwerking met internationale veiligheids- en normalisatie-instellingen. Hoewel cyberdreigingen wereldwijd zijn, weten we dat vereisten lokaal verschillen en de uitdagingen uniek zijn voor elke organisatie. Door middel van diepgaande technische en zakelijke expertise, onze eigen cybersecurity operations centers, best practices en frameworks, werken we eraan om ervoor te zorgen dat veiligheid onderdeel uitmaakt van alles wat we doen en niet als bijzaak wordt gezien.

"... de maakindustrie is een van de meest kwetsbare en meest getroffen industrieën als het gaat om cyberaanvallen"

Over CGI

CGI, opgericht in 1976, behoort tot de grootste IT en business consultancy bedrijven ter wereld. Wij werken op basis van inzichten en resultaat om het rendement van uw investeringen te maximaliseren. In 17 bedrijfstakken op 400 locaties wereldwijd bieden we uitgebreide, schaalbare en duurzame IT- en business consultancy diensten die wereldwijd beschikbaar worden gesteld en lokaal worden geleverd.

Voor meer informatie
Bezoek cginederland.nl
Mail ons via info.nl@cgi.com