OT Cybersecurity-inzichten om de risico's effectief te beperken

Een overzicht van kwetsbaarheden hielp Jacobs Douwe Egberts (JDE) om risico's te mitigeren, door de adequate mitigatiemaatregelen te implementeren. CGI bleek een betrouwbare partner in OT / ICS-beveiliging, waarde toe te voegen en de cyberbeveiliging van de fabriek te verbeteren en daarmee de risico's te verminderen.

JDE maakt deel uit van JDE Peet's, 's werelds grootste pure-play koffie- en theebedrijf, met hoofdkantoor in Nederland en een uitgebreid portefeuille van wereldwijde, regionale en lokale merken.

In 2017 werd een van de merken getroffen door een malware-incident die een verstoring veroorzaakte in de wereldwijde productie, verzending en facturering en dat gedurende meerdere dagen, resulterend in een verlies van € 100 miljoen. Dit was een belangrijke trigger om in alle fabrieken een cybersecurityprogramma te starten over de gehele Operational Technology (OT) / ICS-omgeving.

De uitdaging

Het is geen geheim dat de maakindustrie een van de meest voorkomende is als het gaat om cyberaanvallen. Er is veelal onvoldoende diepgaande kennis en capaciteit om cyberbeveiligingsbedreigingen effectief aan te pakken. JDE had behoefte aan deskundig inzicht alsook overzicht van alle relevante cyberbeveiligingsrisico's en mogelijkheden om bedreigingen en kwetsbaarheden in fabrieken te beperken. Deze uitdaging omvatte alle OT computersystemen die worden gebruikt om de gehele industriële operatie te besturen en te beheren.

De oplossing

Om de OT / ICS-omgevingen in fabrieken te beoordelen, gebruikte CGI haar OT Security Assessment. Deze aanpak geeft inzicht in de volwassenheid van het bestaande OT-beveiligingsbeleid en de manier waarop dit beleid is geïmplementeerd. Deze aanpak omvat goed voorbereide locatiebezoeken, gestructureerde interviews met relevante medewerkers, toetsing van de fabriek aan de IEC62443-standaard en een OT/ICS netwerktopologiescan.

Gespecialiseerde apparatuur wordt aangesloten op het OT / ICS-netwerk voor geautomatiseerde asset discovery en om een topologiekaart te genereren die alle relevante assets en onderlinge relaties toont. Op specifieke cybercrimegevoelige gebieden wordt ook dataverkeer gecontroleerd.

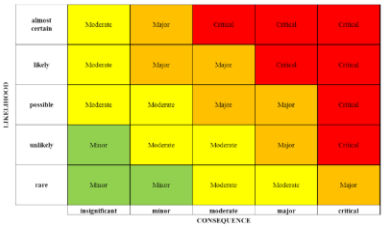
Een OT / ICS Cyber Security Assessment omvat doorgaans:

- Maturity assessment
- IEC62443 / NIST800 assessment
- Validatiefase in de fabriek
- Discoveryfase in de fabriek, met aandacht voor zowel fysieke als logische OT / ICS-beveiliging en gedocumenteerde bevindingen
- OT / ICS-netwerkscan en analyse, inclusief detectie van assets, anti-malwarelandschap, identiteits- en toegangsbeheer, firewalls alsook toegang op afstand

JDE
JACOBS DOUWE EGBERTS

CGI OT-beveiligingsbeoordelingen zijn gebaseerd op relevante wereldwijde ICS-conformiteitsnormen zoals NIST en ISO/ISA/IEC.

CGI voert beoordelingen uit met meerdere on-site teams (met elk twee beoordelaars) gespecialiseerd in OT-beveiliging, met een uniforme aanpak voor consistente rapportage. Voorbereiding alsook firewall- en netwerkanalyse, evenals OT / ICS-architectuurevaluatie werden verzorgd door het CGI OT Security Center of Excellence.



Op verzoek van JDE is voor elk specifiek mitigatieadvies een risico-inventarisatie en risico-heatmap, mitigatieadvies en budgetindicatie opgenomen in het beoordelingsrapport.

De risicobeoordeling, die naast de risico's, ook waarschijnlijkheid en impact omvatte, is met de geadviseerde mitigaties van een prioriteit voorzien wat JDE in staat heeft gesteld om OT / ICS-cyberbeveiligingsprioriteiten te definiëren.

Bewustzijn verhogen

Naar aanleiding van de beoordelingen en rapportage is een OT / ICS cybersecurity awareness video gemaakt op basis van bevindingen van de on-site assessments. Deze video is aangeboden aan fabrieks-medewerkers voor trainingsdoeleinden.

Waarom CGI?

JDE selecteerde CGI vanwege capaciteit in missiekritieke omgevingen en relevante OT cybersecurity-expertise om alle JDE-fabrieken wereldwijd te beoordelen, met een uniforme aanpak en binnen het gestelde tijdsbestek. CGI zorgde voor een team van specialisten met diepgaande kennis op het gebied van procesbesturing.

Na de beoordelingen kreeg CGI van JDE de opdracht om relevante risicobeperkende maatregelen te implementeren. Door de weerbaarheid van de fabrieken te verbeteren, is CGI een betrouwbare partner gebleken in OT / ICS-beveiliging.

Over CGI in cyberbeveiliging

CGI heeft ruim 40 jaar ervaring in het ontwikkelen en beveiligen van kritieke bedrijfssystemen in complexe en missiekritieke omgevingen over de hele wereld, inclusief defensie- en inlichtingensectoren.

We investeren in onze referenties en werken nauw samen met internationale veiligheidsverenigingen en normalisatie-instanties. Hoewel cyberdreigingen wereldwijd zijn, weten we dat de vereisten lokaal variëren en dat de uitdagingen uniek zijn voor elke organisatie. Door deskundig talent, diepgaande technische en industrie kennis, centra voor beveiligingsoperaties, best practices en frameworks, zorgen we ervoor dat controles worden ingebakken, niet zomaar toegevoegd.

Over CGI

CGI, opgericht in 1976, behoort tot de grootste IT- en business consultancy bedrijven ter wereld. CGI is actief op honderden locaties over de hele wereld en levert end-to-end diensten en oplossingen, waaronder strategisch IT- en business consultancy, systeem-integratie, managed IT en diensten op het gebied van bedrijfsprocessen.

Voor meer informatie

Bezoek cginederland.nl

Mail ons via info.nl@cgi.com