International virksomhed opnår cybersikkerheds-certificering på rekordtid og styrker sin konkurrenceevne markant

Certificeringen er en blåstempling af virksomhedens cybersikkerhedsstyrke og giver kunderne et signal om, at de trygt kan købe deres produkter.

I en verden, hvor snart sagt alting eksisterer og opererer på digitale præmisser, stiger risikoen for cyberangreb også. Det garderer man sig i EU imod ved at lovgive om IT-sikkerhed (information technology security) og OT-sikkerhed (operation technology security).

Særlige krav til kritisk infrastruktur

Som leverandør til bl.a. vandforsyninger hører virksomheden til en del af Danmarks *kritiske infrastruktur*. Det betyder, at virksomheden skal opfylde en række særlige sikkerhedskrav, bl.a. NIS2, som handler om generel it-sikkerhed, og EUCRA (EU Cyber Resilience Act), som gælder fysiske produkter, der er koblet til digitale kommunikationsenheder. Også andre EU-lovgivninger som AI Act og Data Act er i spil.

Lovkrav opfyldes rammeværk

Bag ved lovkravene ligger en række standarder, som man bruger til at opfylde reglerne. ISA/IEC62443 er en af de vigtigste standarder inden for OT-sikkerhed med en cerificering i den første delstandard, ISA/IEC62443-**4-1**, opfylder virksomheden ikke alene europæiske lovkrav, men også intentionerne i alle andre globale lovgivninger.

"Når man er en verdensomspændende virksomhed, bliver det både for uoverskueligt og for usammenhængende at skulle fokusere på alle landes individuelle lovgivninger. Nu har vi indført en standard, så vi opfylder alle intentioner på tværs af internationale lovgivninger. Man kan sige, at vi helgarderer samtidig med, at vi fremtidssikrer," fastslår repræsentant fra virksomheden.

Certificering på rekordtid

Arbejdet med certificering begyndte i foråret 2024 og forventede egentlig at være i mål i Q2 2025 eller – hvis optimismen blev skruet i vejret – Q1. Men allerede i december 2024 var certificeringen en realitet. Forklaringen er, ifølge virksomheden, at man hele tiden har haft fokus på at drive arbejdsprocessen effektivt og formået at tænke ud af boksen og se alternative løsninger undervejs.

Endnu højere sikkerhedsmål

I første omgang koncentrerede virksomheden sig om at få ISO27000-rammen på plads. Dernæst kom første del af ISA/IEC-standarden, -4.1, i hus., hvormed virksomheden rangerer på modenhedsniveau 2, hvilket er højt, når det gælder modenhed inden for OT-sikkerhed.

Men virksomheden har nu besluttet sig for at gå efter modenhedsniveau 3. Det er en direkte billet til at opfylde kravene i Cyber Resilience Act, som træder i kraft i december 2027. Hvis en virksomhed til den tid ikke opfylder kravene, kan den ikke anvende CE-mærket på sine produkter – og det sætter i sidste ende en stopper for, at kunderne køber dem. CE-mærket er nemlig et bevis på, at man også i sin OT-sikkerhed har styr på dokumentation, processer, kontroller og den organisatoriske forankring.

Unikt samarbejde

Certificering er kommet i hus gennem et utraditionelt samarbejde med fire selvstændige konsulenter. I den indledende fase af projektet var der tilkoblet et stort konsulenthus, men virksomheden besluttede, at det optimale ville være at samle fire stærke profiler med spidskompetencer inden for hvert deres felt: Programledelse, projektledelse, subject matter expertise og organizational change management.

"Vi vil ikke hvile på laurbærrene. Der er ingen tvivl om, at vi hurtigt, effektivt og med en høj grad af kvalitet og professionalisme har nået et vigtigt skridt på vejen mod den bedst mulige OT-sikkerhed. Men verden er i forandring, trusselsdynamikkerne ændrer sig hele tiden, og vi er også en organisation i konstant bevægelse. Så ud over at vi nu stiler efter det næste modenhedsniveau, har vi et skarpt øje på alt, der handler om at pleje, tilpasse og forbedre det, vi allerede har opnået inden for sikkerhed," siger repræsentant fra virksomheden.