CENTER FOR CYBERSIKKERHED

Ledelsens opgaver i forbindelse med sikring af industrielle kontrol-systemer

Anvendelse af it-systemer til styring og overvågning af fysiske systemer i industriel produktion og kritisk infrastruktur, giver nye muligheder for forretningen. Men medfører også nye driftsmæssige risici.

Effektiv og sikker teknologianvendelse kræver forståelse og bidrag fra alle i organisationen. It-sikkerhed kan ikke laves effektivt af én afdeling eller ét kontor i en virksomhed, men beror på en løbende dialog, så medarbejderne ved, hvad forretningen skal kunne, hvornår og med hvilke ressourcer, og ledelsen ved, hvad der er muligt, realistisk og hensigtsmæssigt fra et teknisk og et praktisk perspektiv.

Center for Cybersikkerhed anbefaler, at it-sikkerhed integreres i risikostyringen i alle virksomheder, og at man overvejer at samle forretningsspecifik risikovurdering og it-risikovurdering i en fælles organisation.

For at sikre den nødvendige dialog i forretningen bør ledelsen tage ansvar for følgende opgaver:

1. Definer mål for it-sikkerhed, så medarbejderne ved, hvad de skal arbejde for, og hvilke krav de skal efterleve. Dette kan udmøntes i politikker og strategier, samt evt. implementering af relevante sikkerhedsstandarder som ISO 270XX, IEC 62443, NIST eller anden relevant standard.
2. Foretag helhedsorienterede risikovurderinger, der definerer og risikovurderer alle forretningskritiske processer.
3. Etabler en organisering, der sikrer, at it-sikkerhed styres på samme måde som andre forretningsrisici.
4. Etabler og vedligehold et overblik over systemerne, således at sammenhæng mellem systemers funktioner, komponenter og delsystemer er tydelig. Som en del af dette overblik bør man fastlægge intervaller for softwareopdateringer samt risiko- og sårbarhedsvurderinger.
5. Ved implementering af nye systemer skal hele livscyklussen klarlægges og gennemtænkes. Opstart, anvendelse, drift og

afvikling skal tænkes ind i systemet fra start. Dette er særligt vigtigt for industrikontrolsystemer, da der ofte er tale om kostbare systemer, der forventes at have en lang levetid.

6. Gør medarbejderne bevidste om, at de arbejder i en virksomhed, hvor it-risici er lige så vigtige som andre forretningsrisici. Gennem løbende dialog opnås et bedre billede af forretningens mål og risici, så medarbejderne kan tage ejerskab af såvel risici som forretningen, og medarbejderne kan bidrage med bekymringer og gode ideer.
7. Tag ansvar for bemyndigelse af roller og opgaver til medarbejderne, så adgangsstyring såvel fysisk som digitalt kan styres efter ledelsens beslutning og anvisning.
8. Rekruttér, organisér og videreuddan med en strategisk målsætning for øje. It-sikkerhed kan ikke outsources eller løses ved ansættelse af én medarbejder, men er en indlejret del af forretningen.

CENTER FOR CYBERSIKKERHED

Kastellet 30
2100 København Ø
Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk