Industriel Sikkerhed i Søgelyset

Fordi sikringen af flere kompetencer til OT-sikkerhed er et *fælles* ansvar

White Paper / Efterår 2023

> For efterspørgslen på cyber- og informations sikkerhedskompetencer er stor, men både myndigheder og virksomheder oplever, at det er vanskeligt at skaffe de rette profiler til opgaverne. Der er derfor behov for at styrke udbuddet af kompetencer, hvis sikkerheden skal løftes bredt set
>
> National strategi for cyber- og informationssikkerhed 2022-2024: 23

Resume

Efterspørgslen på kompetencer indenfor cybersikkerhed, er en kendt problemstilling. Situationen er dog vokset sig særlig kritisk indenfor industriel sikkerhed, også kendt om OT (Operationel Teknologi) sikkerhed, der omhandler sikkerheden af fysiske produktionsmiljøer, herunder samfundskritiske funktioner, der kommet i søgelyset for cyberkriminalitet og terror. Her er kompetencemanglen endnu større.

Det skyldes flere årsager.

Regeringens indsats for at styrke udbuddet af kompetencer, har primært været på cyber og informationssikkerhed indenfor IT, og langsigtede indsatser målrettet længerevarende akademiske uddannelser. I modsætning til 'IT-sikkerhed' er OT-sikkerhed i dag et område med få uddannelsestilbud. Problemstillingen er tilspidset af en 'underviser flaskehals', hvor der findes alt for få specialister med viden på området, som kan stå til rådighed for undervisning og træning.

OT-sikkerhed har som fagområde ikke haft stærke sponsorer i organisationerne. Ejerskabet har haft tendens til at falde mellem to stole ofte mellem IT og Produktion med konsekvensen, at ingen forpligter vigtige medarbejderne i tilegnelsen af viden på området.

For at øge udbuddet af kompetencer til industriel sikkerhed, ses et behov for flere kortsigtede indsatser, der kan imødekomme den aktuelle efterspørgsel. For at bremse en negativ udvikling, må der samtidig ske en langsigtet indsats for at bringe OT-sikkerhed på uddannelsesskemaet for dem, der vil udgøre den fremtidige arbejdsstyrke.

Ovennævnte vil dette White Paper præsentere løsninger til.

Indholdsfortegnelse

Indledning

Kære produktionsvirksomhed,

Hvad skal man prioritere blandt alle forretningskritiske områder på agendaen, når man driver virksomhed og kritisk produktion i 2023? Hvad er vigtigst, når du skal navigere i en omskiftelig verden, hvor den teknologiske udvikling medfølger nye muligheder, men også nye sårbarheder?

Du skal forholde dig til bl.a. nye lovkrav og reguleringer givet den nye maskineforordning og NIS2, geopolitik, bæredygtighed, digitalisering, og cybersikkerhed. Ikke mindst, skal du forholde dig til den moderne forbrugere, hvor faren for en ødelæggende shitstorm lurer, hvis din virksomhed ikke lever op til principper om ansvarlighed og bæredygtighed.

Sandheden er, at din forretning - helt ude på fabriksgulvet - er blevet digital, givet et konstant fokus på økonomi, effektivisering, optimering og automatisering. Den øgede forbundethed mellem nyt og gammelt og behovet for indsigt til at kunne træffe rette beslutninger, betyder samtidig at din forretningens sårbarheder i højere grad får digitale vinkler, hvorfor cybersikkerhed med god grund fortjener din højeste bevågenhed.

Du investerer sikkert i oprustningen af cybersikkerhed, herunder i services, teknologier og certificeringer, for at efterleve compliancekrav og styrke din virksomheds forsvar og modstandsdygtighed. Men når din investering også ud i produktionsmiljøet og ud til anskaffelsen af vigtige cyber kompetencer i din organisation?

Cybersikkerhed ikke kun en opgave, der bor i 'IT sikkerhed', men også i de funktioner, som har processer eller arbejdsgange, der linker til den fysiske (og kritiske) produktion. I disse miljøer gælder principper om stabilitet og tilgængelighed, der stiller helt andre krav til arbejdet med cybersikkerhed. Hvad gør du der?

For du finder det muligvis svært at få øje på uddannelse og træning målrettet medarbejdere, der beskæftiger sig med drift, vedligeholdelse og udvikling af den fysiske og kritiske produktion. Vi ved at disse medarbejdere er blevet centrale for at gøre din virksomhed modstandsdygtig og leverancesikker i en digital virkelighed, hvorfor vi er gået sammen på tværs af branchen for at præsentere løsninger, der kan hjælpe din virksomhed med investere i den vigtigste ressource - medarbejderne.

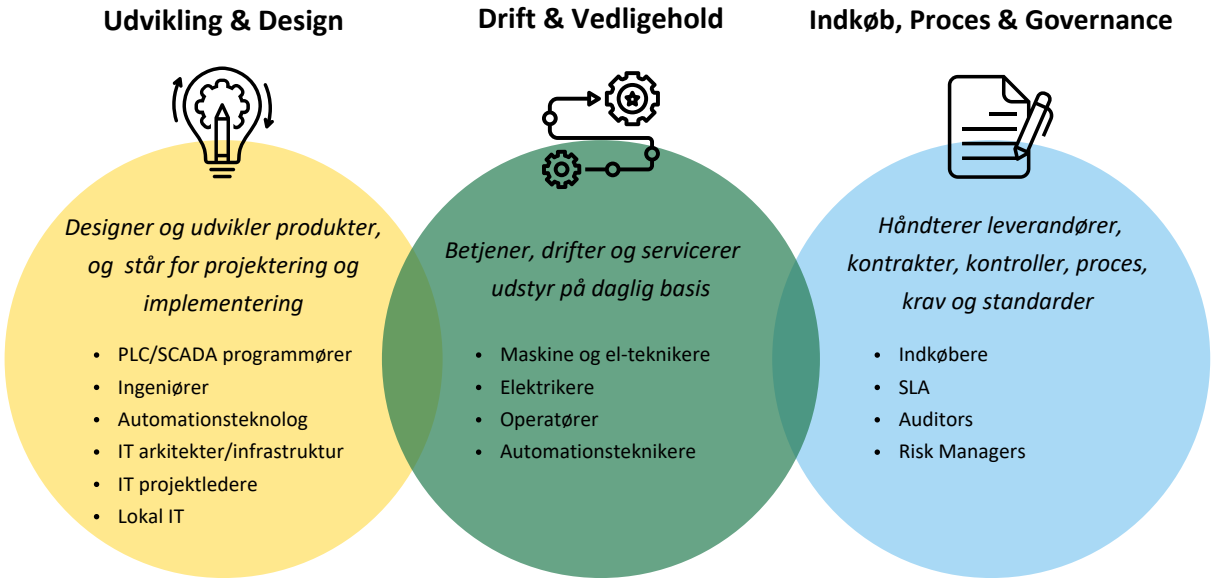
Med venlig hilsen *Arbejdsgruppen for OT-sikkerhed*

Om arbejdsgruppen

På baggrund af den aktuelle problemstilling, er følgende virksomheder og uddannelsesinstitution; Danish Crown, Danfoss, Siemens, Norlys, DIN forsyning, ICS Range, Treschow&Son og Syddansk Erhvervsskole gået sammen i en arbejdsgruppe med formålet om, at øge udbuddet af kompetencer indenfor industriel sikkerhed (OT sikkerhed).

Norlys, Danish Crown, Danfoss, DIN forsyning og Siemens repræsenterer brancherelevante virksomheder indenfor energi, fødevare, forsyning og leverandør, hvor problemstillingen udspiller sig. ICS Range repræsenterer specialister og eksperter indenfor OT-sikkerhed, der sideløbende underviser og researcher trends og sårbarheder i anvendt OT-udstyr. Treschow&Son repræsenterer en cyber talent supply virksomhed med indsigt i branchens udbud og efterspørgsel.

Arbejdsgruppen har identificeret et særligt behov for OT-sikkerhedskompetencer indenfor tre målgrupper, som fremgår af nedenstående Figur 1.



Figur 1 - Identificerede målgrupper for OT-sikkerhedskompetencer

Det vurderes at målgruppen 'Drift & Vedligehold' er størst, samt at målgruppen 'Udvikling & Design' er mest akut for at bremse OT-sikkerheds udfordringer i tidlige projektfaser. Eftersom institutioner som International Society of Automation (ISA) tilbyder en række kurser til målgruppen 'Indkøb, Proces & Governance', samt efterspørgslen fra industrien er størst indenfor 'Udvikling & Design' samt 'Drift & Vedligehold', er arbejdsgruppen fokus primært, men ikke udelukket, på initiativer rettet mod de to sidstnævnte målgrupper.

Hos 'Udvikling & Design' målgruppen er cybersikkerhed kommet på agendaen, men der er behov for at branchen stiller OT-sikkerhedsspecialister til rådighed for at styrke forståelsen for arbejdet i praksis. Hos 'Drift & vedligehold' målgruppen findes kurser leveret af fx Siemens og SektorCERT, men eftersom målgruppen rummer den største beskæftigelse, er der behov for flere initiativer, der løfter opgaven.

> Vi har automationsteknikere og el-teknikere, som vedligeholder og servicerer vores maskiner, men som i deres uddannelse ikke har stiftet noget kendskab til cybersikkerhed. Dét vi har brug for er, at udvikle sikkerhedskompetencer hos dem, der står nede i OT miljøet og i den daglige drift.

Henning Winter, CISO, Danish Crown

> Problemet er, at vi lige nu ikke kan finde eller hyre nogen i Danmark, der har de skills, som vi har behov for. Men med initiativer som fx 'Train the Trainer' kan vi give vores egne folk viden på området, som de kan føre videre internt i organisationen i tråd med virksomhedens værdier. Jeg ser et stort potentiale for dette koncept, da det kan bruges internt i forskellige virksomheder med stor effekt.

Henrik Christensen, Head of Smart Manufacturing, Danfoss

> Vi bliver nødt til at uddanne de folk, der har fingrene helt nede i OT. Ingen kan løfte den opgave alene. Det kræver skalering og et samarbejde på tværs af branchen. Jeg håber at vi med arbejdsgruppens initiativer, får sat skub i flere uddannelser, der passer til de forskellige niveauer i hele OT økosystemet - lige fra de, der designer og bygger maskinerne, til de, der efterfølgende skal servicere dem. Det er vigtigt at få dækket hele paletten.

Morten Kromann, Head of Industrial Security - RC, Siemens

Løsningen

Udfordringen er både nutidig og fremtidig, hvorfor der er behov for kort såvel som langsigtede strukturelle indsatser for at sikre tilstrækkelige kompetencer til området.

Med fingeren på pulsen over de aktuelle kompetencemæssige udfordringer, er det væsentligt at mobilisere virksomhederne på tværs af industrien i indsatsen. De har mulighed for at bidrage med kompetente specialister, som undervisere, samt sikre at kompetenceudviklingen matcher behovet.

Arbejdsgruppen har identificeret tre indsatser for at imødekomme det aktuelle og fremtidige behov:

1. Industriel Sikkerhed på Erhvervsuddannelserne
2. Train the Trainer
3. Industriel Sikkerhed kurser for Begyndere og Øvede

De tre indsatser er uddybet i følgende afsnit.

Industriel Sikkerhed på Erhvervsuddannelserne

Indsats: kortsigtet og langsigtet

Beskrivelse: Denne indsats fokuserer på at at styrke kommende og aktuelle arbejdsstyrke ved at aktivere erhvervsuddannelsesinstitutionerne og bringe OT-sikkerhed på uddannelsesskemaet, herunder integreret på AMU kurser målrettet faglærte og ufaglærte i industrien.

Hvorfor? Erhvervsuddannelserne har cybersikkerhed på agendaen, men de mangler dybde, aktualitet og en mere praktisk øvelsesbaseret tilgang til læring. OT-sikkerhed kan med fordel sidestilles med 'god virksomhedspraksis' og kan som en del af AMU opnå en skalering, der gavner virksomheder og samfund.

Målgruppen: Faggrupper, der arbejder med vedligeholdelse og servicering af teknisk produktionsudstyr, og dermed en gruppe der har adgang til kritiske systemer. Det gælder bl.a. elektrikere, industrioperatører, industriteknikere, automatikteknikere og data teknikere.

I**ntentionen:** Få OT-sikkerhed integreret i pensum sidestillet med industriens krav til 'Safety' og integreret i erhvervsuddannelsers forståelse af hvad, der betegner et et ansvarligt og 'sikkert' arbejdsmiljø i dag.

Yderligere anbefalinger om relevante tiltag for erhvervsskolerne på OT-sikkerhed kan findes i appendix.

Train the Trainer

Indsats: kortsigtet

Beskrivelse: Denne indsats fokuserer på den aktuelle arbejdsstyrke og imødekommelsen af udfordringen med 'underviser flaskehalsen'.

Hvorfor? Med få OT-sikkerhedskompetencer i industrien er underviserne også få. Det er samtidig omkostningsfuldt og svært at sende alle medarbejdere på uddannelse og kurser af hensyn til den daglige drift. 'Train the Trainer' konceptet skaber en fleksibel og skalerbar måde for virksomhederne at sikre den interne opkvalificering. Ved at oplære trænere internt, opnår virksomhederne en multiplikator effekt idet de på én og samme tid får udviklet og fastholdt vigtige medarbejdere.

Målgruppe: Interne medarbejdere heriblandt programmører, ingeniører, automationsteknologer, IT-arkitekter, IT-projektledere, lokal IT, Maskine og el-teknikere, elektrikere, operatører, automationsteknikkere, indkøbere, auditors, Risk managers, SLA, der kan og har potentiale for at varetage træning og undervisning af kollegaer.

Forløb: 4 undervisningsdage + eksamen fordelt på to uger. Der vil være vægt på praktiske øvelser for at sikre at læring på begynderniveau er integreret. Derudover skal der undervises i Formidling og Præsentationsteknik.

Intentionen: Flere undervisere, der udover den interne træning i virksomhederne, kan fungere som vigtige ambassadører for OT-sikkerhed – også som en undervisningsressource på uddannelserne.

Industriel Sikkerhed for Begyndere og Øvede

Indsats: kortsigtet

Beskrivelse: Denne indsats er rettet mod den aktuelle arbejdsstyrke og imødekommer behovet for et øget udbud af kurser på forskellige niveauer.

Hvorfor? For at øge udbuddet af kvalificerede kurser, hvor praktiske øvelser og eksempler fra den virkelig verden gør OT-sikkerhed relevant for den enkeltes dagligdag.

Målgruppe: Her fokuseres på medarbejdere, der arbejder med drift og vedligehold af produktionsudstyr bl.a. el-teknikere, elektrikere, operatører, automationsteknikkere, supportere.

Forløbet foregår som 2 dages kursus - en kombination af undervisning og praktiske øvelser. På Begynder kurset introduceres deltagerne til grundlæggende begreber og principper indenfor OT-sikkerhed. På Øvede kursus videreudvikler deltagerne deres færdigheder. Undervisningen er dialogbaseret og praktiske øvelser er en gennemgående og central del af undervisningen.

Intention: Undgå at gøre OT-sikkerhed for teoretisk, samt hurtigt øge vigtige medarbejdernes forståelse og kompetencer på området. Ikke mindst, er det intentionen at facilitere viden og sparring mellem fagfolk til gavn for løsninger og perspektiver på lignende problemstillinger på tværs af industrien.

Inspirationshistorier fra branchen

En række virksomheder har valgt at dele ud af deres erfaringer med både interne og eksterne undervisningsprogrammer og initiativer, der styrker deres medarbejdernes samarbejde, kompetencer og interesse for arbejdet med OT-sikkerhed. De er beskrevet her til inspiration.

Norlys

Som leverandør af landsdækkende kritisk infrastruktur, er OT-sikkerhed højt på agendaen i Norlys. Virksomheden har skabt et cybersikkerhedscommunity bestående af pt. 50 medarbejdere, der finder IT/OT-sikkerhed spændende og som derigennem får tilbudt forskellige træningsforløb og kurser indenfor feltet. For at skabe intern awareness omkring OT-sikkerhed, samler Norlys medarbejdere på tværs af afdelinger på en række kursusforløb for at styrke kommunikationen og forståelsen omkring problemstillinger. Nedenstående er et eksempel.

Introduktion til OT-sikkerhed for IT drift og GRC medarbejdere
En OT-sikkerhedsekspert sammensatte en dag, der introducerede begge funktioner, der ikke har noget kendskab til OT-sikkerhed, til vigtige begreber, samt om vigtige forskelle mellem OT og IT sikkerhed. Det særligt positive var at GRC teamet fandt sessionen utrolig givende og mente Compliance teamet skulle med næste gang.

“Når det bliver konkret og praktisk, er det dér, det giver noget læring. Selvom folk har forskellige forudsætninger for at forstå OT-sikkerhed, og nogle synes det er meget svært, har det givet en bredere forståelse på tværs af vores teams” - Martin Hansen, OT Security Manager, Norlys

TV 2 Danmark

Med landsdækkende Public Service-forpligtelser, er TV 2 Danmark en del af kritiske broadcast infrastruktur. TV 2 Danmark har netop igangsat en decentralisering af den operationelle cybersikkerhed, med stiftelsen af det foreløbigt første ‘Cybersecurity Guild‘ med udvalgte system specialister som aktive deltagere. Dette initiativ skal sikre større ejerskab og vidensdeling af cybersikkerhed ude i de forskellige forretningsfunktioner. Træning og styrkelse af interne sikkerhedskompetencer sker bl.a. via eksterne kurser, som ved nedenstående eksempel.

Introduktion til OT-sikkerhed for teknikere i produktionen
Teknikere i udviklingsteknologi deltog i et to-dags online introduktionskursus til OT-sikkerhed, for at blive klogere på, hvordan de kan beskytte deres udviklings- og driftsmiljø. Selvom det ved første øjekast synes at ligge uden for scope af TV 2's produktionsmiljø, fandt de hurtigt frem til at TV 2 konceptuelt har, hvad der kan betegnes som ICS/OT-systemer, hvor OT-kurset gav en masse brugbar indsigt.

“Det viste sig at være yderst relevant og inspirerende at blive klogere på de problemstillinger og udfordringer, som jo er de samme, som dem vi har med at gøre i vores produktionssystemer. ICS og OT-sikkerhed er utvivlsomt relevant for rigtig mange virksomheder, der har en form for produktionsmiljø som jo også skal beskyttes mod cybertrusler - som kræver en anden tilgang end til gængse IT systemer” - Carsten Bengtsen, IT Security Specialist, TV 2 Danmark

ICS Range har også hjulpet en række virksomheder i industrien med udgangspunkt i specifikke situationer og behov. Gennem en række tilpassede kurser, er virksomheder blevet klædt på til at takle væsentlige udfordringer eller opgaver, der kan løfte deres videre arbejde med OT-sikkerhed. Enkelte cases er beskrevet i følgende.

Case for Transport og logistikvirksomhed

En international virksomhed, der leverer transport og logistik services havde udfordringer med kommunikationen på tværs af fagområder. Der var dermed et behov for at mindske afstanden, når det kom til at adressere vigtige underleverandører, ved at tydeliggøre, hvorfor IT og OT sikkerhed på hvert sit punkt var vigtigt, hvor de kan spille sammen, og hvor de ikke kan.

OT-sikkerhedskursus med fokus på leverandørstyring
ICS Range sammensatte et kursus for IT-sikkerhed, OT-drift, indkøb og compliance medarbejdere. Alle forlod kurset med konkret viden om, hvordan man får rammesat de rigtige krav til leverandører af sikkerhedstests på deres kritiske systemer - set i forhold til compliance og indkøb. Deltagerne var særligt imponerede over ICS Range evne til at spænde bredt over forskellige faggrupper og gøre det relevant for alle.

Case for Produktionsvirksomhed

En international produktionsvirksomhed befandt sig i en proces, hvor de skulle teste drift-sikkerheden af nyt produkt.

Pentesting af produkt - forstå hvordan en hacker tænker
ICS Range sammensatte et to-dags forløb for virksomhedens softwareudviklere, IT-sikkerhed- og automatiseringsmedarbejdere, hvor de med live demonstrationer af pentesting, fik indblik i en hackers måde at finde gemte eller utiltænkte sårbarheder. Deltagerne synes det var rigtig spændende og relevant at få indsigt i en hackers tankemønstre og angrebsvinkler.

Appendix: Yderligere tiltag erhvervsskoler

Ved at implementere yderligere 10 tiltag kan erhvervsskolerne forbedre kvaliteten af OT-sikkerhedsundervisningen og forberede eleverne bedre på at håndtere de udfordringer, de vil stå over for i arbejdsverdenen inden for teknisk produktionsudstyr.

1. Udvikling af Specialiserede Kurser

Skolen kan udvikle specialiserede kurser i OT-sikkerhed, der omfatter både teoretisk viden og praktiske færdigheder. Disse kurser skal være nøje tilpasset behovene i branchen og inkludere emner som risikostyring, trusselsvurdering og sikkerhedsteknikker specifikke for OT-miljøer.

2. Erfarne Instruktører og Eksperter

Skolen bør ansætte erfarne instruktører og eksperter inden for OT-sikkerhed. Disse instruktører kan ikke kun levere teoretisk undervisning, men også dele deres praktiske erfaring og indsigter fra arbejde inden for OT-sikkerhedsområdet.

3. Laboratorie- og Simuleringsfaciliteter

Skolen bør investere i moderne laboratorie- og simuleringsfaciliteter, der giver eleverne mulighed for at arbejde med OT-udstyr og systemer i et kontrolleret og sikkert miljø. Dette giver dem praktisk erfaring med OT-sikkerhedsprocedurer.

4. Praktikmuligheder og Industrielt Samarbejde

Skolen kan etablere partnerskaber med virksomheder inden for industrien for at give eleverne praktikmuligheder. Dette giver dem mulighed for at anvende deres viden i den virkelige verden og opbygge netværk med fagfolk.

5. Opdatering af Læseplaner

Løbende opdatering af læseplaner er afgørende for at sikre, at undervisningen forbliver relevant og aktuel i lyset af hurtige ændringer inden for OT-sikkerhed. Skolen bør have mekanismer på plads for at tilpasse læseplanerne i overensstemmelse med de nyeste trusler og teknologier.

6. Certificeringer og Eksamensforberedelse

Skolen kan tilbyde forberedelse til anerkendte certificeringer inden for OT-sikkerhed, hvilket kan forbedre elevernes beskæftigelsesmuligheder. Dette kan omfatte kurser, der specifikt fokuserer på eksamenstræning.

7. Læringsressourcer og Værktøjer

Skolen kan give eleverne adgang til online ressourcer, værktøjer og software, der er relevante for OT-sikkerhedsundervisningen. Dette kan hjælpe eleverne med at fortsætte deres læring og forskning uden for klasseværelset.

8. Overvågning og Evaluering

Skolen bør etablere en proces for at overvåge og evaluere elevernes præstation og forståelse af OT-sikkerhed. Dette kan omfatte tests, projekter og praktiske øvelser.

9. Bevidsthedsprogrammer

Skolen kan også udføre bevidsthedsprogrammer, der informerer eleverne om vigtigheden af OT-sikkerhed og opfordrer dem til at være ansvarlige og etiske i deres arbejde.

10. Samarbejde med Industrielle Organisationer

Skolen bør samarbejde med industrielle organisationer, der er dedikeret til cybersikkerhed og OT-sikkerhed. Dette samarbejde kan føre til ressourcer og information om de seneste tendenser og bedste praksis.

Arbejdsgruppens parter 2023