Også for ledige (6 ugers)

Cybersikkerhed videregående

Kort fortalt

På de nyeste og fremtidens tekniske installationer har en lang række af de digitale løsninger, der arbejdes med, en forbindelse til den fysiske verden. Et brud på sikkerheden kan potentielt have omfattende konsekvenser og forårsage uheld og skader i den fysiske verden i form af tab af både virksomhedsmæssige og personfølsomme data, voldsomme materielle skader, personskade eller i yderste konsekvens dødsfald. Mange intelligente og digitale løsninger er baseret på sensorer, der løbende foretager dataopsamling fra omgivelserne bl.a. om folks handlinger og dermed potentielt opsamler data om personlig adfærd og rutiner. Dermed vokser behovet for sikre digitale løsninger.På kurset får du viden om cybersikkerhed ved tilslutning af komponenter til industrielle netværk og større netværk i bygninger. Søgeord: cybersikkerhed, industrielle netværk, grøn omstilling, dataopsamling

Hold

Der er pt. ingen hold udbudt til dette kursus. Brug evt. kursusagenten for at blive adviseret om nye hold.;

Kontakt

Roskilde Tekniske Skole,
kursusafdelingen
46 300 400

Kursuspris

AMU-målgruppe:
DKK 416,00

Uden for AMU-målgruppe:
DKK 1.813,80

Tilmelding

Fag: Cybersikkerhed videregående

Fagnummer: 49718	**Varighed:** 2 dage
Pris, AMU-målgruppe: DKK 416,00	**Pris, uden for AMU-målgruppe:** DKK 1.813,80

Målgruppe: Uddannelsen er udviklet til faglærte elektrikere og tilsvarende målgrupper, der i deres job har brug for videregående kompetencer om cybersikkerhed.

Beskrivelse: Efter kurset kan deltageren anvende viden om cybersikkerhed ved tilslutning af komponenter til industrielle netværk og større netværk i bygninger. Det betyder:
Deltageren har viden om betydningen af cybersikkerhed på netværk, såsom risikoanalyse, password, firewall, vpn, kryptering og risikoen ved at anvende offentlige netværk.
Deltageren anvender viden om øget sikkerhed ved brug af separate netværk uden direkte adgang til øvrige netværk samt på maskin- og procesanlæg (kundens netværk).
Deltageren kan anvende viden om begrænsning af operativsystemer til de absolut nødvendige funktioner, med så lille angrebsoverflade som muligt.
Deltageren har viden om ¿¿software, hardware og proceduremetoder og kan anvende denne til at beskytte applikationer mod eksterne angreb.
Deltageren kan udvælge komponenter for passende sikkerhedsforanstaltninger til fysisk at minimere risikoen for hackerangreb i indgående opkald via trådløse og kablede netværk til fx SCADA- eller Building Management Systemer (BMS)-netværk, og kan foretage opkobling af netværkene til internettet med stærk godkendelseskontrol, så der opnås sikker kommunikation.
Deltageren anvender producentens vejledning om korrekt konfiguration samt identificerer om et produkt er certificeret efter en standard og om regelmæssige softwareopdateringer understøttes. Deltageren afklarer, hvilke data produktet opsamler og hvordan disse data bliver krypteret ved opbevaring og/eller når de sendes over netværk.
Deltageren overdrager installerede produkter til kunden, så det fremstår tydeligt hvilken løsning kunden har overtaget og deres ansvar i den forbindelse.