Cybersikkerhed grundlæggende + videregående

Fag: Cybersikkerhed grundlæggende

Fagnummer: 49717	**Varighed:** 1 dag
Pris, AMU-målgruppe: DKK 218,00	**Pris, uden for AMU-målgruppe:** DKK 1.073,00

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

Beskrivelse: Efter kurset kan deltageren anvende viden om cybersikkerhed ved tilslutning af enkle komponenter til netværk i bygninger. Det betyder:
Deltageren har viden om betydningen af cybersikkerhed på netværk, såsom password, firewall, vpn, kryptering og risikoen ved at anvende offentlige netværk.
Deltageren har kendskab til brug af software, hardware som f.eks. USB og IoT samt proceduremetoder for risikobaseret tilgang for at beskytte applikationer mod eksterne angreb.
Deltageren kan installere en aktiv komponent opkoblet på internettet og etablere en sikker portåbning i firewall til komponenten.
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.
Deltageren overdrager installerede produkter til kunden, så det fremstår tydeligt hvilken løsning kunden har overtaget og deres ansvar i den forbindelse.

Kontakt

Kursusadministrationen
46300400
rts@rts.dk

Kursuspris

AMU-målgruppe:
DKK 654,00

Uden for AMU-målgruppe:
DKK 2.959,00

Tilmelding

Fag: Cybersikkerhed videregående

Fagnummer: 49718	**Varighed:** 2 dage
Pris, AMU-målgruppe: DKK 436,00	**Pris, uden for AMU-målgruppe:** DKK 1.886,00

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.