Utbildningsbeskrivning - lärarledd

Utbildningens namn:
IT- och cybersäkerhet för svenska elsektorn

Ämnesområde:
IT-säkerhet med fokus på processnära miljöer

Målgrupp:
Kursen vänder sig framförallt till säkerhetsansvariga när det gäller IT och/eller industriella informations- och styrsystem eller motsvarande verksamma vid elbolag. Kursen är också mycket användbar för personer som arbetar som kravställare och projektledare av stora IT/SCADA/ICS-system, systemägare och leveransansvariga inom elföretag som arbetar med IT och/eller automationssystem.

Syfte och mål:
Kursen är utformad för att ge deltagarna tillämpad kunskap om skyddsmekanismer och tekniska säkerhetslösningar. Den ger dessutom tips på hur man i det löpande säkerhetsarbetet bättre upptäcker och hanterar säkerhetsproblem mot IT- och SCADA/ICS-system.

Målet med kursen är att deltagarna ska få:
- ökad förståelse för hur attacker mot industriella kontrollsystem kan gå till
- ökad förståelse för de komplexa beroendeförhållanden som finns mellan automationslösningar och IT-stöd och verksamhet i elbolag.
- god förståelse för tillämpning och fördelarna med olika tekniska säkerhetslösningar i IT- och SCADA/ICS-miljöer.
- prova att använda enkla verktyg och lösningar för att skapa ett IT-mässigt grundskydd.
- en ökad förståelse för vikten av ett löpande IT- och cybersäkerhetsarbete.
- kunskap om hur man använder verktyg för att löpande följa upp och upptäcka avvikelser eller säkerhetspåverkande händelser i IT- och SCADA/ICS-miljöer.

Kursinnehåll:
Inledning
Kursen inleds med presentation av föreläsare samt en kort redovisning av Svenska kraftnäts motiv bakom denna kurs. Syfte och mål med kursen introduceras samt en kort genomgång av praktiska detaljer. En kort genomgång av tillämpliga grundläggande terminologi, koncept och modeller för IT- och cybersäkerhet och hur cyberfysiska system påverkas i det moderna företaget.

Förevisning och genomgång av hot med hjälp av demonstrator
Inledande demonstration där olika exempel på angrepp mot SCADA/ICS-miljö förevisas. Med hjälp av en demonstrator visas på ett verklighetstroget sätt exempel på hur angrepp idag sker mot företag och organisationer. Exemplen omfattar även delar där angreppen går hela vägen in mot SCADA/ICS-miljön för att påvisa vilka konsekvenser detta kan medföra.

IT- och SCADA/ICS-säkerhet och kopplingar mot säkerhetsskydd, säkerhetsanalys, hot- risk- och sårbarhetsanalyser
En kort genomgång av rättsliga krav och de arbetsmetoder som ingår i säkerhetsarbetet för att skapa säkrare infrastrukturlösningar i svenska elbolag. Exempel på rättsliga krav är Svenska kraftnäts föreskrifter för elberedskap och säkerhetsskydd. Exempel på hot baseras på urval av Svenska kraftnäts hotkatalog.

Genomgång av IT-säkerhetsarkitektur och dess olika komponenter
En närmare genomgång av de tekniska komponenter, principer, de modeller och koncept som bör ingå i en IT-säkerhetsarkitektur. Exempel på säkerhetskoncept som gås igenom är zon-modeller, separation och säker fjärråtkomst. Exempel på säkerhetsprinciper är skydd i djupled. Exempel på säkerhetskomponenter är brandväggar, intrångsdetekteringssystem, logginsamlingssystem, behörighetshanteringssystem, fjärråtkomstlösningar.

Orientering om olika tekniska lösningar för skydd, övervakning av nätverk/system/applikationer
Principgenomgångar av olika tekniska skydd inom IT- och cybersäkerhet. Exempel på hur tekniska skydd såsom brandväggar, nätkryptering och logganalys kommer att användas. Exempel och tips på hur säkerhetsförbättringar av existerande IT- och automationskomponenter, såsom PLC:er eller industriella nätverksswitchar, kommer att gås igenom.

Stegvis uppbyggnad av en säker IT/SCADA/ICS-miljö med hjälp av demonstratormiljön
Med hjälp av demonstrationer och beskrivning av typfall kommer vi under kursen stegvis bygga upp en säkrare IT/SCADA/ICS-miljö som stoppar och upptäcker de angrepp som utfördes i början av kursen. Vid slutet av kursen kommer en komplett och uppsäkrad miljö redovisas, vilket avser att fungera som exempel och referens för ett svenskt elbolag.

Gruppövningar och diskussionsstund
Särskilda diskussioner om moderna hot, såsom APT-angrepp eller avancerade angrepp mot elbolag i deras verksamhet för elproduktion och eldistribution. Deltagarna ges möjlighet att ta upp specifika ämnen och problemområden till diskussion med föreläsaren och övriga deltagare.

Summering och avslutning
Kursen avslutas med reflektioner, kursutvärdering samt kursintyg utdelas.

Förkunskaper:
Det krävs grundläggande IT-kunskap (typ konceptuell förståelse av datorer, nätverk mm), vidare är kännedom om IT- och informationssäkerhetsarbete och kontrollsystem en fördel.

Min antal: 10

Max antal: 24

Lokal: Skepparholmen konferens, Nacka

Datum: 11-13 mars 2019

Tid: start kl 1200 den 11 mars, slut kl 1300 den 13 mars

Föreläsare: Robert Malmgren, Erik Johansson

Kunskapstest? Nej

Certifiering? Kursintyg

Kursansvarig (Svk): Svante Nygren

Verktyg: Inga egna verktyg krävs