Grundläggande kurs: Säkerhet i industriella informations- och styrsystem

NCS3 – Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet

Säkerhet i industriella informations- och styrsystem *(tidigare kallad Säkerhet i Industriella Kontrollsystem, SIK) är en praktiskt inriktad kurs som ger en introduktion till informationssäkerhet inom industriella informations- och styrsystem för samhällsviktig verksamhet. Kursen riktar sig till dig som arbetar praktiskt med informations- och styrsystem, till exempel som drifts- och utvecklingsingenjör.*

Introduktion

Datoriseringen av de system som förser samhället med bränsle, el, värme, vatten och transporter går fort. IT-system integreras i befintliga processer för att effektivisera verksamheten då digitaliseringen underlättar informationsflödet mellan system och användare.

Industriella informations- och styrsystem har traditionellt sett varit isolerade från omvärlden och byggt på robust industriell teknik. Idag bygger de i huvudsak på samma teknik som administrativa IT-system, teknik som ofta är mindre robust och som introducerar nya sårbarheter. Samtidigt ansluts styrsystem i allt högre grad till både interna nätverk och till Internet. Detta resulterar i en radikalt förändrad hotbild, vilket är något som du får lära dig att hantera på kursen.

Kursupplägg

Kursen genomförs under två dagar på FOI i Linköping och förutsätter att deltagarna har grundläggande kunskap om datornätverk och industriella informations- och styrsystem, samt ett allmänt intresse för IT- och informationssäkerhet.

Deltagarna kommer att få en praktisk förståelse för IT-säkerhet då kursen ger en god överblick samt tydliggör de villkor som är specifika för industriella informations- och styrsystem.

Efter genomgången kurs är målet att deltagarna ska:

- Ha förståelse för betydelsen av och möjligheterna med att aktivt arbeta med säkerhetshöjande insatser i industriella informations- och styrsystem.
- Känna till lämpliga verktyg och metoder för att identifiera sårbarheter i industriella informations- och styrsystem.
- Kunna delta i arbetet med att förbättra och utveckla säkerheten i en organisations industriella informations- och styrsystem.

FOI

MSB Myndigheten för samhällsskydd och beredskap

Ur kursinnehållet

IT-säkerhet – en översikt. Inledningsvis presenteras grundläggande begrepp och metoder för att skydda informationstillgångar. Här får du exempelvis lära dig hur åtkomst till IT-system kan kontrolleras, vilka autentiseringsmetoder som kan användas samt vilket skydd en brandvägg kan ge. Du får även kunskap om vem en angripare kan tänkas vara och vilka drivkrafter som påverka angriparen.

Hot och risker mot styrsystem. Dagens styrsystem använder sig alltmer av IT-komponenter och blir följaktligen mer sårbara för skadlig kod. För att ge en ökad förståelse för vad detta innebär beskrivs hur olika typer av skadlig kod fungerar. Bland annat beskrivs virus, rootkits och trojaner samt hur dessa kan inverka på funktionen hos industriella informations- och styrsystem.

Laborationer och demonstrationer. För att visa hur viktigt det är att skydda känslig information genomförs laborationer och demonstrationer. Dessa ger insikt i hur lätt det kan vara för en obehörig att ta sig in i till synes isolerade datornätverk. Med hjälp av fritt tillgänglig programvara får deltagarna själva prova på att preparera hårdvara, kartlägga datornätverk och system, identifiera sårbarheter samt utföra ett IT-angrepp mot ett styrsystem.

Behovet av IT-säkerhet för styrsystem. Budskapet från laborationsmomenten förstärks med exempel på incidenter som inträffat och kompletteras med diskussioner kring deltagarnas egna erfarenheter. Utöver tekniska säkerhetsåtgärder är det även viktigt att förstå människans roll i det säkerhetshöjande arbetet. Kompetensutveckling och administrativa säkerhetsprocesser såsom incidet hantering, teknisk revision och kontinuitetshantering är viktiga instrument för att komplettera tekniken.

Praktik. Under kursens andra dag genomförs en övning som syftar till att utvärdera säkerheten i ett uppsatt styrsystemsnätverk. Moment som ingår är systemkartläggning, sårbarhetsanalys samt att ta fram förslag på säkerhetshöjande åtgärder.

Erfarenhetsutbyte

I många driftorganisationer är det endast en person som ansvarar för IT-relaterade säkerhetsfrågor i styrsystemsmiljön. Detta arbete sker dessutom ofta i mån av tid och utöver ordinarie arbetsuppgifter vilket gör det svårt att följa med i det snabbt föränderliga område som IT-säkerhet utgör. Därför är en viktig del av kursen det erfarenhetsutbyte som sker samt de kontakter som skapas mellan deltagarna. För att stödja dessa mål försöker FOI och MSB att fylla kurserna med deltagare från samma eller likartade branscher.

Om NCS3

Sedan 2008 driver Totalförsvarets forskningsinstitut (FOI) tillsammans med Myndigheten för samhällsskydd och beredskap (MSB) NCS3, ett nationellt kompetenscentrum med fokus på säkerheten i industriella informations- och styrsystem. Inom NCS3 bedrivs studier, utbildning och övningar för myndigheter och företag som arbetar med samhällsviktig verksamhet. Denna verksamhet har gett FOI en unik kompetens inom området, en kompetens som också används vid risk- och sårbarhetsanalyser på samhällsviktiga infrastrukturer.

För mer information

www.foi.se/si3s ncs3@foi.se