Övning i IT-incidenthantering

Arbetar du som systemadministratör och känner att dina kunskaper om IT-säkerhet och incidenthantering behöver förbättras? Då har du nu chansen! Vår kurs ger en möjlighet att på ett realistiskt sätt få öka kunskapen och öva förmågan att hantera IT-incidenter. Kursen sträcker sig över fyra dagar och består av tre delar: teori, praktik och uppföljning.

Kursupplägg

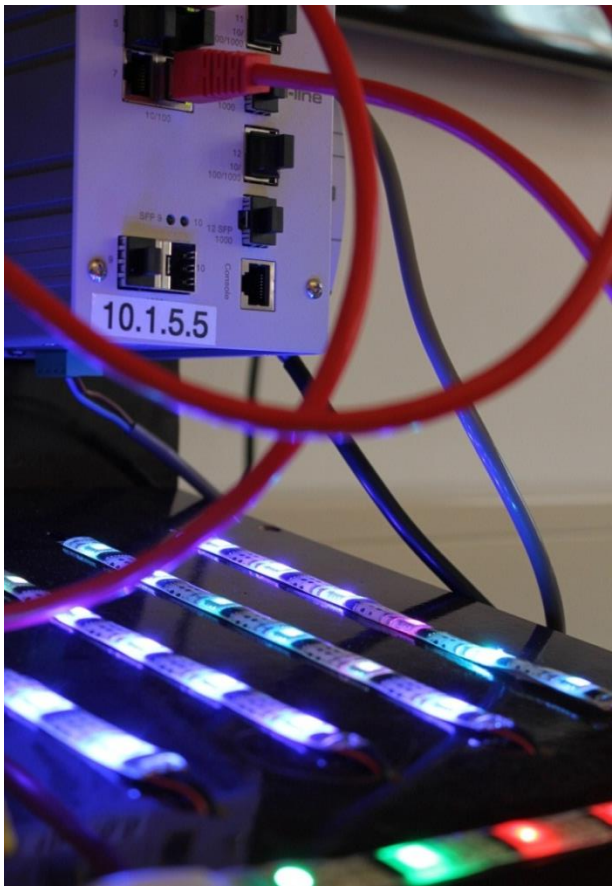
Kursens tre delar: teori, praktik och uppföljning, är till för att ge en fördjupad förståelse och praktisk övning i hur IT-incidenter kan hanteras.

Den genomförs under 3,5 dagar vid FOI i Linköping. Den första två dagarna ägnas åt teori och förberedelser inför en praktisk övning.

Den tredje dagen är en ren övningsdag där ni praktiskt kommer att få ta er an ett antal incidenter i en IT och styrsystems-miljö.

Sista dagen består av genomgång, uppföljning och diskussion av övningen.

Målgruppen för denna övning är främst erfarna systemadministratörer eller motsvarande.



Teori och förberedelser

Teorin syftar dels till ge grundläggande kunskaper om IT-incidenthantering samt till att ge en inblick i hur de verksamhetskritiska system vi använder som exempel fungerar. Bakgrunden ges för att skapa en förståelse för hur systemen är uppbyggda och bör hanteras för att skyddas mot angrepp. Teorin avslutas med en genomgång av hantering av IT-säkerhetsincidenter, som bland annat baseras på incidenthanteringsmetoden från NIST, SP800-61rev2.

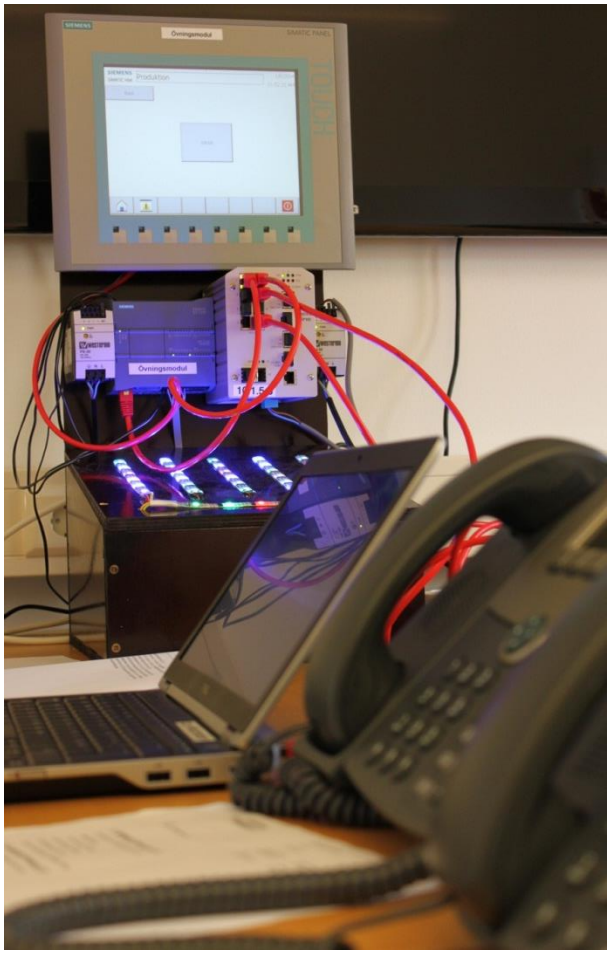
Efter teorigenomgångarna kommer ni att praktiskt få bekanta er med övningsmiljön CRATE (Cyber Range And Training Environment, som är en av Europas största cyberövnings-anläggningar) samt de verktyg som finns att tillgå under övningen. Exempel på verktyg kan vara: Zenmap, NexPose och Wireshark. Ni som deltagare kommer sedan att arbeta i grupp och lösa uppgifterna tillsammans.

Scenario

Två konkurrerande företag. Ni i den deltagande gruppen har alla blivit nyanställda på IT-avdelningen på ett av företagen. Den gamla IT-avdelningen har lämnat företaget och ni ska nu ta över driften av IT-systemen och produktionen. Målet är att säkerställa att angreppen på IT-systemen inte påverkar de verksamhetskritiska systemen.

Öva förmåga

Övningen genomförs under dag tre, och ni ska tillsammans som en grupp lösa ett antal IT-relaterade incidenter. Huvuduppgiften är att se till att produktionsprocessen fortgår oavsett vad, gruppen måste samtidigt förhindra och motverka IT-angrepp.



Uppföljning

Den sista dagen består av en genomgång av övningen, uppföljning samt diskussioner. Ni får se när och hur angreppen skedde och hur ni som grupp hanterade incidenten. Därefter tar diskussionen vid: vad sköttes bra, vad kunde ha skötts bättre och andra tankar om spelet. Vikt läggs på att diskutera hur de nya kunskaperna kan anpassas och appliceras på den egna dagliga verksamheten.

Mål

Efter kursen är målet att ni ska ha fått:

- mer kunskap om olika verktyg som finns tillhands för incidenthantering samt ha praktiska erfarenheter av att använda verktygen.
- praktiska kunskaper om hur IT-incidenter kan förebyggas och hanteras.
- nya kunskaper att använda i den dagliga verksamheten.

För mer information

Mikael Wedlin

Telefon: 013- 37 80 96
Mail: mwe@foi.se