KURSPLAN

Säkerhet för kritisk infrastruktur (operativ teknologi)

Security for Critical Infrastructure (Operational Technology)

7,5 högskolepoäng (7.5 credits)

Kurskod: DV2617
Huvudområde: Datavetenskap, Programvaruteknik
Utbildningsområde: Teknik
Utbildningsnivå: Avancerad nivå
Fördjupning: A1N - Avancerad nivå, har endast kurs/er på grundnivå som förkunskapskrav

Undervisningsspråk: Engelska
Gäller från: 2022-08-29
Fastställd: 2022-03-01

1. Beslut

Denna kurs är inrättad av dekan 2021-11-10. Kursplanen är fastställd av prefekten vid institutionen för datavetenskap 2022-03-01 och gäller från 2022-08-29.

2. Förkunskapskrav

För tillträde till kursen krävs minst 120 hp varav minst 90 hp inom det tekniska området och minst 2 års yrkeserfarenhet inom område som är relaterat till mjukvaruintensiv produkt och/eller tjänsteutveckling (visas exempelvis genom intyg från arbetsgivare.)

3. Syfte och innehåll

3.1 Syfte

Denna kurs syftar till att ge studenterna färdigheter för att analysera hot mot ICS (Industrial Control Systems) som används vid cyberattacker mot kritisk infrastruktur, såsom avancerade långvariga hot (APTs), attacker mot sårbarheter (exploits), attacker mot leverantörskedjor, förstörare (wipers) samt utpressningsprogram (ransomware).

3.2 Innehåll

Kursen ger studenterna färdigheter i att analysera hot mot ICS samt kunskaper i att försvara kritisk infrastruktur mot cyberattacker. Detta görs genom att analysera de mest destruktiva cyberattackerna mot ICS som har skett under det senaste decenniet, exempelvis men inte enbart Stuxnet, BlackEnergy, Industroyer, Solorigate och WhisperGate. Kursen täcker också säker konfiguration och försvarstillvägagångsätt av SCADA (Supervisory Control And Data Acquisition) och cyberfysiska system (CPS) samt aktuella cybersäkerhetsbestämmelser och -standarder.

4. Lärandemål

Följande lärandemål examineras i kursen:

4.1 Kunskap och förståelse

Efter genomförd kurs ska studenten kunna:
• redogöra för de mest förekommande säkerhetshoten mot ICS
• förstå de tillvägagångssätt som används vid cyberattacker mot kritisk infrastruktur
• Redogöra för olika försvarstekniker för ICS

4.2 Färdighet och förmåga

Efter genomförd kurs ska studenten kunna:
• Identifiera, analysera, klassificera och blockera cyberattacker mot ICS
• Välja och tillämpa lämpliga försvarslösningar för ICS

4.3 Värderingsförmåga och förhållningssätt

Efter genomförd kurs ska studenten kunna:
• Utvärdera och bedöma hur effektiv cyberförsvaret är inom specifika ICS miljöer.

5. Läraktiviteter

Undervisningen sker i form av online föreläsningar, inspelat videomaterial, tillsammans med skrivet material, litteratur och forskningslitteratur. Under kursens gång kommer kommunikation, feedback och diskussioner med lärare och andra deltagare att ske via e-post och kursens lärplattform.

6. Bedömning och examination

Examinationsmoment för kursen

Kod	Benämning	Omfattning	Betyg
2210	Inlämningsuppgift 1	2,5 hp	GU
2220	Inlämningsuppgift 2	2,5 hp	GU
2230	Inlämningsuppgift 3	2,5 hp	GU

Kursen bedöms med betygen G Godkänd, UX Underkänd, något mer arbete krävs, U Underkänd.

I kurstillfällets information inför kursstart framgår i vilka examinationsmoment som kursens lärandemål examineras samt gällande bedömningsgrunder.

Examinator kan, efter samråd med högskolans FUNKA-samordnare, fatta beslut om anpassad examinationsform för att en student med varaktig funktionsvariation ska ges en likvärdig examination jämfört med en student utan funktionsvariation.

7. Kursvärdering

Kursvärdering ska göras i enlighet med BTH:s beslut om frågeställning i kursvärderingar och beslut om process för hantering och uppföljning av kursvärderingar.

8. Begränsningar i examen

Kursen kan ingå i examen men inte tillsammans med annan kurs vars innehåll, helt eller delvis, överensstämmer med innehållet i denna kurs.

9. Kurslitteratur och övriga lärresurser

Material såsom forskningsartiklar och annat kursmaterial tillhandahålls på kursens lärplattform och via BTHs biblioteksresurser, samt rekommendationer för vidare läsning.