HÖGSKOLAN DALARNA

Kursplan

Datasäkerhet och integritet 7,5 högskolepoäng, Grundnivå 1

Data Security and Integrity - Undergraduate Level 7.5 Credits*, First Cycle Level 1

Lärandemål

Efter avslutad kurs ska den studerande kunna

- redogöra för de hotbilder som finns vid it-användning.
- använda olika slags it-säkerhetsverktyg för egna säkerhetstester, skydd av information och utrustning.
- bedöma olika informationstekniska lösningars styrkor och svagheter vad gäller datasäkerhet
- översiktligt känna till den lagstiftning som gäller inom områdena it-säkerhet och personlig integritet.
- analysera och föreslå lämpliga åtgärder för att förbättra it-säkerheten i en verksamhet.

Innehåll

Kursen behandlar förvaltningsfrågor och praktiska konsekvenser i samband med att säkra it-system. Kursen fokuserar på hotbilder, kryptografi, en översyn av TCP/IP och säkra nätverk, åtkomstkontroll, brandväggar, värdars härdning, applikationssäkerhet, dataskydd, incidentrespons, säkerhetspolicy och planering. En teoretisk förståelse stöder en stor praktisk del där de studerande lär sig att både granska it-system och att använda olika slags mjukvaror för it-säkerhet.

Kursen är uppdelad i fem delmoment om vardera 1,5 högskolepoäng.

Delmoment 1 (1,5 hp).
Denna del beskriver översiktligt hotbilder och it-säkerhetsproblem. Grunder och praktiska färdigheter inom kryptering, hashar, digitala signaturer, och nyckelhantering tas upp, vilket är centrala begrepp inom it-säkerhet:

- Introduktion och terminologi
- Vanliga hackertekniker och it-hot
- IT och samhällets sårbarhet
- Kryptering, hashar, digitala signaturer och nyckelhantering
- Säker kommunikation

* 1 Credit = 1 ECTS

- Säker E-post

Delmoment 2 (1,5 hp)
Del 2 fördjupar sig i områden introducerade i delmoment 1, bl.a. hur vanliga nätverksattacker utförs och hur man skyddar sig mot dem. Vidare att kunna använda olika slags mjukvaror för it-säkerhet:

- Hur attackerare kan få obehörig åtkomst till eller störa normala driften av ett nätverk
- Nätverkssäkerhet för trådbundna (LAN) och trådlösa (WLAN) nätverk
- Fysiska åtkomstverktyg som lösenord och biometri
- Autentisering och nätverksäkerhet
- Katalogtjänster, PKI och certifikat
- Åtkomstkontroll och loggar
- Kryptering av filer och volymer

Delmoment 3 (1,5 hp)
I delmoment 3 behandlas TCP/IP och säkra nätverksprotokoll och att praktiskt installera, konfigurera och utvärdera brandväggar. Samt incident respons och utföra en enklare forensisk analys:

- Brandväggar (firewalls) och arkitektur
- Proxies och intrångsdetektion
- Incident respons och forensisk analys

Delmoment 4 (1,5 hp)
Detta delmoment ger en introduktion och djupare bearbetning av administrationssäkerhet, bl.a. att praktiskt kunna utföra säkerhetstest, samt skydda enskilda värdar och dess data:

- Operativsystemsäkerhet och värdars härdning
- Virusskydd
- Applikationssäkerhet och värdars härdning
- WWW-tjänster och internetsäkerhet
- Skydda lagrad data genom fysisk säkerhet och backup

Delmoment 5 (1,5 hp)
I det avslutande delmomentet, som kan genomföras på ett företag/organisation, ska de tidigare förvärvade kunskaper och färdigheter, användas i ett mindre it-säkerhetsprojekt. De studerande behöver i uppgiften skaffa sig nödvändig information, analysera problemställningar och använda olika byggstenar inom it-säkerhet. Momentet avslutas med ett lösningsförslag där träning i muntlig och skriftlig presentation ges.

- Risk- och sårbarhetsanalys
- IT-säkerhetspolicy, säkerhetsmodeller och strategier
- Legala och etiska aspekter, informationshantering och informationsklassificering

Examinationsformer
De 4 första delmomenten examineras genom skriftliga och praktiska inlämningsuppgifter utifrån delmomentens mål. Det sista delmomentet examineras skriftligt och muntligt.

Arbetsformer
Kursen ges på ett distansöverbryggande och interaktivt sätt och kräver tillgång till en dator med internetanslutning. Studiehandledning, föreläsningar, inlämningsuppgifter, laborationer m.m. återfinns i ett webbaserat kursrum och kan tillgodogöras oberoende av tid och rum. I kursrummet finns för varje delkurs en studiehandledning som innehåller läsanvisningar, beskrivning av examinationsuppgifter och kriterier för betygsättning för kursen.
De studerande ska delta i olika diskussionsforum i kursens webbaserade kursrum.

Betyg
Som betygsskala används U–VG.

För VG på kursen krävs betyget VG på minst tre av delkurserna.

Förkunskapskrav
Hård Infrastruktur 7,5 hp

Övrigt
En dator som kan köra motsvarande Windows 7 64 bit eller högre och bredbandsuppkoppling med minst 2 Mbit krävs för studierna. En virtuell miljö (maskin) kan behövas i vissa delmoment. Ett headset och s k webbkamera är också ett krav då delar av examinationen kan ske över Internet.

Ersätter IK1020.

Summary in English
This course looks at management issues and practical implications related to securing information systems. It focuses on Cryptography, a review of TCP/IP and Secure Networks, Access Control, Firewalls, Host Hardening, Application Security, Data Protection, Incident Response, and Security Policy and Planning. A clear theoretical understanding supports a large practical component where students learn to audit information systems and use contemporary security software.
The course is divided into five parts, each one worth 1.5 credits.

Ämnestillhörighet:
Informatik

Ämnesgrupp:
Informatik/Data- och systemvetenskap

Utbildningsområde:
Tekniska området, 100%

Kursen kan ingå i följande huvudområde(n):
1. Informatik

Fördjupningsbeteckning för respektive huvudområde:
1. G1F

Fastställd:
Fastställd 2015-06-11
Kursplanen gäller fr.o.m. 2015-09-04