HÖGSKOLAN I BORÅS

Grundläggande informationssäkerhet
Basic Information Security
7,5 högskolepoäng
7,5 credits

Ladokkod: 41F09A
Version: 1.0
Fastställd av: Utbildningsutskottet 2014-08-22
Gäller från: HT 2014

Nivå: Grundnivå
Huvudområde (successiv fördjupning): Data och systemvetenskap (G1F)
Utbildningsområde: Teknik
Ämnesgrupp: Datateknik
Förkunskapskrav: Uppfyller kraven till IT-tekniker eller innehar motsvarande kunskaper
Rekommenderade förkunskaper
Kursen bygger på och utvecklar kunskaperna Nätverk III/LAN-säkerhet och WAN-access,7,5 hp och Supportkunskap 7,5 hp
Betygsskala: U, 3, 4 eller 5

Innehåll
Kursen innehåller följande huvudsakliga områden:
- teknisk informationssäkerhet (som t.ex. nätverkssäkerhet, systemsäkerhet och internetsäkerhet)
- strategisk informationssäkerhet (säkerhetspolicyarbete, säkerhetsstandards och säkerhetsorganisation samt klassning av informationstillgångar)
- operativ informationssäkerhet (incidenthantering och krishantering samt revision)

Mål
Det övergripande målet är att studenten efter kursen ska ha en grundläggande förståelse för hur datanätverk kan säkras samt ha en grundläggande färdighet och förmåga att hantera säkerhetsfrågor ur såväl ett verksamhets- som ett tekniskt perspektiv.

Studenten ska efter genomgången kurs kunna:

1 Kunskap och förståelse
1.1 använda den etablerade terminologin och redogöra för tekniska och praktiska problem inom området,
1.2 känna till de vanligaste typerna av attacker mot IT-system och kunna vidta lämpliga åtgärder för att skydda dessa,
1.3 förstå grundstrukturen i säkerhetsprotokoll och kunna arbeta med olika modifikationer av dem,
1.4 vara redo att delta i utvecklings- och utredningsarbete med säkerhetsproblematik,
1.5 redogöra för grundläggande metoder och tekniker för att möjliggöra olika verksamheters behov av IT och samtidigt undvika de säkerhetsproblem som kan uppstå då dessa verksamheter ingår i en större organisation,
1.6 redogöra för de grundläggande riktlinjerna enligt etablerade metoder i professionen (ITIL) angående användning av informationsteknologi för hantering av säkerhetsrelaterade frågor,
1.7 beskriva hot och säkerhetsproblem som finns i nätverk och implementera en lämplig säkerhetspolicy för att motverka dessa,
1.8 beskriva hur tunnelprotokoll används för att koppla samman LAN över publika och privata WAN-infrastrukturer,
1.9 beskriva hur kryptering och VPN-tjänster fungerar och används för att skydda trafik som skickas över publika WAN-infrastrukturer.

2 Färdighet och förmåga
2.1 visa förmåga att med helhetssyn självständigt identifiera, formulera och hantera tekniska lösningar ur ett säkerhetsperspektiv,
2.2 analysera och utvärdera IT-system med avseende på säkerhet,
2.3 analysera relevanta hot,

2.4 utforma en översiktlig plan för åtgärder och uppföljning utifrån analysen samt dokumentera motiven för valda åtgärder,
2.5 praktiskt applicera grundläggande metoder och tekniker för att tillgodose olika verksamheters behov av IT och samtidigt uppnå en tillfredställande IT-säkerhet inom organisationen,
2.6 konfigurera grundläggande säkerhetsfunktioner i routrar, switchar och brandväggar,
2.7 filtrera trafik i routrar och brandväggar,
2.8 konfigurera, verifiera och felsöka tunnelprotokoll för att koppla samman LAN över publika och privata WAN-strukturer,
2.9 konfigurera, verifiera och felsöka tjänster för monitorering av nätverkskomponenter,
2.10 felsöka och åtgärda vanligt förekommande fel i nätverk, brandväggs-, och routerkonfigurationer,

3 Värderingsförmåga och förhållningssätt
3.1 utvecklat ett medvetet och personligt förhållningssätt avseende olika aspekter kring säkerhetsrelaterade frågor,
3.2 utvecklat ett förhållningsätt till användning av informationsteknologi för hantering av säkerhetsrelaterade frågor i en förankring till etablerade metoder i professionen (ITIL).

Undervisningsformer

Undervisningen utgörs av en kombination av föreläsningar, seminarier och laborationer i olika system under handledning. Utanför den normala undervisningen tillkommer grupparbeten och enskilt arbete. Undervisningen bedrivs normalt på svenska, men undervisning på engelska kan förekomma. Litteraturen är på engelska och svenska.

Examinationsformer

Kursen examineras genom följande examinationsmoment:

Laboration Nätverk - (Mål 2.6 - 2.10)
Lärandemål:
Högskolepoäng: 1
Betygsskala: Underkänd eller Godkänd

Laboration 1 UTM - (Mål 2.5 - 2.7)
Lärandemål:
Högskolepoäng: 1,5
Betygsskala: Underkänd eller Godkänd

Skriftlig tentamen - (Mål 1.1-1.9 och 2.1-2.4)
Lärandemål:
Högskolepoäng: 4
Betygsskala: U, 3, 4 eller 5

Seminarium - (Mål 2.2, 3.1 och 3.2)
Lärandemål:
Högskolepoäng: 1
Betygsskala: Underkänd eller Godkänd

Den skriftliga tentamen bestämmer kursens slutbetyg vilket utfärdas först när samtliga moment godkänts.

Studentens rättigheter och skyldigheter vid examination är enligt riktlinjer och regelverk vid Högskolan i Borås.

Kurslitteratur och övriga läromedel

CCNA Security (online-material)

Elektroniskt kompendium.
Online-manualer i de i kursen använda system.
OGC, ITIL V# and Information Security, Jim Clinch, White Paper May 2009

Studentinflytande och utvärdering

Akademichefen och kursansvarig lärare ansvarar gemensamt för att studenternas synpunkter på kursen systematiskt och regelbundet inhämtas. Resultaten av utvärderingarna bör återföras till studenterna och ska vara rådgivande inför kursens framtida utformning.

Övrigt

Övergångsregler:
Studenter som läst enligt tidigare kursplaner examineras på momenten: Skriftlig Tentamen, Laboration 1 och Seminarium