

## System- och nätverkssäkerhet: omfattande introduktion - 4 dagar

*kurser 468*

- Du får lära dig att**
- Analysera risken för säkerhetshot och skydda din organisations system och data
  - Minska känsligheten för angrepp med hjälp av brandväggar och kryptering
  - Bedöma alternativa mekanismer för autentisering av användare och värd
  - Hantera den ökade säkerhetsrisk som Internet och intranät innebär
  - Skydda nätverksanvändare från fientliga program och virus
  - Fastställa vilka säkerhetshot som måste beaktas i din organisation
- Sammanfattning** I dagens Internetberoende arbetsmiljö måste organisationer binda samman sina system över företagsomspännande och virtuella privata nätverk och nå även de användare som rör på sig. Varje anslutning ökar sårbarheten för angrepp från konkurrenter och hackare. På den här kursen får du lära dig att analysera riskerna i dina nätverk och vad som behövs för att välja lämpliga motåtgärder som utsattheten.
- Vem bör delta** Kursen är värdefull för den som behöver grundläggande kunskaper för att utveckla och implementera ett säkerhetsupplägg som skyddar företagets information mot säkerhetshot.
- Workshops** Workshops som ger dig erfarenhet av att analysera system- och nätverkssäkerhet, bl.a. ingår att:
- Knäcka lösenord med hjälp av regnbågstabeller
  - Söka igenom system med Microsoft Baseline Security Analyzer (MBSA)
  - Säkra betrodd serveråtkomst med hjälp av digitala certifikat
  - Förhindra oönskad nätverksåtkomst med en personlig brandvägg
  - Kryptera och signera viktiga data
  - Avslöja och åtgärda sårbar kommunikation med hjälp av fjärrvärdar

## System- och nätverkssäkerhet: omfattande introduktion - 4 dagar

*kurser 468*

### Bygga en säker organisation

#### Verkliga hot som påverkar säkerheten

- Hackare inne och utanför
- Tjuvlyssning
- "Spoofing"
- Snokande
- Trojanska hästar
- Virus
- Avlyssning

#### En policy för cybersäkerhet: ditt grundskydd

- Definiera dina mål för informationssäkerhet
- Bedöma exponeringen

### Kryptografi för nybörjare

#### Skydda data med symmetrisk kryptering

- Välja algoritmer: DES, AES, RC4 och andra
- Välja lämplig nyckellängd och fördelning av nycklar

#### Lösa nyckelfördelningsproblem med asymmetrisk kryptering

- Generera nycklar
- Kryptera med RSA
- PGP och GnuPG
- Bedöma Web of Trust och PKI

#### Säkerställa integritet med omkastning

- Kasta om med MD5 och SHA
- Skydda data under överföring
- Skapa digital signatur

### Kontrollera användarens och värdens identitet

#### Utvärdera traditionella, statiska lösenordsscheman

- Skapa lösenord som förhindrar gissningsförsök
- Skydda mot attacker via "social ingenjörskonst"
- Kryptera lösenord för att hindra password sniffing

#### Kraftfulla autentiseringsmetoder

- Besvara utmaningar för att förhindra "man-in-the-middle-attacker"
- Förhindra återinloggning med engångslösenord och symboliska lösenord
- Använda biometrik som en del i tvåfaktorsautentisering

#### Autentisering av värdar

- IP-adressernas brister
- "Adress-spoofing" och dess motåtgärder
- Lösningar för trådlösa nätverk

### Förhindra systemintrång

#### Upptäcka sårbarheter i systemet

- Söka hål i operativsystemet
- Upptäcka problem med åtkomsträttigheter till filer
- Begränsa åtkomsten med fysisk säkerhet

#### Kryptera konfidentiella filer

- Kryptera med applikationsspecifika verktyg
- Återskapa krypterad data

#### Härda operativsystemet

- Låsa användarkonton
- Säkra administratörsrättigheter
- Skydda mot virus

### Skydda data mot nätverksintrång

#### Söka efter sårbarheter

- Begränsa åtkomsten till kritiska tjänster
- Förhindra buffertspill

#### Minska attacker av typen denial of service (DoS)

- Säkra DNS
- Begränsa följderna av "common attacks"

#### Använda brandväggar för att kontrollera nätverkstrafiken

- Jämföra olika brandväggar
- Förebygga intrång med filter
- Implementera en policy för cybersäkerhet

#### Bygga nätverksbrandväggar

- Utvärdera brandväggars egenskaper
- Välja en brandväggsarkitektur och en personlig brandvägg

### Göra nätverket konfidentiellt

#### Hot från LAN

- Snokande i nätverket
- Lindra hoten från anslutna värdar
- Partitionera nätverket för att förhindra dataläckage
- Identifiera sårbarheter i trådlös LAN

#### Konfidentiella anslutningar utåt

- Göra nätverket konfidentiellt genom kryptering
- Säkra datalänkar med PPTP och L2TP
- Middleware informationssäkerhet med SSL och TLS
- Använda SSH (Secure Shell)

#### Skydda data med IPsec

- Autentisering av externa platser
- Tunna trafiken mellan platserna
- Utväxla nycklar

### Administrera organisationens säkerhet

- Utveckla en säkerhetsplan
- Hantera incidenter
- Räkna upp de sex kritiska stegen