

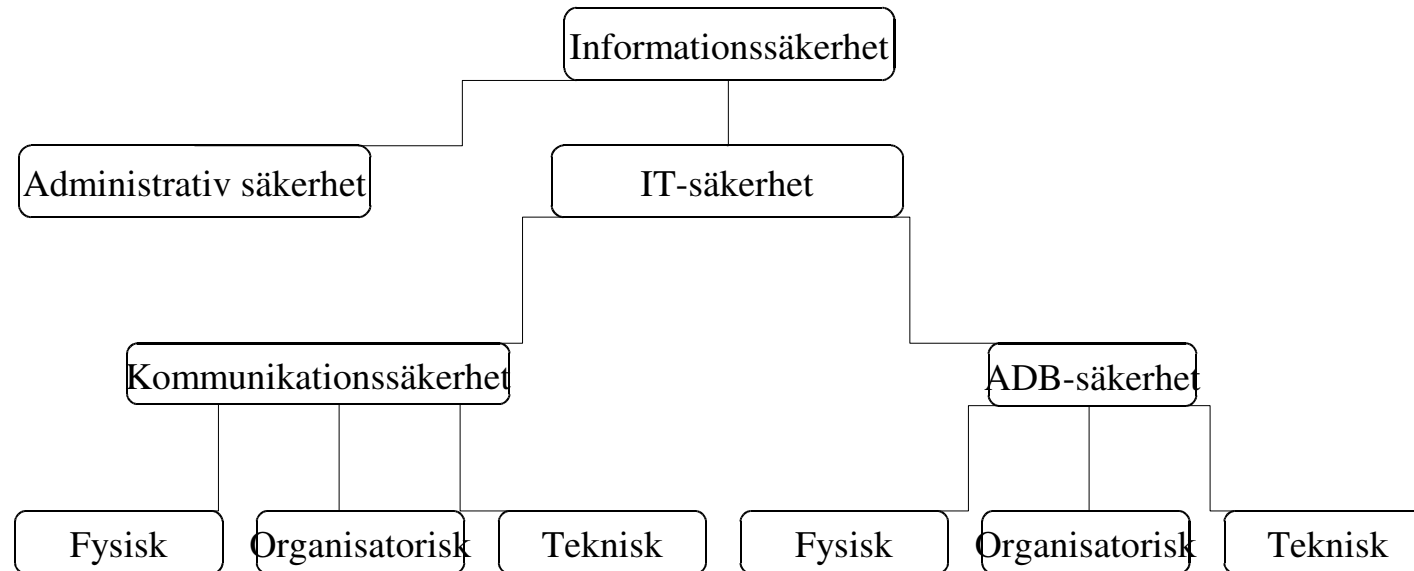
Informationssäkerhet

Varför informationssäkerhet?

Informationssäkerhet för vem?

Målet är "rätt" informationssäkerhet

Vad avses med informationssäkerhet



Aspekter på informationssäkerhet

- Tillgänglighet (resilience)
- Riktighet (integrity)
- Sekretess (privacy)

- Spårbarhet (trackability)
- Oavvislighet (non-repudiation)

Lagar och rättsliga krav

- Offentlighet, sekretess och tystnadsplikt
- Förvaring, arkivering
- Personlig integritet, marknadsföring
- Ensamrätt
- Regler om kryptering
- Straffrättsliga regler
- Ytterligare lagar
- Övriga "nyckelord" som tangerar rättsregler

Exempel på verkliga händelser på en kommun

Separat presentation

Risikanalyser

- Inventera skyddsvärda tillgångar
- Fastställ hoten mot tillgångarna
- Kombinationen av en tillgång och ett hot blir en risk
- Risken har sannolikhet och konsekvens
- Upprätta en riskmatris
- Fastställ åtgärder

Risikanalyt, exempel på skyddsvärda tillgångar

- Anseende
- Människor
- Information
- System och program
- Kommunikation
- Fysiska tillgångar, datorer och annan utrustning
- Lokaler
- Material
- Kapital

Tänkbara hot mot informationssäkerheten

- Mänskliga hot
 - Avsiktliga
 - Oavsiktliga
- Hot i omgivningen
 - Naturliga
 - Övriga

Risikanalyt, hot – allmänna exempel

- Förlust
- Stöld
- Brand
- Bristande kvalitet
- Obehörig åtkomst
- Obehörig användning
- Avbrott och katastrof

Hot - exempel i praktiken

- Sabotage / hackers / otrevlig programkod
- Brist på kunskap
- Driftstörning samtidigt med dålig backup
- Dåligt skydd mot obehöriga
- Dålig kvalitet / felaktig information

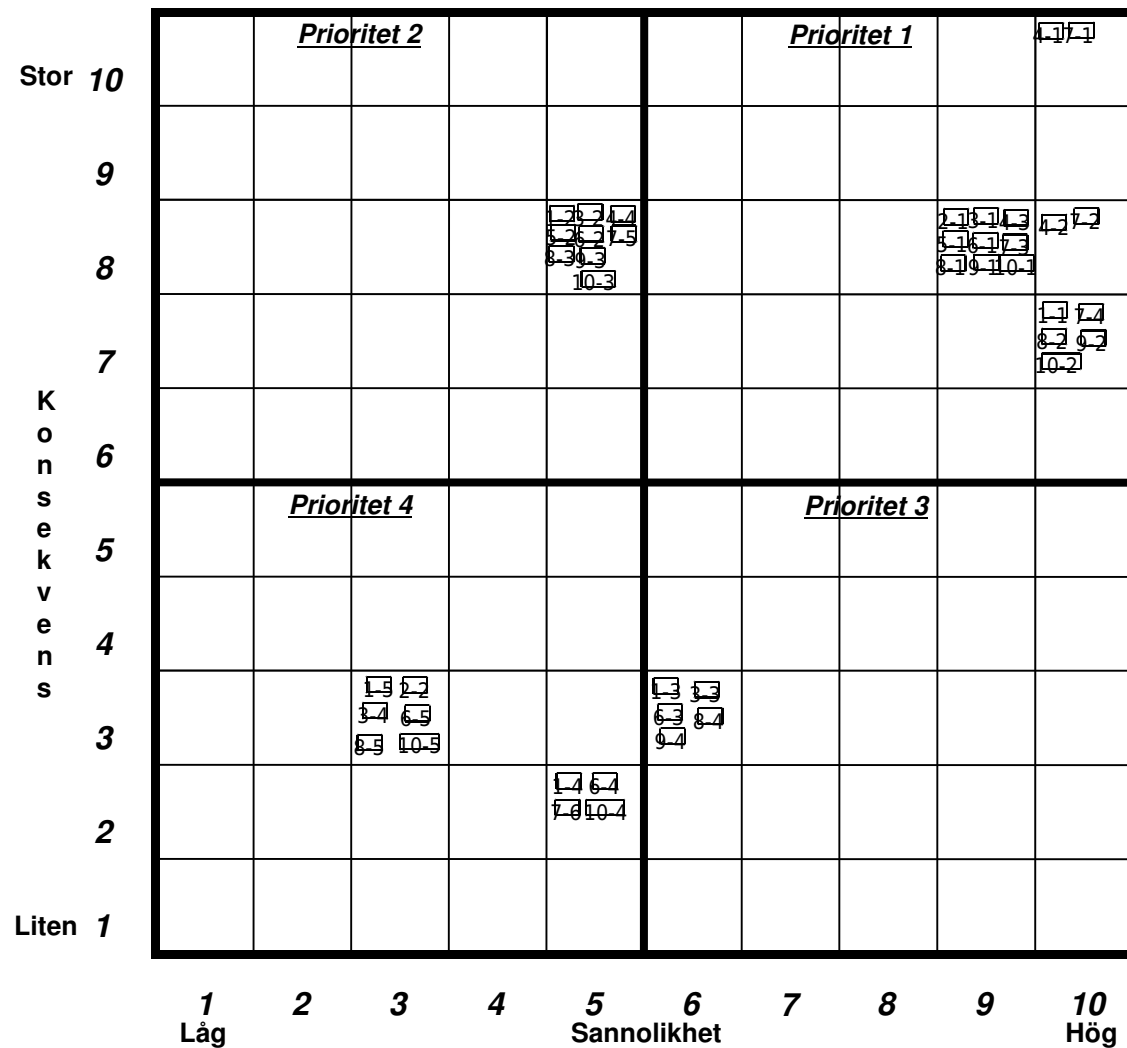
Risicanalys, riskbedömning

Kombinationen av en tillgång och ett hot är en risk

För varje risk:

- Bedöm sannolikheten att det ska inträffa
- Bedöm konsekvenserna om det inträffar
- Plotta in resultatet i riskmatris

Riskmatris, exempel



Risikanalyt, lite om kvadranterna

- Prio 1: hög sannolikhet stor konsekvens
 - Prio 2: låg sannolikhet stor konsekvens
 - Prio 3: hög sannolikhet låg konsekvens
 - Prio 4: låg sannolikhet låg konsekvens
-
- Man vill först och främst flytta prio 1 risker neråt eller till vänster

Risicanalys, prioritera, åtgärda

- Värdera kvadranterna
- Fastställ vad som ska flyttas
- Fastställ orsakerna för varje risk
- Fastställ förebyggande skydd
- Fastställ skadereducerande skydd

Förebyggande skydd och skadereducerande skydd

- Med förebyggande skydd flyttar vi oss till vänster i matrisen och sänker sannolikheten för att risken ska falla ut
- Med skadereducerande skydd flyttar vi oss nedåt i matrisen och begränsar skadorna om risken trots allt fallit ut

Exempel på skyddsåtgärder

- Policy och instruktioner
- Avtal
- Utbildning
- Tekniska / logiska åtgärder
- Fysiska åtgärder
- Försäkringar
-

Skyddsåtgärder – att tänka på

- En skyddsåtgärd kan ”bota” många risker. Både hög och lågprioriterade
- Vissa risker kräver flera skyddsåtgärder
- Nu kan vi ta hänsyn till de eventuella skyddsåtgärder som redan fanns

Exempel på IT-relaterade hot elak kod (malware) sida 1 (3)

- Botnet
- Click-jacking
- Cookie-filer
- Cracking
- Cross-site scripting (XSS)
- DOS och DDOS (denial of service)
- Hoax (bluff, lurendrejeri)

Exempel på IT-relaterade hot elak kod (malware) sida 2 (3)

- Infekterade filer, webbsidor, bilder
- Nätfiske (phishing)
- Ping flooding
- Portscan
- Relay host (relä-värd)
- Social engineering
- Spam – junk mail (skräppost, massutskick)

Exempel på IT-relaterade hot elak kod (malware) sida 3 (3)

- SQL-injection
- Syn-flood, flooding
- Trojaner
- USB-minnen eller CD
- USB-minnen typ U2
- Virus
- Worms (maskar)

Skyddsåtgärder, exempel 1 (2)

- Skydd för router
- Skydd för datorn – skydda information
- Problem med andra apparater
- Uppdatera datorn
- Backup – skyddskopiering
- Både admin och användarkonton

Skyddsåtgärder, exempel 2(2)

- Lösenord
- E-post
- Att surfa med webbläsare
- Sociala medier
- Bankaffärer
- Att handla på Internet