Metoder för att öka informationssäkerheten

och därmed minska säkerhetsriskerna

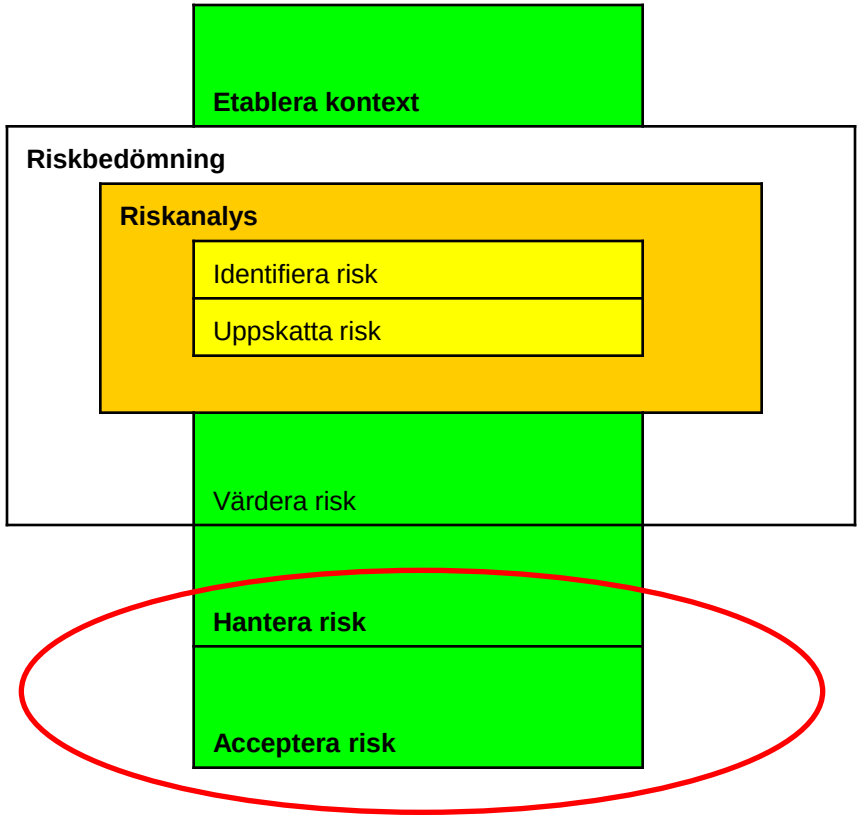
Mål

Att utifrån en riskanalys

- identifiera förbättringsåtgärder som ökar säkerheten i verksamheten
- kunna välja lämpliga åtgärder som minskar risken i sammanhanget

Att hantera risker

- Etablera kontext
- Riskbedömning med riskanalys
- Värdera risk
- **Hantera risk**
- **Acceptera risk**



Planera att minska risken

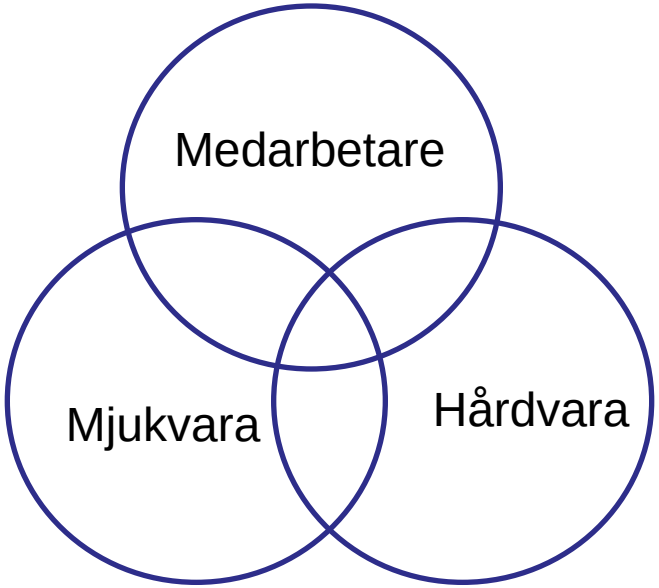
- Reducera risken
- Bibehåll risken
- Undvik risken
- (sälj den)

- Gör en plan över risker och åtgärder!

Använd indata från riskanalysen

- Skyddsvärda informationstillgångar?
- Vad används de till?
- Var finns de?
- Hur skyddas de idag?

Länkarna i informationskedjan



Exempel på informationstillgångar

- Information
  – kunddatabas, arbetsmetodik, dokument (ritningar, avtal, prislistor, etc.)
- Program
  – applikationer, operativsystem...
- Tjänster
  – kommunikationstjänster, abonnemang...
- Fysiska tillgångar
  – servrar, datamedia, nätverk...

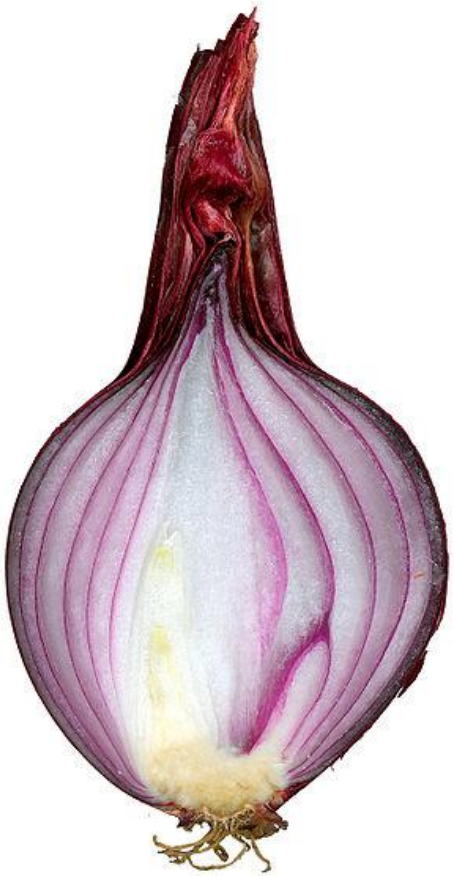
Diskutera

- Är **individen/människan** en skyddsvärd informationstillgång?
- Vad används människor till?
- Var finns de?
- Hur skyddas de idag?

Skyddsfilosofi

- Lökskalsprincipen
  - skydd i flera lager
- Gäller för både människor och teknik

Många lager ger ett robust system



Skyddsfilosofi i 14 lager

1. Säkerhetsledning (säkerhetspolicy, processer, instruktioner)
2. Personalen (utbildning)
3. Tillgänglighet och tillförlitlighet (teknik)
4. Kringmiljön (fysisk miljö)
5. Tillträde för personal och andra människor
6. Försörjning – el, luft, etc.
7. Brandskydd
8. Skydd mot vattenskador
9. Systemsäkerhet
10. Nätverk och telekommunikation
11. Systemutveckling och systemändringar
12. Persondatorer och arbetsstationer
13. Säkerhetskopiering och arkivering
14. Kontinuitetsplanläggning

Några sätt att öka säkerheten

Vad och hur ska vi göra för att skapa säkerhet på djupet?

- Definiera enkla åtgärder som ger skydd i vart och ett av de 14 lagren!
- Jobba gruppvis – 10 minuter

Några sätt att öka säkerheten

- Tydlig säkerhetspolicy, processer och rutiner (1)
- Tydliga instruktioner som underlättar för användare att göra rätt (1)
- Utbilda/träna alla medarbetare i informationssäkerhet (2)
- Säkra arbetsmiljön: lås, märkning, övervakning, tillträdeskontroll (4, 5,12)
- Säkra tekniska lokaler: el, luft, skydd mot brand och vattenskador (6, 7, 8)
- Säkra system: konfigurationsstyrning av system och applikationer (3, 9, 10)
- Ändringshantering (11)
- Klassning och arkivering av data och dokument (13)

Att skapa en säkerhetskultur

- Säkerhets**policy**
  (**vad**)
- Gemensamma **processer och rutiner**
  (**hur**)
- Begripliga **instruktioner** för vanliga människor
  (**vem** gör **vad** och **hur**)

Att skapa en säkerhetskultur

- Varje **individ** har ansvar för att upprätthålla informationssäkerheten **lokalt**
  (inte enbart en fråga för IT-avdelningen eller säkerhetsansvarig)
- Prata med medarbetarna om effekten av (o)säkerhet
- Skapa engagemang i gruppen genom att lyssna och ta vara på idéer och förslag
- Följ upp fel och incidenter – mät!
- Arbeta förebyggande!
  Planera – Genomför - Följ upp - Förbättra

Diskutera

- Hur skapar du en effektiv säkerhetskultur?
- Utgå från gruppens riskanalys

Förslag på aktiviteter

- En stående punkt på personalmöten
  - säkerhetsfrågor
- Dramatisera och avdramatisera säkerhet, berätta om incidenter och deras effekter i ”besvär, tid och pengar”, t ex demonstrera tangentbordsloggning mha USB-minne
- Visa hur bra lösenord/fraser ser ut
- Byt lösenord regelbundet
- Skapa riktlinjer för säker surfning
- Skapa riktlinjer för hantering av sociala media

Förslag på aktiviteter

- Publicera säkerhetsinformation på intranätet, anslagtavlor, toalettdörrar, i fikarum – överallt där personalen kan läsa den
- Håll rent på skrivbordet
- Lås in viktiga dokument när de inte används
- Håll rent vid skrivare och kopiatorer
- Kasta oanvända utskrifter i säkerhetsbehållare
- Registrera och eskortera alltid besökare – in och ut

Facebook, YouTube, Twitter...

Sociala media

- Har yngre och äldre olika uppfattning om vad man kan berätta om sig själv?
- Accepterat eller inte på jobbet?
- Finns det riktlinjer för användning?
  (lösenord, profiluppgifter, användning)

- Har du googlat på ditt namn?

Om lösenord – råd från SITIC

- Lösenord är personliga och får inte överlåtas.
- Ett lösenord ska bestå av **minst åtta tecken** och bestå av minst tre av de fyra teckenuppsättningarna **versaler, gemener, siffror och icke-alfanumeriska tecken (specialtecken)**.
- Lösenordet får inte vara detsamma som användarnamnet eller bestå av delar av användarnamnet.
- Lösenordet får **inte vara knutet till personlig information** som till exempel namn, personnummer och telefonnummer.
- Ett lösenord får inte vara en vanlig teckenkombination, ett ord eller en vanlig kombination av ord som finns i ordböcker eller används i dagligt språkbruk, oberoende av språk.
- Ett lösenord får inte vara ett ord som är skrivet baklänges.
- En användares lösenord som används inom organisationen får inte vara likadant som andra lösenord som används utanför organisationen.
- Lösenord ska bytas var tredje månad och får inte vara likadant som ett tidigare nyttjat lösenord.
- **Lösenord** bör inte skrivas ned. En anteckning om lösenordet ska behandlas som en **värdehandling**.

Surfa lugnt

- Svara inte på ”udda” mejl
- Öppna inte bilagor i onödan, kan innehålla en trojan som öppnar en bakdörr till datorn
- Tacka **NEJ** till erbjudanden som är **för bra** för att vara sanna – inget är gratis!
- Skicka inte pengar, personuppgifter eller kontouppgifter till någon du inte känner
- Betala aldrig i förskott på Blocket och liknande sajter

13 goda råd från PTS

1. **Stäng av datorn när den inte används**
2. Ha en brandvägg och ett antivirusprogram installerat på datorn - håll dem uppdaterade **(IT-avd)**
3. Ta regelbundet säkerhetskopior av viktig information lagrad på datorn **(IT-avd)**
4. **Var noga med lösenord – välj med omsorg, byt ofta och håll det hemligt**
5. Uppdatera ditt operativsystem och din webbläsare regelbundet **(IT-avd)**
6. **Var försiktig med att lämna ut personliga uppgifter - se upp för nätfiske (phishing)**
7. **Undvik skräppost – använd flera e-postadresser**
8. **Öppna inte bifogade filer i e-posten utan eftertanke**
9. **Ladda ned med försiktighet**
10. Skydda ditt trådlösa nätverk **(IT-avd)**
11. Undvik kapning av modem – surfa med ljudet på **(? - IT-avd)**
12. Var uppmärksam på spionprogram – kontrollera datorn regelbundet
13. **Var medveten om cookies**

Standarder

- ISO/IEC 27002:2005 Informationsteknik – Säkerhetstekniker – **Riktlinjer för styrning av informationssäkerhet**
- ISO/IEC 27005:2008 Informationsteknik – Säkerhetstekniker – **Riskhantering för informationssäkerhet**

Handböcker på svenska

- **Stora säkerhetshandboken – en praktisk årskalender** Agneta Syrén/SIS Förlag
- **Svenska IT-säkerhetshandboken 1.0**, LabCenter
- **Säkra ditt företag, informationssäkerhet för chefer och ledare**, Nicklas Lundblad/Liber
- **Effektiv säkerhetsorganisation**, Jan-Olof Andersson/SIS Förlag
- **Säkerhetshuset**, Jan-Olof Andersson/SIS Förlag
- **Helsäkert, en bok för dig om säker information**, Dataföreningen i Sverige/Studentlitteratur

Om du vill veta mer – webben

- www.informationssäkerhet.nu
  Portal för informationssäkerhetsarbete
- www.sakerhetspolisen.se
  ”Säkerhetsskydd, en vägledning”
- surfalugnt.se
  Surfa lugnt-kampanjen
- www.pts.se
  Tretton goda råd