Riskanalys och riskhantering

Margaretha Eriksson,
civ.ing. och doktorand i informationssäkerhet KTH

Föreläsning 2

Mål

- känna till stegen i en risk- och sårbarhetsanalys
- kunna använda risk- och sårbarhetsanalys
- kunna självständigt genomföra en enkel risk- och sårbarhetsanalys

Riskanalys

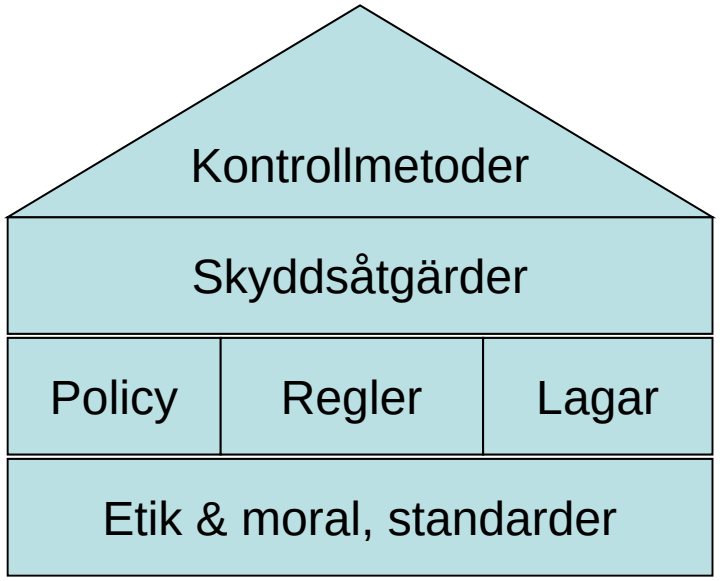
- Ur verksamhetsperspektiv (servicekvalitet)
- med avseende på informationstillgångar
- i avgränsat system

Riskanalys i korthet

1. Identifiera skyddsvärda tillgångar, viktiga för verksamheten
2. Identifiera hot mot dem
3. Identifiera befintliga säkerhetsåtgärder
4. Identifiera svagheter
5. Vilka konsekvenser kan det få?
6. Skapa några scenarier för att bedöma riskerna m h a konsekvens och sannolikhet
7. Hantera identifierade risker på lämpligt sätt

Filosofin ”Säkerhetshuset”

En stabil grund…

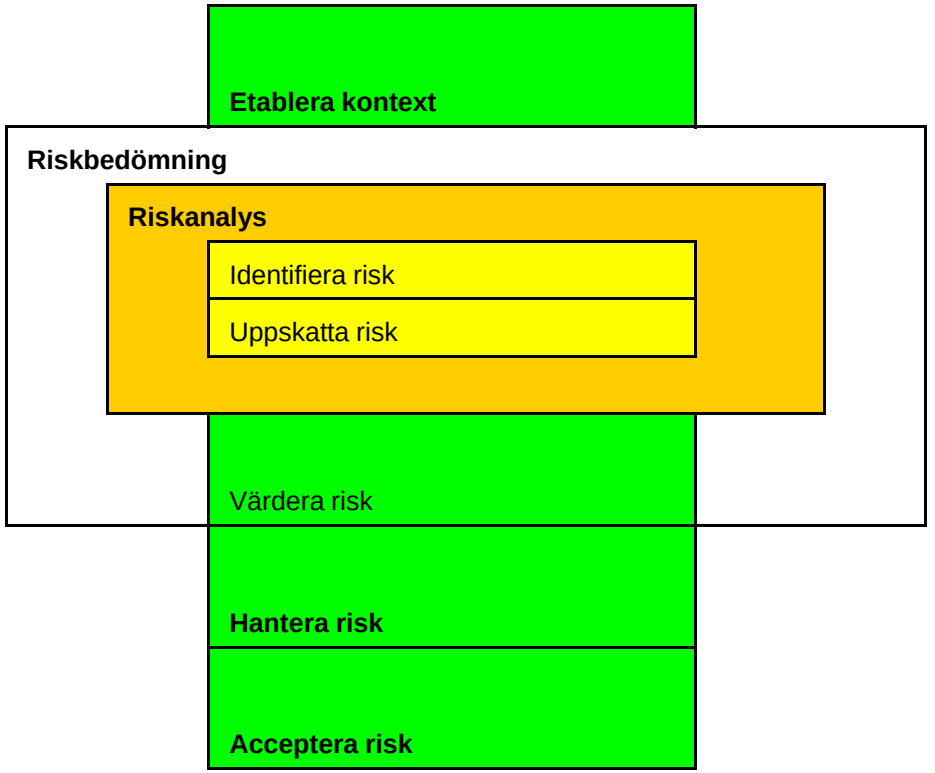


Hot och sårbarheter

- Vilka är hoten?
- Vad kan hända?
- Hur stor är risken?
- Hur stora blir konsekvenserna?

Riskhanteringsprocessen

- Sammanhang (kontext)?
- Riskbedömning med riskanalys
  - Identifiera risk
  - Uppskatta risk
- Värdera risk
- Hantera risk
- Acceptera risk



Kontext - riskvärdering

Ta fram **relevant information** om informationssäkerheten i organisationen

- Grundläggande kriterier för **riskvärdering**
  - strategiska värden
  - lagar och avtal?
  - konfidentialitet, integritet, tillgänglighet; ”CIA”
  - externa förväntningar
  - goodwill och renommé

Kontext - påverkan

- Kriterier för **påverkan** på
  - värdering och klassning av tillgången
  - verksamheten
  - affären och ekonomiska värden
  - planer och deadlines
  - renommé
  - efterlevnad av lagar och avtal

Kontext - riskacceptans

- Grundläggande kriterier för **riskacceptans**
  - accepteras och fastställs av högre chef
  - uppskattad vinst/uppskattad risk
  - flera riskklasser?
  - krav på framtida åtgärder?
- Verksamhetskriterier
- Lagar och föreskrifter
- Drift
- Teknik
- Ekonomi
- Sociala och humanitära faktorer

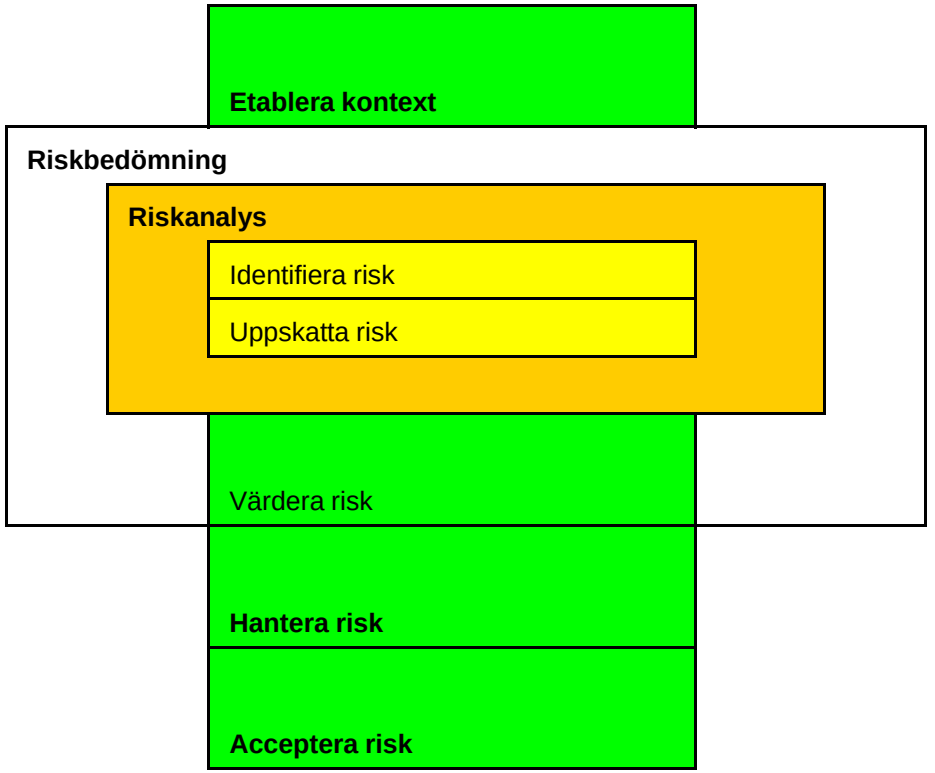
Kontext - organisation

- Process för riskhantering
- Roller och ansvar?
- Intressenter?
- Relation mellan organisation och intressenter?
- Eskalering av beslut – till närmast högre chef
- Arkivering av redovisande dokument

OBS Denna organisation ska vara godkänd av ansvarig chef i organisationen.

Riskbedömning

- **Riskbedömning och riskanalys**
  - Identifiera risk
  - Uppskatta risk



Riskbedömning

- Identifiera, kvantifiera eller beskriv riskerna
- Prioritera m a p kriterier för
  - riskvärdering och
  - relevanta verksamhetsmål

Identifiera risker

- Händelse som kan leda till skada
- Hur, var och varför?

Identifiera värdefulla tillgångar

... som behöver skyddas med:

- Namn på tillgång
- Ägare
- Plats
- Funktion

Namn	Systemägare	Plats	Funktion
Server xx	IT-avd	Rum 321	Webbserver
Router xx			
Brandvägg xx			

Identifiera hot

Identifiera hot mot värdefulla tillgångar

- Information från
  - incidenter
  - systemägare
  - användare
  - hotkataloger (”levande” innehåll)
- Varifrån (källa)

Identifiera sårbarheter

- Identifiera sårbarheter inom
  - organisation,
  - processer och rutiner,
  - hanteringsrutiner,
  - personal,
  - fysisk miljö,
  - konfiguration av info-system,
  - maskin- och programvara,
  - kommunikationsutrustning,
  - externa parter
- Identifiera befintliga och planerade säkerhetsåtgärder
- Identifiera konsekvenserna m a p ”CIA”

Resultat

Lista med incidentscenarier med konsekvenser för tillgångar och verksamhet

Uppskatta enskilda risker

- Kvalitativt
  (Låg, Mellan, Hög)
- Kvantitativt
  (t ex 1-10-skala eller kostnad,
  om det går att uppskatta)

Uppskatta konsekvenser

Använd listan med incidentscenarier

- Tillgångens ersättningsvärde? (återställning eller ersättning av information)
- Konsekvenser för verksamheten?

HD

Publicerad 20 april 2009 kl. 06:16 Uppdaterad 20 april 2009 kl. 08:48

Dyr nota efter virusattacken

Runt en miljon kronor kommer kommunens nota att landa på för det elakartade datavirus som drabbade Region Skåne och lamslog Höganäs Kommuns datasystem i januari. Och vad värre är att det i princip kan hända igen.

HÖGANÄS. – Lägger man ihop IT-avdelningens kostnader på 350 000 kronor och de kostnader som kommer av förseningar och ineffektivitet i övrig verksamhet hamnar summan på någonstans runt en miljon kronor, säger kommunchef Per Selldén.

Vad det exakta beloppet blir går först att räkna ut vid årsskiftet.

Förutom stora kostnader och huvudbry för de anställda har virusattacken lett till ett ökat säkerhetstänkande inom kommunen. Sedan i januari har man uppdaterat operativsystemet och minskat ner de anställdas befogenheter. Mer sköts nu av IT-avdelningen.

Men enligt IT-chefen i Höganäs kommun Bo Nilsson är det omöjligt att skapa ett helt säkert system.

– Det är ett stort problem att det inte går att skydda sig mot sådana här attacker till 100 procent. Det ställer ju frågor kring hur vi har byggt upp

Detta hände

Det var under trettonhelgen, den 3-4 januari, som en trojan, eller om man så vill en "datamask", på okänt sätt tog sig in i Höganäs kommuns datanätverk. 750 datorer och 900 konton drabbades och lamslogs. Stoppet varade i nästan två veckor. Samma virus spred sig också till Region Skånes datanätverk. Över 10 000 datorer drabbades, vilket ledde till risker för patienter.

Bedöm sannolikhet för incidentscenario

- Bedöm sannolikheten för varje scenario baserat på
  - erfarenhet
  - statistiska underlag, t ex incidentrapporter
- Avsiktliga hotkällor
  - motiv och förmåga hos angripare
  - attraktionsvärde
- Oavsiktliga hotkällor
  - geografiska faktorer som
    extremt väder, vulkanutbrott, mänskliga fel, etc
- Sårbarheter
- Befintliga säkerhetsåtgärder och hur effektiva de är

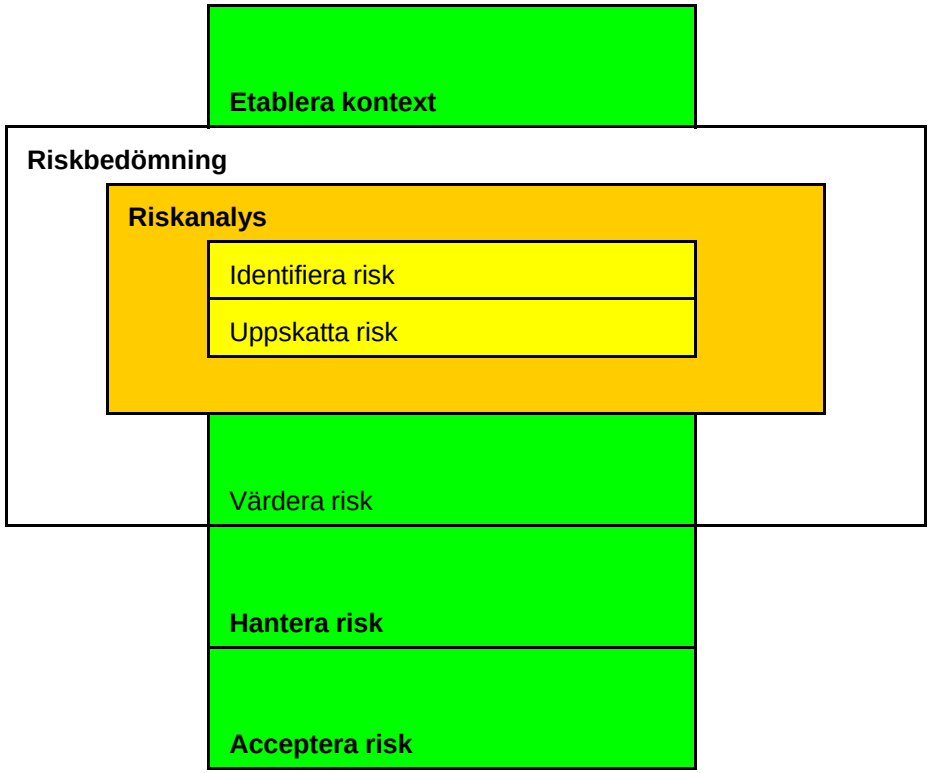
Nivå för uppskattad risk

Uppskattad risk = **S** x **K**

Sannolikhet för incidentscenario **x Konsekvens**

Värdera risk

- **Värdera risk**
- Hantera risk
- Acceptera risk



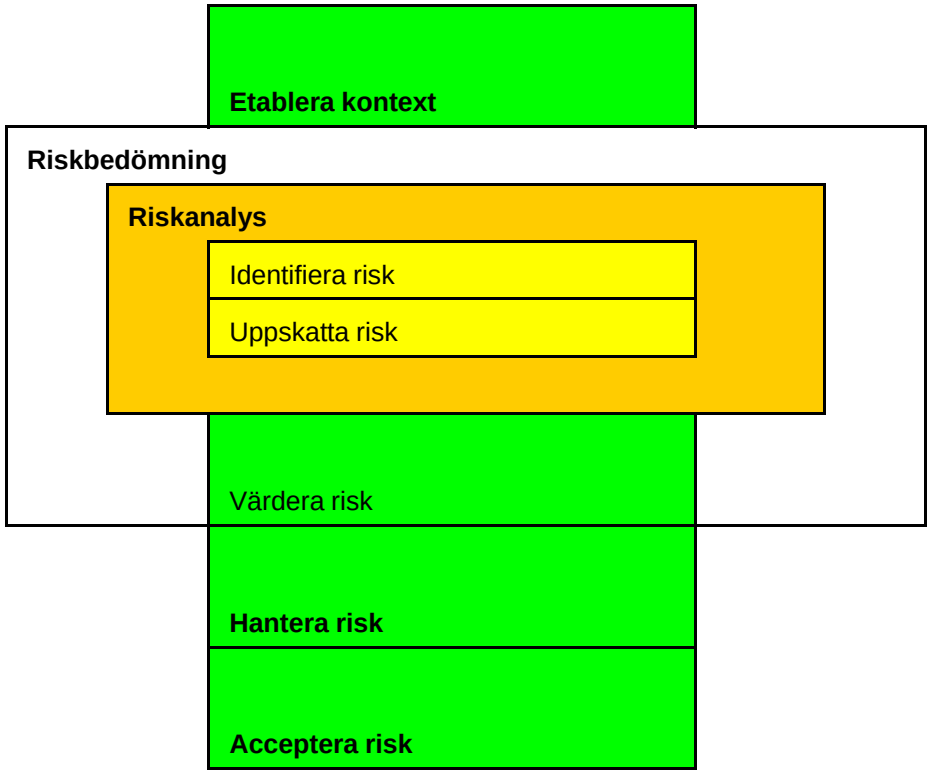
Värdera risk

- Jämför risknivåerna med
  - kriterierna för riskvärdering
  - kriterierna för riskacceptans
- Är kriterierna relevanta?
- Är system eller process viktig?

- Besluta om aktiviteter och prioriteringar

Hantera risk

- **Hantera risk**
- Acceptera risk



Hantera riskerna

- Säkerhetsåtgärder för att
  - reducera,
  - bibehålla,
  - undvika, eller
  - överföra risker
- Skriv en plan för riskhantering

- **Chefen** ska aktivt acceptera risken!

Om risk- och sårbarhetsanalys

- Vem ska läsa rapporten?
  målgrupp: chefer eller tekniker?
- Kortfattad, inte längre än nödvändigt
  (Det är en kort rapport, ingen uppsats!)
- Klassificera och hantera rapporten som **konfidentiell information**

RSA-rapportens rubriker

- Kort beskrivning
- Bakgrund
- Område
- Inblandad teknik/utrustning
- Inblandande personer
- Vem äger problemet?
- Scenario/case
- Konsekvenser
- Riskbedömning
- Hur riskerna hanteras

Exempel på RSA-rapport

- **Kort beskrivning:** ”Den nya webblösningen har långa svarstider (min 30 sekunder) vid mer än 10 samtidiga användare och upplevs som segt. Dessutom har sajten gått ner fullständigt vid flera tillfällen och orderdata har försvunnit.”
- **Bakgrund:** ”2011 investerade företaget i ett nytt webbhandelssystem för ökad tillgänglighet. System skulle kunna hantera 300 transaktioner/samtidiga användare utan att prestanda påverkades …”
- **Område:** ”Webbhandelssajt, orderdatabas, etc.”
- **Inblandad teknik/utrustning:** ”Webb, webbserver, ISP, etc.”
- **Inblandade personal:** ”Webbdesign, IT-avdelning, säljavd.”
- **Vem äger problemet:** ”IT-avdelningen? Leverantören? Säljavd?”

Exempel på RSA-rapport (forts.)

- **Konsekvens:** ”Genom att webben är seg eller helt nere tappar vi kunder som går till andra webbhandlare.”
- **Riskbedömning:**
  Hur riskbedömning skett i detta fall: Varför detta sätt att bedöma risk är rimligt i detta fall:
  Värdering:
  Prioritering:
  Åtgärdsplan:
- **Hur riskerna kan hanteras:**
  Diskussion:
  (Kring uppgiften i stort, vad som har gått bra, vad som kunde ha gått bättre)