Riskhantering

Del av kursen ETE352 Cybersäkerhet – grunder och medvetenhet som ges vid Linköpings universitet

Mikael Asplund

LINKÖPINGS UNIVERSITET

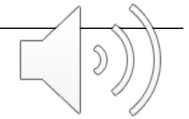
Vad är risk?

- Risk som ett hot
  - Svensk ordbok: ”möjlighet till negativ utveckling eller negativt resultat”
  - Exempel: att en dator blir infekterad

- Risk som ett mått
  - Risk = Konsekvens x Sannolikhet

Varför riskhantering?

- Nödvändig del av all verksamhetsstyrning
- Går inte att eliminera alla säkerhetshot
  - Prioritering nödvändigt
- I ökande utsträckning lagkrav och leverantörskrav



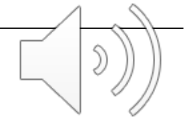
Riskhantering vs. hotmodellering

Riskhantering

- Inte bara cybersäkerhet
- Fokus på organisationen
- Tydlig ekonomisk relation
- Hotmodellering en del av eller input till riskhantering

Hotmodellering

- Specifikt för cybersäkerhet
- Fokus på system och hot
- Tekniskt mer detaljerad
- I vissa fall (PASTA) inkluderar riskhantering



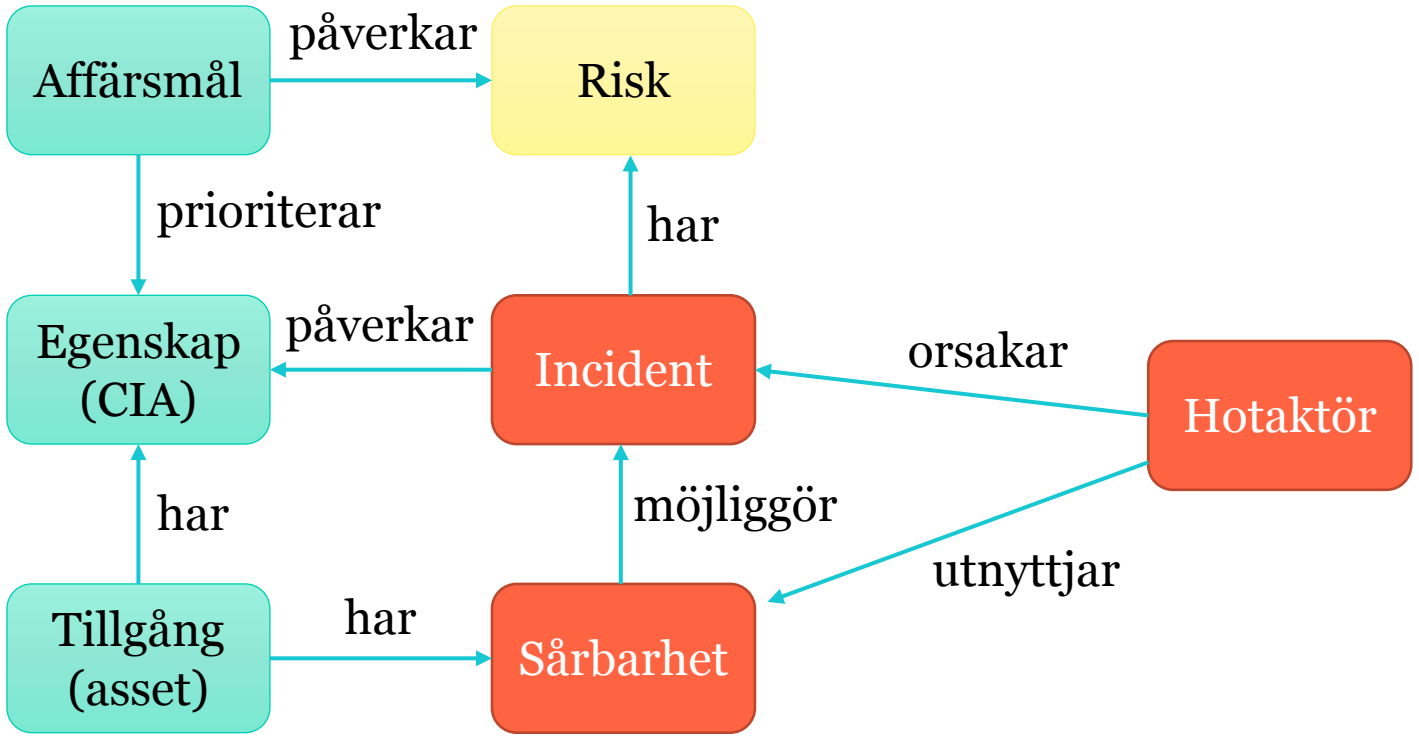
Tillgång
Asset

- Information, tjänst, enhet eller annat som är av värde för en organisation.

- Vilken egenskap ska skyddas/kan hotas hos en tillgång?
  - CIA, STRIDE

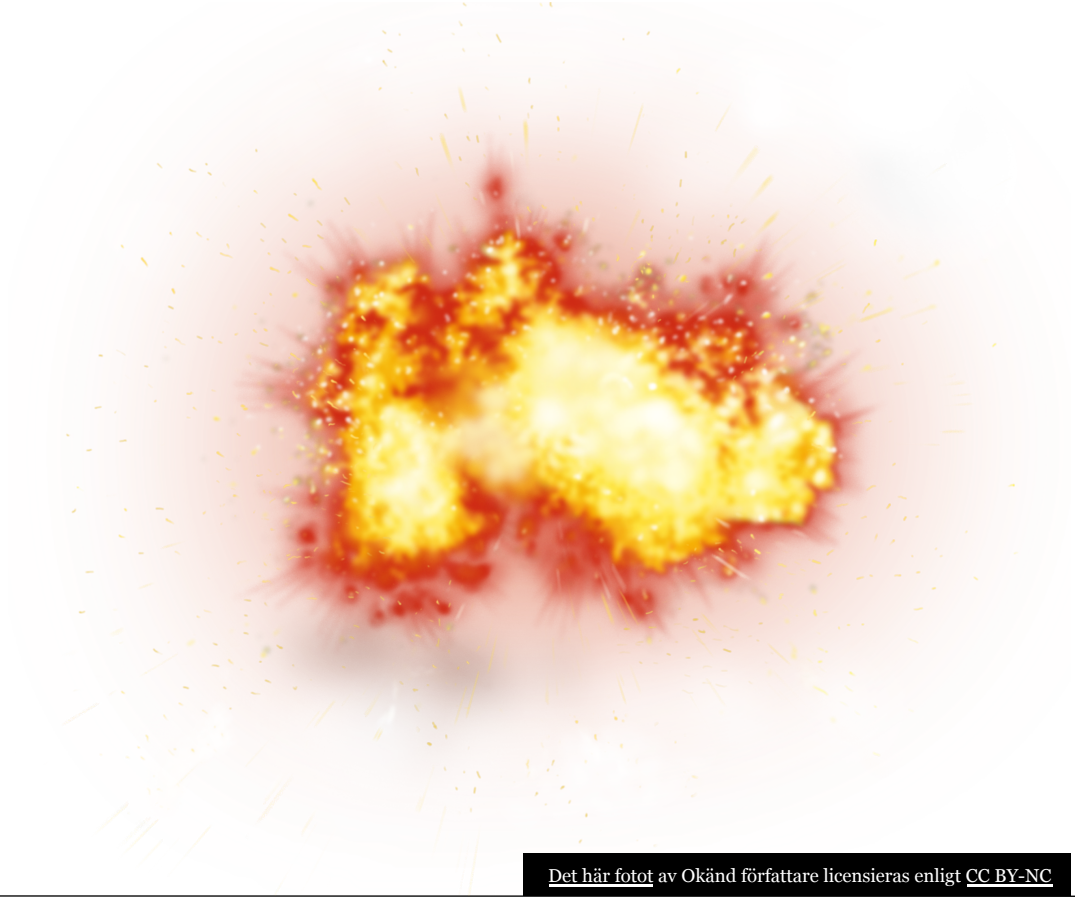
- Inom informationssäkerhet: fokus på datatillgång

Grundläggande begrepp



Konsekvens

- Hur drabbas organisationen?
- Skala som ska definieras av organisationen
- Kan vara olika skalor för olika typer av konsekvenser



Exempel från informationssakerhet.se

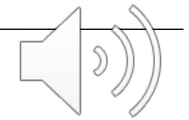
Konsekvens	Ekonomisk förlust	Minskat förtroende	Avbrott i verksamheten
Allvarlig	2 miljoner kronor och uppåt eller avvikelse på över 20% av budget	Ihållande drev i rikstäckande medier, eller av organiserade grupperingar i sociala medier. Ej endast enskilda personer pekas ut, utan även organisationens grundläggande kultur.	Avbrott i en eller flera kritiska verksamheter som är längre än godtagbart. Omfattande omprioriteringar av verksamheten.
Betydande	500 000 – 2 miljoner kronor eller avvikelse på 10-20% av budget	Nyheter i både riks- och lokalmedia och i organiserade grupperingar i sociala medier. Missnöjet är dock begränsat till enskilda händelser eller enskilda personers agerande.	Avbrott i en kritisk verksamhet som är längre än godtagbart. Stora omprioriteringar av verksamheten.
Måttlig	1 – 500 000 kronor eller avvikelse på 5-10% av budget	Enstaka missnöjda individer som uttalar sig i sociala medier, eller en mindre notis i lokalpress.	Avbrott i en eller flera verksamheter som inte är kritiska och som är längre än godtagbart. Mindre omprioriteringar av verksamheten.
Försumbar	Ingen förlust	Liten negativ uppmärksamhet	Försumbara avbrott i verksamheten och/eller inga omprioriteringar av verksamheten.

Sannolikhet

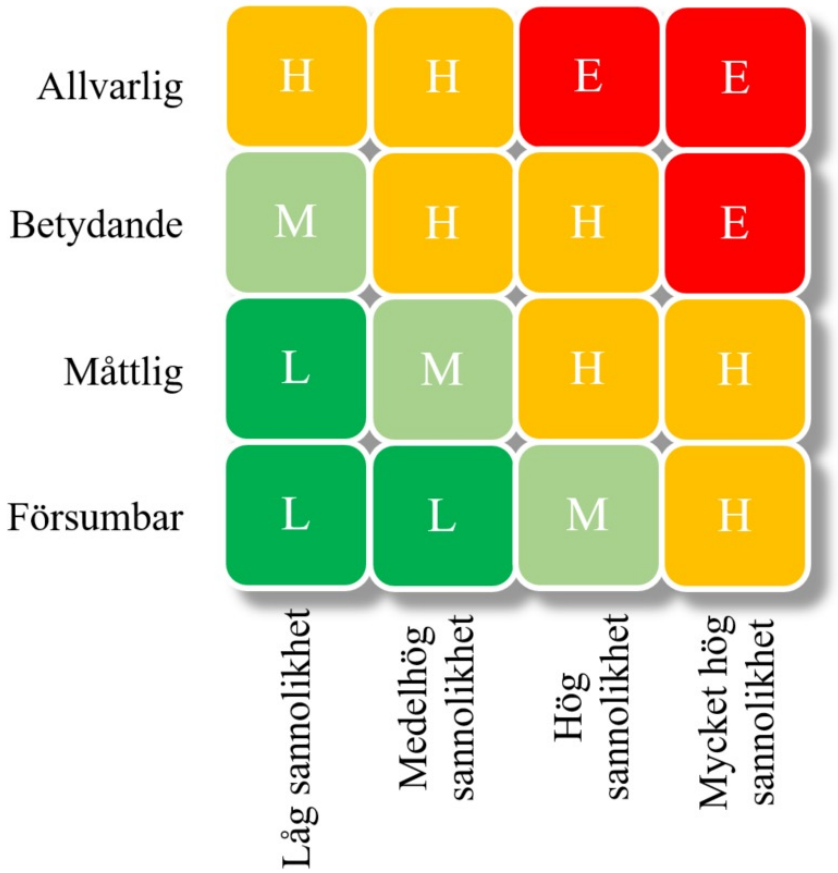
- Måste kombineras med en viss tidsperiod
  - Sannolikhet per år
  - Sannolikhet under en produkts livstid
- Sannolikhet under en viss tidsperiod == Genomsnittlig frekvens
- En skala räcker, men varierar mellan organisationer

Begrepp	Intervall
Mycket hög sannolikhet	1-10 ggr/år
Hög sannolikhet	0,5-1 ggr/år
Medelhög sannolikhet	0,05-0,5 ggr/år (mellan en gång vartannat till en gång per 20 år)
Låg sannolikhet	< 0,05 ggr/år (mindre än en gång per 20 år)

www.informationssakerhet.se



Riskmatris



www.informationssakerhet.se

https://cybersakerhet-grund.ida.liu.se

LINKÖPINGS UNIVERSITET