Riskanalys och informationssäkerhet 7,5 hp

Margaretha Eriksson
Civ.Ing. och doktorand i informationssäkerhet KTH
irbiskonsult@tele2.se

Föreläsning 1

Vad menar vi med ”säkerhet”?

Säkerhet är en grad av skydd mot fara, skada, förlust, och brott.
Säkerhet som en form av skydd är *strukturer och processer som ger eller förbättrar säkerhetsförhållandena.*

Säkerhet är “en form av skydd där en separation skapas mellan tillgångarna och hotet". Det omfattar, men är inte begränsat till, att eliminera antingen tillgången eller hotet.

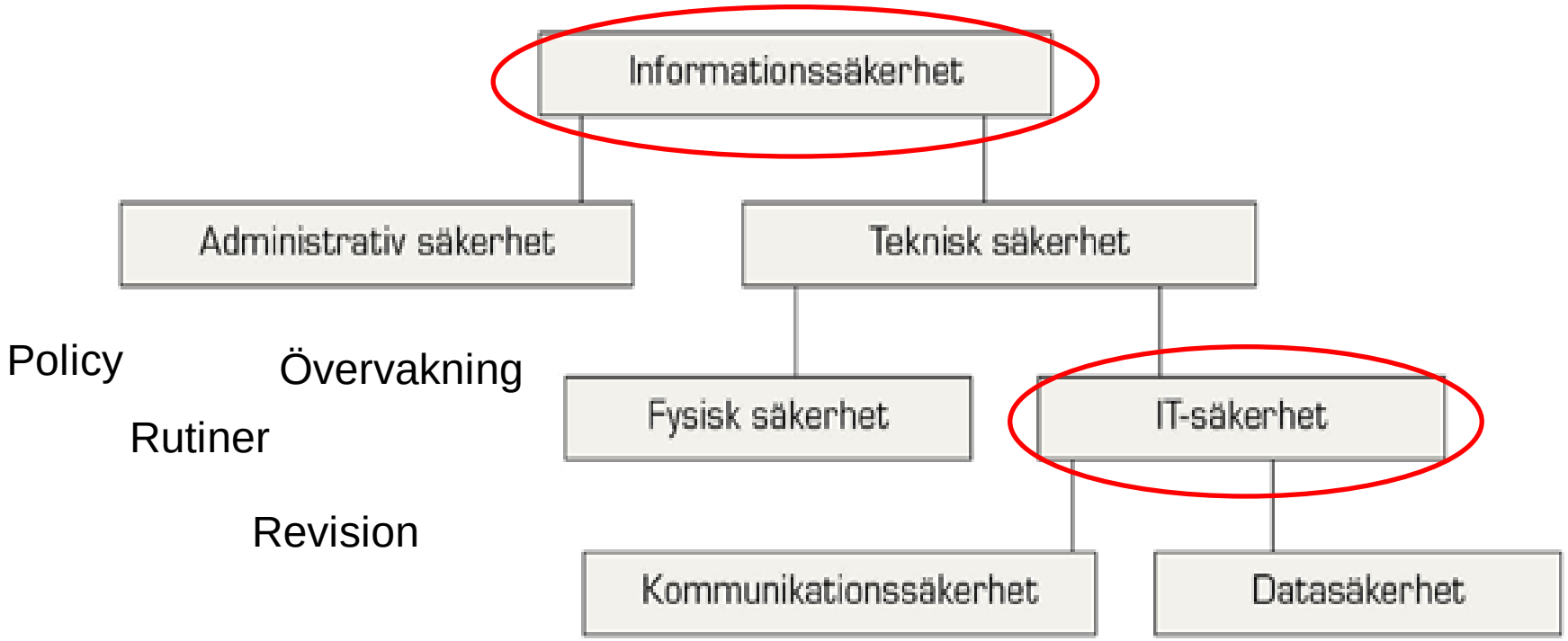
Wikipedia/Institute for Security and Open Methodologies (ISECOM) i OSSTMM 3

Vad menar vi med ”säkerhet”?

Uppdelning enligt internationell standard

- Informationssäkerhet – både teknik och administration av system med användare
- IT-säkerhet – teknisk utrustning, datasäkerhet och kommunikationssäkerhet

Många olika slags säkerhet



Viktiga nyckelord

- Informationssäkerhet
- IT-säkerhet
- Informationstillgång
- Konfidentialitet
- Riktighet
- Tillgänglighet
- Ansvarighet och oavvislighet
- Spårbarhet

”Informationssäkerhet”

Definition enligt svensk standard

- **Informationssäkerhet**
  säkerhet för **informationstillgångar** avseende förmågan att upprättålla **konfidentialitet**, **riktighet** och **tillgänglighet**
  (även **ansvarighet** och **oavvislighet**)
- Omfattar fysisk säkerhet,
  IT-säkerhet och administrativ säkerhet

”IT-säkerhet”

Definition enligt svensk standard

- **IT-säkerhet**
  säkerhet beträffande IT-system med förmåga att förhindra obehörig åtkomst och obehörig eller oavsiktlig förändring eller störning vid databehandling samt dator- och telekommunikation

”Informationstillgångar”

Definition enligt svensk standard

- **informationstillgångar**
  en organisations informationsrelaterade tillgångar
- Några exempel:
  information i kunddatabas,
  program, applikationer, operativsystem,
  kommunikationstjänster,
  fysiska tillgångar som datorer och nätverk

”Konfidentialitet”

Definition enligt svensk standard

- **konfidentialitet** *(confidentiality)*
  skyddsmål att innehållet i ett **informationsobjekt** inte får göras tillgängligt eller avslöjas för obehöriga
  (kan kallas sekretess i legala sammanhang)

”Riktighet”

Definition enligt svensk standard

- **riktighet** *(integrity)*
  skyddsmål att informationen inte förändras, vare sig obehörigen, av misstag eller på grund av funktionsstörning

”Tillgänglighet”

Definition enligt svensk standard

- **tillgänglighet** *(availability)*
  skyddsmål där informationstillgångar skall kunna utnyttjas i förväntad utsträckning och inom önskad tid

”Ansvarighet” och ”oavvislighet”

Definitioner enligt svensk standard

- **ansvarighet**
  princip innebärande att en individ givits och påtagit sig visst ansvar och att därvid denne i efterhand kan ställas till svars för sitt handlande
- **oavvislighet**
  skyddsmål att en handling inte i efterhand ska kunna förnekas av utföraren

”Spårbarhet”

Definition enligt svensk standard

- **spårbarhet**
  möjlighet att entydigt kunna härleda utförda aktiviteter i systemet till en identifierad användare
- kräver identifiering och autenticering av användare samt loggning av relevanta händelser i IT-systemet

Hotläget

- Vilka är de största hoten mot informationssäkerheten idag?
- Varför?

- Diskutera!
  3 minuter i grupper om 3 personer

Dagsläget

Några heta områden

- Phishing och social ingenjörskonst
- Bankkonton och betalsystem
- Attacker mot webbaserade styrsystem (s.k. SCADA-system och Stuxnet)
- DOS- och DDOS-attacker mot webb
- Attacker via datorlika telefoner

- ... alltid där det finns pengar att hämta...

Interna och externa hot

Interna

- oavsiktliga fel på grund av **misstag**
- avsiktliga fel av **missnöjd person**

Externa hot

- attacker via **webben,** skräppost, ”Nigeria-brev”, nätfiske
- Obehöriga användare

Hot, risk och riskvillighet

Definitioner enligt svensk standard

- **hot**
  möjlig, oönskad händelse med negativa konsekvenser för verksamheten
- **risk**
  kombination av sannolikheten för att ett givet **hot** realiseras och därmed uppkommande skadekostnad
- **riskvillighet (-aptit)**
  beredskap att ta vissa, större risker balanserade mot förväntade vinstmöjligheter

Riskanalys

- Ur verksamhetsperspektiv (QoS)
- med avseende på informationstillgångar
- i verksamhetskritiska system