En oversikt over forskjellige aspekter ved sikkerhetspolicyer

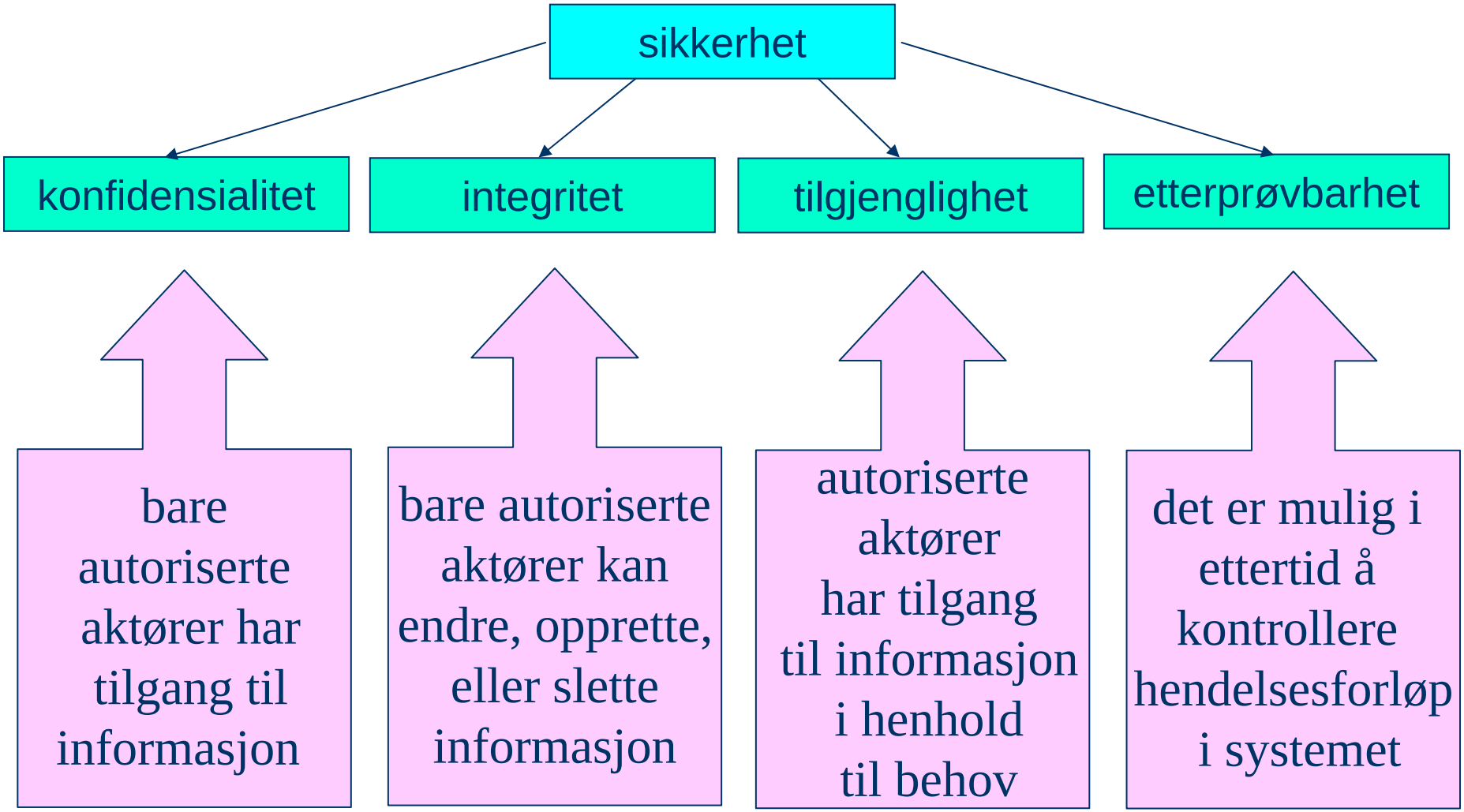
Ketil Stølen
Sjefsforsker/Professor II

SINTEF/UiO
Oslo 23. mars 2006

Innhold

- Hva mener vi med sikkerhet?
- Hva er en policy?
- Policyer versus risikoanalyse
- Policyer versus standarder
- Policyer versus kravspesifikasjoner
- Policyer versus retningslinjer
- Overordnet struktur for en policy
- Organisering av seminaret, samt to formularer

Hva er sikkerhet?



Hva er en policy?

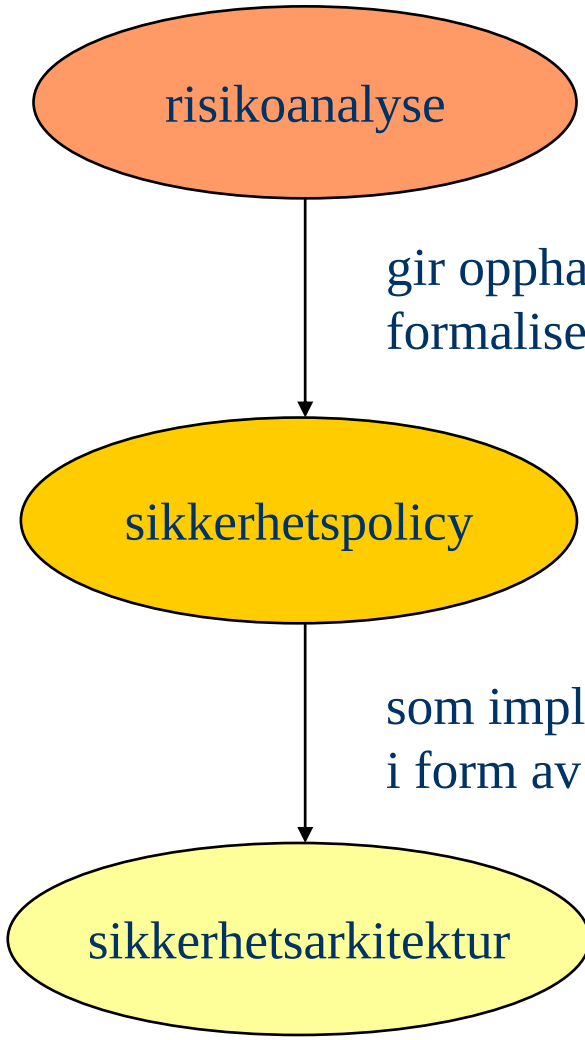
- En policy er typisk et dokument som beskriver spesifikke krav eller regler som må tilfredsstilles

- Håndbok i Informasjonssikkerhet (http://helmersol.nr.no/haandbok/):
  - En sikkerhetspolicy definerer sikkerheten i en virksomhet. Alle generelle overordnede regler for håndtering av informasjon skal nedfestes i et policydokument
  - En sikkerhetspolicy uttrykker hva og ikke hvordan

Policyer versus risikoanalyse

Sikkerhetspolicy = regler, krav og føringer på hvordan aktiva - inkludert sensitiv informasjon - håndteres, beskyttes og distribueres innen en organisasjon og dets IT systemer

Sikkerhetsarkitektur = grovskisse av hvordan sikkerheten i en organisasjon ivaretas rent teknisk



MEN, DETTE ER EN FORENKLING !!!!!

Ulike typer standarder

- Formell standard
  - US: akkreditert av American National Standards Institute (ANSI)
  - Norge: akkreditert av en av de norske standardiseringsorganisasjonene
    - Standard Norge
    - Norsk Elektroteknisk Komite (NEK)
    - Post og Teletilsynet (PT)
- Åpen standard – EU har fremsatt 4 minimumskrav:
  - ikke-kommersiell, fra dokumentasjonen, ingen royalty, fri gjenbruk
  - Eksempel: html som vedlikeholdes av W3C
- De facto standard
  - Standard fordi så mange bruker formatet
  - Eksempel: filformatet MS Word Doc

Policyer versus standarder

- En standard er et dokument som beskriver viktige deler av et produkt, en tjeneste eller en arbeidsprosess
- Standarder gir for eksempel løsninger på hvordan produkter bør fremstilles og hvordan systemer bør beskrives

- Standarder er typisk mer generelle, og har et bredere domene enn policyer

Policyer versus kravspesifikasjoner

- En kravspesifikasjon beskriver krav til et systems funksjonalitet, kvalitet etc.
- En policy beskriver krav til hvordan systemet skal konfigureres, og hvordan det skal brukes
- En policy implementeres på toppen av den vanlige funksjonaliteten
- Det er implisitt at det som begrenses av policyen har potensial til å bryte med den

Policyer versus retningslinjer

- En retningslinje er typisk en samling av systemspesifikke forslag til ”best praksis”
- En retningslinje er ikke et krav (som hører hjemme i en policy) men mer en sterk anbefaling

Struktur for et policydokument

1. Hensikt – formålet med policyen
2. Domene – avgrensning av dens gyldighetsområde
3. Policy – selve policybeskrivelsen
4. Håndhevelse – konsekvensen ved ikke å følge den
5. Definisjoner – viktig å definere sentrale begreper
6. Revisjonshistorie – en policy endrer seg over tid, og dette må dokumenteres

Policy for dette seminaret

- Hver foredragsholder har 20 minutter til rådighet
- Jeg reiser meg når det gjenstår 3 minutter
- Spørsmål stilles etter hvert foredrag
- Det er satt av 5 minutter til spørsmål og svar for hvert foredrag

To skjemaer vi gjerne ser at dere fyller ut

- Seminarevaluering
  - Hjelper oss å bli bedre
- Spørreundersøkelse
  - Bidrag til forskning
  - Del av Jenny Hougens hovedoppgave