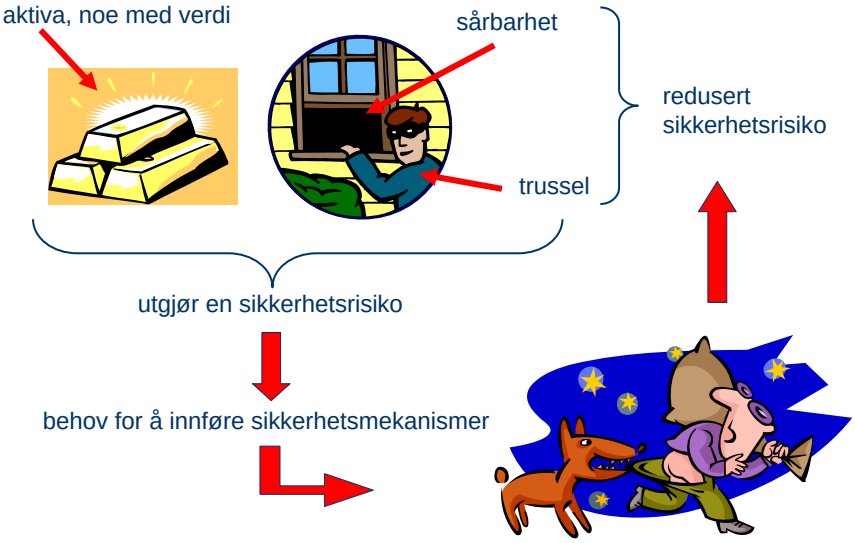
Hvordan analysere personvernsrisiko

Seminar om rike medier, brukervennlighet og personvern

12/6-08

Heidi E. I. Dahl
SINTEF

Sentrale begreper



Hvorfor CORAS?

Personvern er en tverrfaglig utfordring:

- Beslutningstakere
- Jurister
- Programmerere
- Drift
- Brukere

- ✓ Vi er avhengig av god kommunikasjon
- ✓ Deltakerne i analysen trenger en felles forståelse av problemstillingene som analyseres
- ✓ Resultatene må være lett tilgjengelige for en som ikke har deltatt i analysen

CORAS

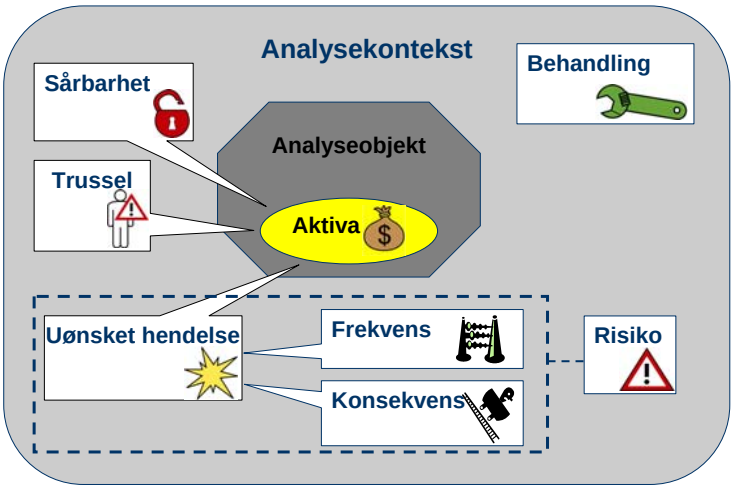
CORAS-diagrammene

- Er laget for å dokumentere, analysere og kommunisere informasjon om sikkerhetsrisikoer
- Er lette å lese
- Bruker intuitive ikoner

CORAS

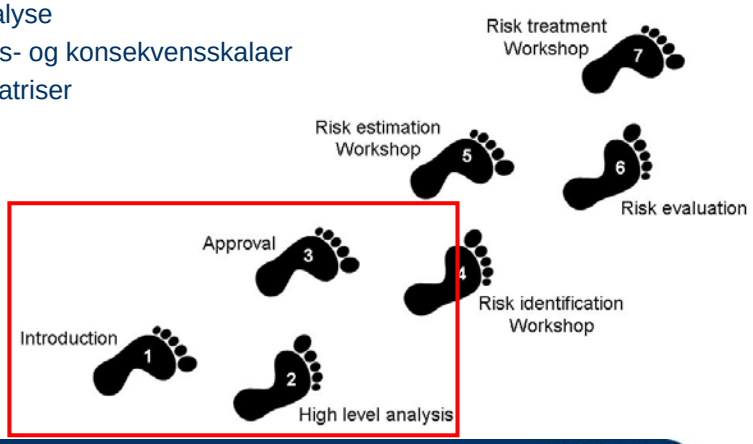
- Utviklet gjennom empiriske undersøkelser og en serie av industrielle feltstudier (prosjekter finansiert av EU og Forskningsrådet)
- Basert på internasjonale standarder for risikohåndtering (bl.a. AS/NZS 4360:2004)

Analyseprosessen

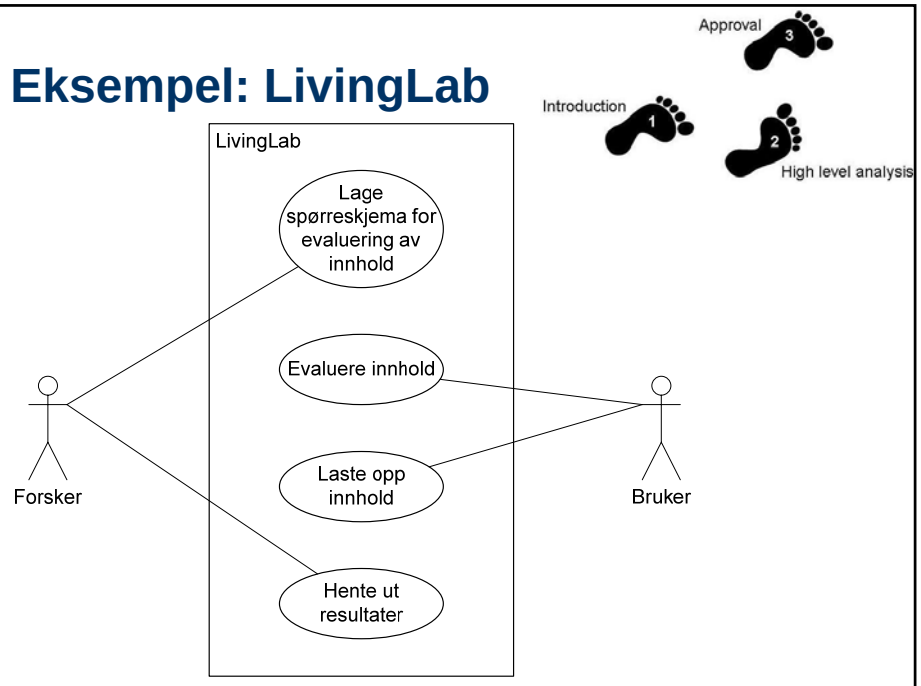


Innledende møter

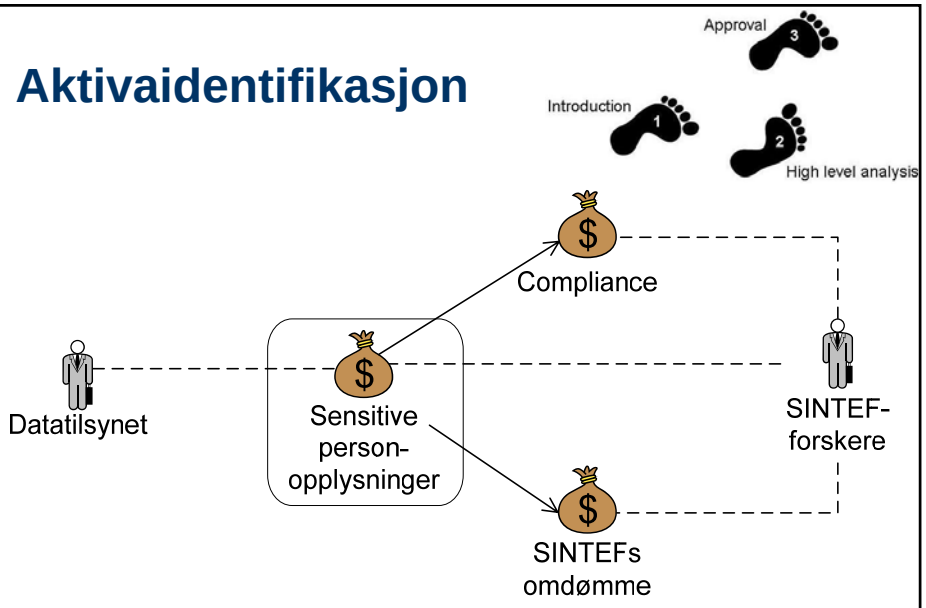
- Systembeskrivelse
- Aktivadiagrammer
- Grovanalyse
- Frekvens- og konsekvensskalaer
- Risikomatriser



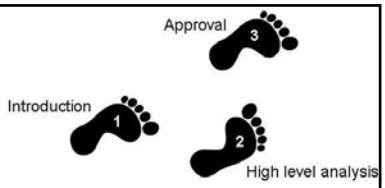
Eksempel: LivingLab



Aktivaidentifikasjon



Sannsynligheter og konsekvenser



Sannsynlighet	
1	sjelden
2	av og til
3	jevnlig
4	ofte

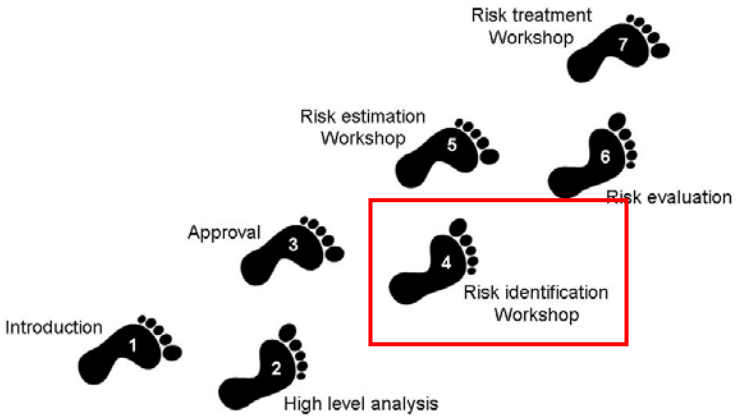
Konsekvens (Sensitive personopplysninger)	
1	ufarlig
2	moderat
3	alvorlig
4	katastrofalt

Risikomatrise (Sensitive personopplysninger)

k \ s	sjelden	av og til	jevnlig	ofte
ufarlig				
moderat				
alvorlig				
katastrofalt				

Risikoidentifikasjon

→ Trusseldiagrammer



Hva er truslene?

4 Risk identification Workshop


Hacker


Forsker


Bruker


Sensitive person-opplysninger

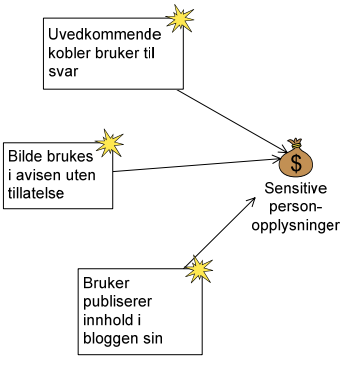
Hva er vi redde skal skje?

4 Risk identification Workshop


Hacker

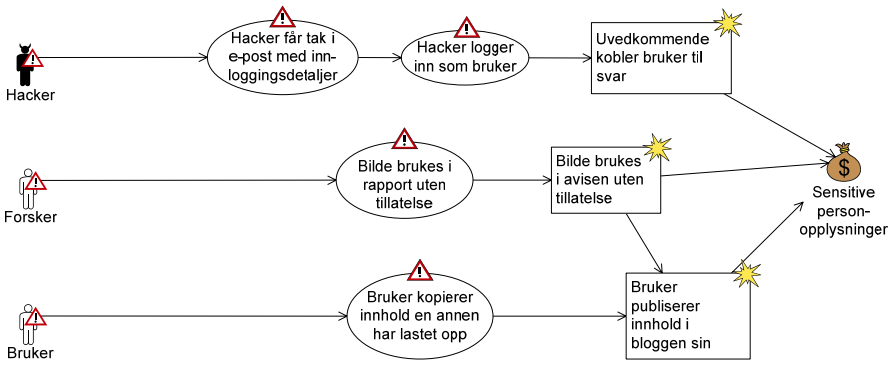

Forsker


Bruker



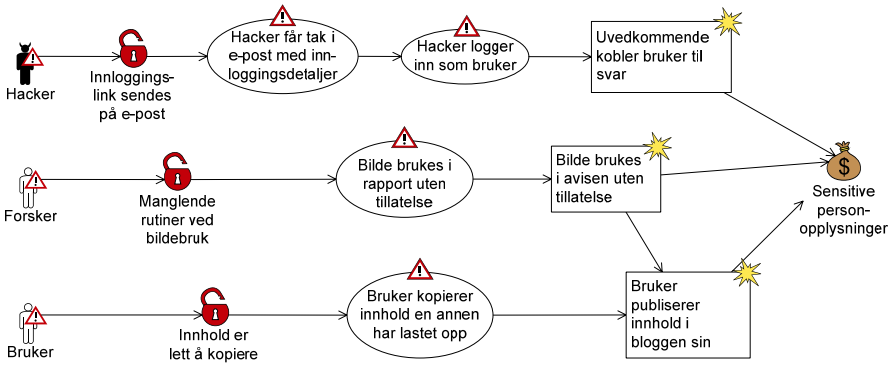
Hvordan skjer det?

4 Risk identification Workshop



Hvilke sårbarheter gjør det mulig?

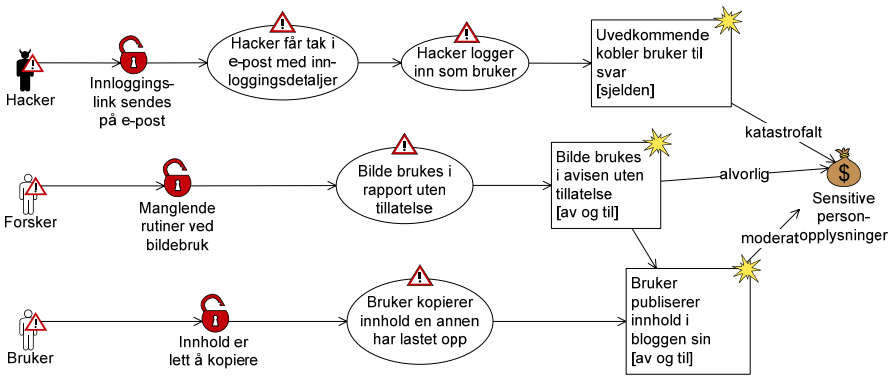
4 Risk identification Workshop



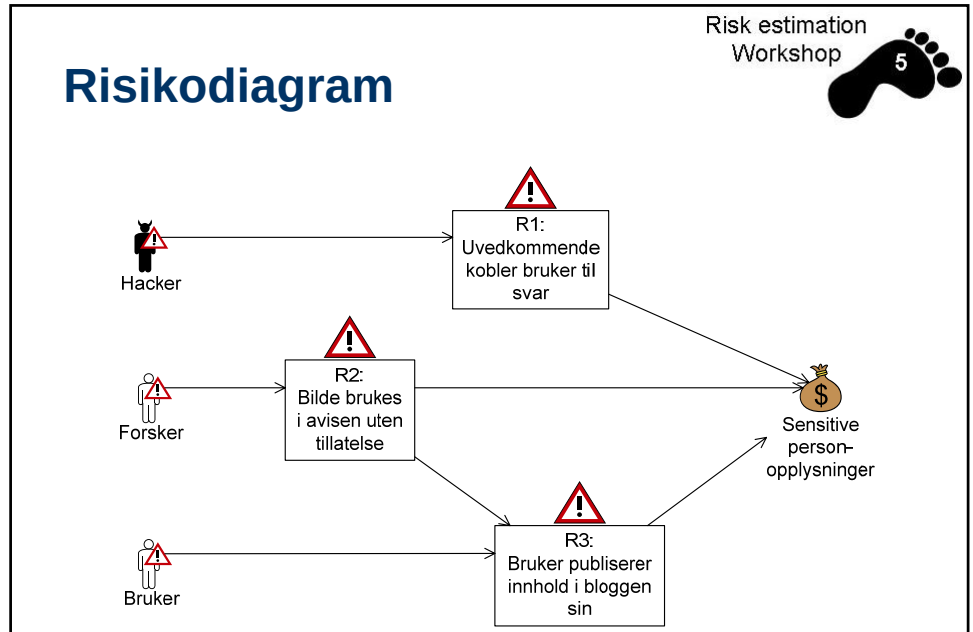
Risikoestimering

- Trusseldiagrammer med sannsynlighets- og konsekvensestimeringer
- Risikodiagrammer

Risikoestimering

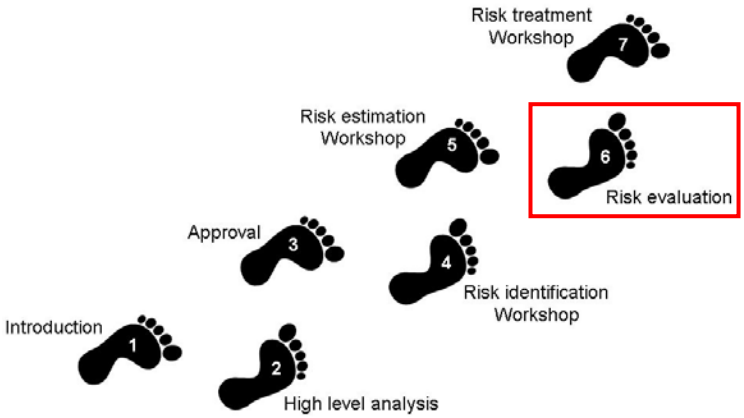


Risikodiagram



Risikoevaluering

→ Risikomatriser



Er risikoene akseptable?

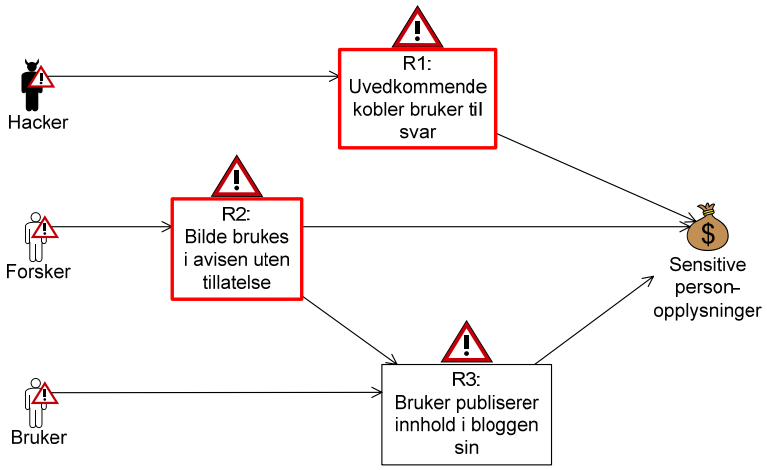
Risk evaluation

Risikomatrise
(Sensitive personopplysninger)

k \ s	sjelden	av og til	jevnlig	ofte
ufarlig				
moderat		Bruker publiserer innhold i bloggen sin		
alvorlig		Bilde brukes i avisen uten tillatelse		
katastrofalt	Uvedkommende kobler bruker til svar			

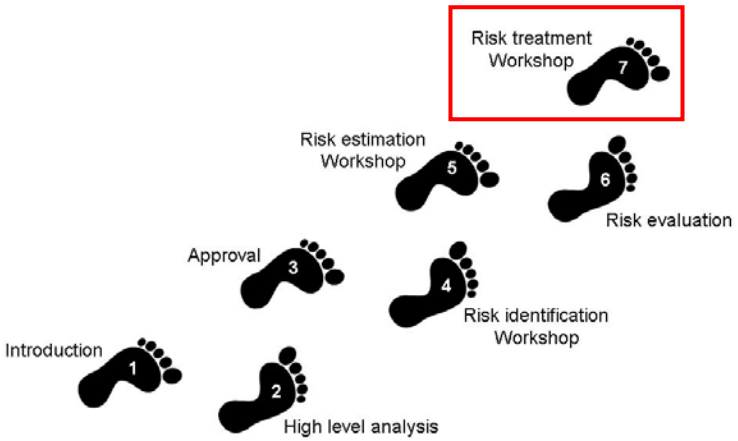
Risikodiagram

Risk evaluation



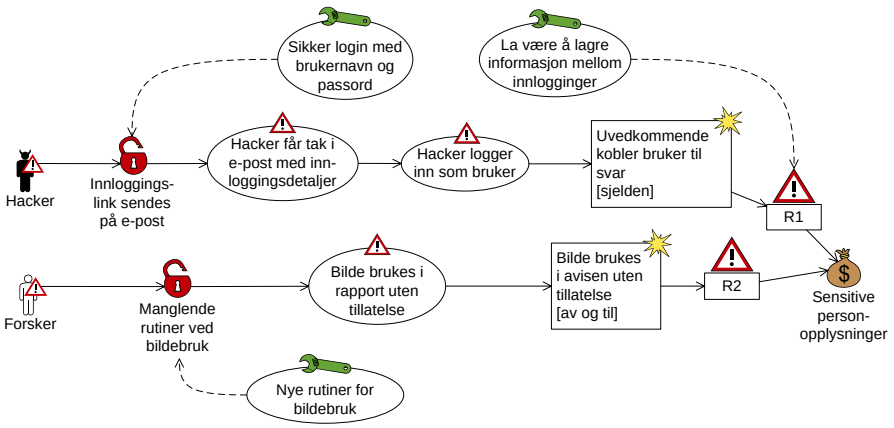
Risikobehandling

→ Tiltak mot uakseptable risikoer



Hva kan vi gjøre for å få risikoene ned på et akseptabelt nivå?

Risk treatment Workshop 7



Konklusjon

Vi har

- Gitt en kort innføring i sikkerhetsanalysebegreper og gangen i en analyse
- Beskrevet hvordan dette gjøres i CORAS
- Gitt et eksempel på hvordan CORAS kan brukes for å analysere personvernsrisiko i rike medier

Spørsmål?

Heidi E. I. Dahl
heidi.dahl@sintef.no