NTNU

Risikoanalyse: Teori og metoder, 2. utgave

Kapittel 20
Sikringsrisikoanalyse

Ingrid Bouwer Utne og Marvin Rausand
ingrid.b.utne@ntnu.no

Oversikt – kapittel 20

- Innledning
- Viktige begreper
- Metodebeskrivelse
  - IKT sikring
  - Fysisk sikring
  - Cyberfysisk sikring
  - Sikring av personopplysning
  - Andre metoder

Innledning

- Virksomhetene og samfunnet som heilhet blir stadig mer digitalisert.
- Angrep over datanettverk – som vi kaller cyberangrep – er i dag en mye større trussel mot de fleste virksomhetene enn kriminelle fysiske handlinger.
- Risiko med utgangspunkt i tilsikta uønska handlinger kaller vi sikringsrisiko.

Sikringsrisiko

Sikringsrisiko kan defineres som*:

- Et uttrykk for forholdet mellom trusselen mot et gitt verdiobjekt og dette objektets sårbarhet overfor den spesifiserte trusselen.

*NS5832 Samfunnssikkerhet - Beskyttelse mot tilsiktede uønskede handlinger - Krav til sikringsrisikoanalyse.

Verdivurdering og verdiobjekt

- **Verdivurdering**:
  - Som underlag for enhver sikringsrisikoanalyse bør virksomheten avgjøre hvilke verdiobjekt som har slik verdi at de skal og må beskyttes.
  - Når verdien skal bestemmes, bør du ta utgangspunkt i den skaden på objektet som gir størst tap.
  - Verdien kan f.eks. klassifiseres som «svært lav», «lav», «moderat», «høg» og «svært høg» verdi.
- **Skjermingsverdige verdiobjekt**:
  - Sikkerhetsloven skiller mellom «vanlige» verdiobjekt og «skjermingsverdige».
    - Tekniske objekt, infrastruktur og informasjonssystem, samt informasjon er skjermingsverdige når grunnleggende nasjonale funksjoner eller sikkerhetsinteresser kan bli skadet.

Informasjonssikkerhet

- Informasjon som bør sikres, finnes i så godt som alle virksomheter:
  - Dette kan dreie seg om virksomhetens arbeidsprosesser, regnskap og opplysninger om ansatte og kunder.
- Informasjonssikkerhet handler om å sikre informasjonens:
  - Konfidensialitet – å sikre at det kun er autoriserte brukere som får tilgang til informasjonen.
  - Integritet – å sikre at informasjonen er fullstendig, nøyaktig og gyldig.
  - Tilgjengelighet – å sikre at informasjonen er tilgjengelig for autoriserte brukere når de har behov for tilgang.

Alle statlige organ er ifølge eForvaltningsforskrifta § 15 pålagt å ha internkontroll på informasjonssikkerhetsområdet.

Trusler

- Fysiske trusler:

Brannstifting	Ran eller overfall
Sabotasje	Bruk av droner til
Spionasje	rekognosering, etterretning
Terrorisme	eller skadeverk
Tjuveri	Andre kriminelle handlinger
Kapring	

- IKT trusler:
  - Lokale trusler
  - Nettverkstrusler
  - Servertrusler

- Blir noen ganger utvida til å inkludere farekilder som:
  - Menneskelige feilhandlinger
  - Tekniske svikt
  - Ikke-tilfredsstillende design
  - Naturhendelser

Trusselaktør

En trusselaktør kan defineres som*:

- Personer, forbund eller fremmed makt som tar sikte på å gjennomføre sikkerhetstruende virksomhet.

Målet for trusselaktøren kan bl.a. være å

- Oppnå økonomisk og/eller politisk vinning
- Skade datamaskiner og/eller nettverk, tekniske system, en virksomhet eller en organisasjon
- Samle fortrolig informasjon
- Skade forsvaret til et land
- Skape frykt ved å spre trusler om vold
- Få tilgang til personopplysninger
- Trakassere enkeltpersoner og grupper og m.fl.

*Nasjonal SIkkerhetsmyndighet

Trusselaktør (ii)

For å utføre et vellykka angrep må trusselaktøren ha:

- Intensjon – som betyr at han både har til hensikt og vilje til å utføre et angrep.
- Kapasitet – som betyr at han har kunnskap, ferdighet og ressurser til å utføre et angrep.

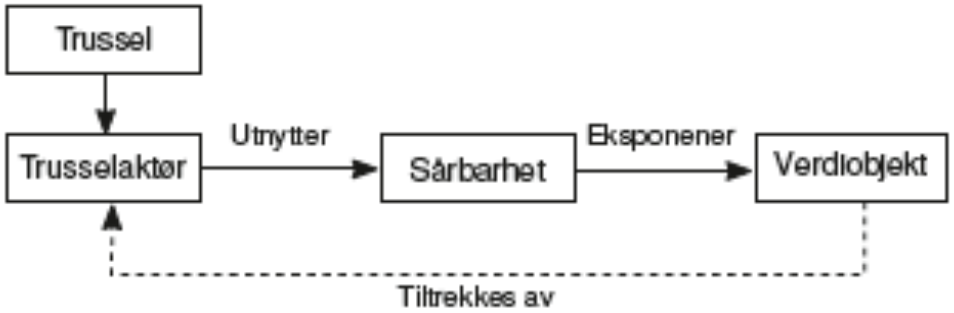
Det som er viktig å vite om trusselaktøren er:

- Hvilken kompetanse og hvilke ressurser har trusselaktøren?
- Hvordan vil trusselaktøren skaffe seg tilgang til verdiobjektene?
- Hvordan vil trusselaktøren gjennomføre angrepet?

Sårbarhet

- Sårbarhet kan defineres som*:
  - Et uttrykk for de problemene et system vil få med å fungere når det utsettes for en uønska hendelse, samt de problemene systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet.

- Sammenhengen mellom verdiobjekt, trussel og sårbarhet kan framstilles som:



*NOU 2000:24 Et sårbart samfunn

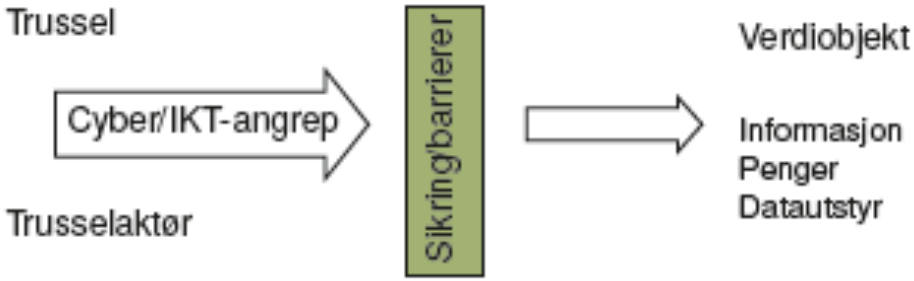
Sikringstiltak

- Vi kan skille mellom tre typer sikringstiltak eller barrierer:
  - Teknologiske tiltak
  - Organisatoriske tiltak
  - Menneskelige tiltak
- Prinsipper for IKT-sikkerhet* grupperes i:
  - Identifisere og kartlegge – å opparbeide og forvalte forståelse om virksomheten.
  - Beskytte – å ivareta en forsvarlig sikring av IKT-miljøet.
  - Opprettholde og oppdage – å opprettholde den sikre tilstanden over tid og ved endringer.
  - Handtere og gjenopprette – som omfatter å handtere sikkerhetstruende hendelser effektivt.

*Nasjonal Sikkerhetsmyndighet

Analysemetode – IKT sikring

- Metoden for sikringsrisikoanalyse som beskrives her, har utgangspunkt i standarden NS 5832 og trefaktormodellen.



- Analysemetoden utføres i ni trinn:

Trinn 0 og 8 (forberedelse og rapportering) er omtalt i kap. 8 og 20.

1. Verdivurdering

Hensikten her er å identifisere de verdiobjektene som – hvis de blir angrepet – kan føre til store konsekvenser for virksomheten. Trinnet forutsetter at du må:

- Lage en oversikt over de verdiobjektene virksomheten har som krever en videre vurdering med hensyn på store konsekvenser.
- Vurdere verdien av hvert enkelt av de utvalgte verdiobjektene med hensyn på konsekvenser.
- Vurdere hvilken verdi hvert av de utvalgte verdiobjektene kan tenkes å ha for en aktuell trusselaktør.

Id.	Verdiobjekt (beskrivelse)	Verdivurdering	
		For virksomheten	For trusselaktør

Hva – hvis analyse

- Når du skal anslå verdien av de ulike verdiobjektene, kan det være nyttig å gjøre en enkel hva-hvis-analyse.
- Eksempler på «hva-hvis»-spørsmål kan være:
  - Hva-hvis kundedatabasen blir gjort ubrukelig?
  - Hva-hvis tilgangen til internett faller ut?
  - Hva-hvis elektrisk kraftforsyning faller ut?
  - Hva-hvis virksomhetens lokaler blir utilgjengelige?
  - Hva-hvis tilgangen til datasystemet blokkeres av et løsepengevirus-angrep?

2. Fastsetting av sikringsmål

- Sikringsmål kan defineres som:
  - Et mål for hva som er ønska eller aksepterbar tilstand for et verdiobjekt under eller etter et IKT-angrep.
- Virksomheten må sjøl bestemme hva som aksepteres av skade på, bortfall av, eller kompromittering av hvert verdiobjekt.
  - Vurderingen gjøres på grunnlag av vurderingen av verdier og konsekvenser i trinn 1 og bør i størst mulig grad baseres på ALARP-prinsippet

3. Trusselvurdering

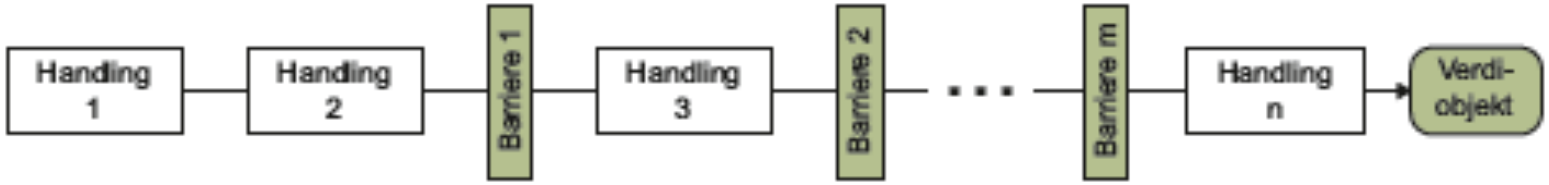
Når verdiobjektene er avdekka og rangert, må du vurdere hva som kan true de enkelte verdiobjektene. Trusselvurderingen skal avdekke:

- Hvilke (generiske) trusler som kan være aktuelle.
- Hvilke trusselaktører som kan tenkes å utnytte hver enkelt av truslene.
- Hvilken intensjon og kapasitet hver trusselaktør har til å angripe de ulike verdiobjektene.
- Hvor alvorlig en gitt kombinasjon av trussel og trusselaktør oppfattes å være.

Nr.	Verdiobjekt	Trussel 1	Trussel 2	Trussel 3	...	Trussel n
1			x			
2		x				x
3						x
4		x		x		
m				x		

4. Utvikling og valg av angrepsscenario

- Dette trinnet identifiserer ulike måter trusselaktøren kan tenkes å gå fram på for å få tilgang til et verdiobjekt i virksomheten.
  - En bestemt følge av handlinger som leder til målet, kalles en angrepsvektor eller et angrepsscenario.
    - I mange tilfelle kan det være nyttig å samle angrepsscenarioene i et angrepstre.
  - I hvilken grad trusselaktøren vil lykkes med et angrep, avhenger av om det er effektive sikringstiltak eller barrierer som kan stoppe ham.



5. Identifikasjon og beskrivelse av sårbarheter

- Hensikten her er å finne slike sårbarheter som gjør at trusselaktøren kan få tilgang til verdiobjekt.
  - Angrepsscenarioene fra trinn 4 viser hvordan trusselaktøren kan tenkes å gå fram for å nå målet sitt.
  - Oppgava nå er å gå nøye gjennom hvert enkelt angrepsscenario og sjekke om virksomheten har gode nok barrierer for å stoppe et angrep som beskrevet i angrepsscenarioet.
  - Når du skal avdekke sårbarheter, er det nyttig å ha tilgang til ei generisk liste over sårbarheter, og det er også utvikla flere metoder for sårbarhetsanalyse som FMVEA.
  - Det er viktig å beskrive usikkerheten i vurderingene.

6. Beskrivelse av risikobildet

I dette trinnet skal du sammenstille du resultatene du fant i trinnene 1–5. Du kan, for eksempel, bruke det skjemaet som er vist her:

Nr.	Angrepsscenario:	Verdi-objekt	Trussel + aktør	Sårbar-het	Del-risiko
1 2 3					

Konsekvensen som kan forårsakes av et angrepsscenario, kan vurderes i følgende typer:

- Skade på personell (vanligvis ikke aktuelt for IKT-sikring).
- Lang nedetid og langvarig redusert drift.
- Økonomisk tap, tap av omdømme og effekt på virksomhetens verdi (aksjekurs).

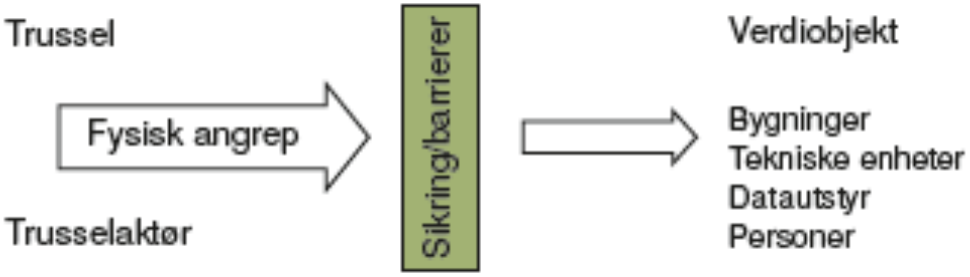
7. Tiltak for å redusere risikoen

- Risikobildet fra trinn 6 må vurderes opp mot de sikringsmålene som ble fastsatt i trinn 2.
- De scenarioene som ikke oppfyller sikringsmålene, må du vurdere grundig og fremme forslag til tiltak som gjør at scenarioene møter sikringsmålene.
- Viktige spørsmål*:
  - I hvor stor grad er virksomheten villig til å akseptere den risikoen som er avdekka?
  - Hvor stor mulighet er det for risikoreduksjon?
  - Hvilke tiltak kan redusere risikoen til et (mer) aksepterbart nivå?
  - Er disse tiltakene forsvarlige ut fra en kostnad/nytte-vurdering samt andre effekter av tiltaket?

*Fra DSB.

Fysisk sikring

- Fysisk sikring skal hindre at uvedkommende får fysisk tilgang til analyseobjektet.
- Når du foretar en risikovurdering av fysisk sikring, kan du følge de samme trinnene som for IKT-sikring og bruke de metodene som er beskrevet i boka.
- Hovedelementene i et fysisk angrep:



Fysisk sikring - trusler

- Viktige trusler er tjuveri, brannstifting, sabotasje, spionasje, terrorisme samt generelt skadeverk.
- Hvis det oppfattes som aktuelt, kan du også ta med naturhendelser (som flom, jordskjelv og lynnedslag), menneskelige feilhandlinger og infrastruktur-feil som trusler.
- Trusselaktøren – eller utstyr han bruker – må være i eller nær analyseobjektet for å foreta et angrep.
  - Eksempler på bruk av slikt utstyr er å plassere et kjøretøy fullt av sprengstoff nær analyseobjektet, bruk av drone til spionasje eller for å slippe ei bombe.

Fysisk sikring - sikringstiltak

Aktuelle tiltak for fysisk sikring omfatter bl.a.:

- Automatisk låsing av dører inn til analyseobjektet
- Adgangskontroll (nøkkelkort med kode e.l.)
- Alarmsystem med video-overvåkning
- Belysning
- Vakthold, gjerder og stengsler
- Brannvarsling og slukkeutstyr
- Rydding nær bygningen der analyseobjektet er plassert
  - Fjerne alt brennbart materiale som kan «friste» en pyroman
  - Fjerne stiger o.l. som kan brukes til å klatre opp til vindu og eventuelle balkonger
  - Fjerne objekt der en trusselaktør kan gjømme seg
- Kontroll og klare rutiner for innslipp av eksterne personer

Cyber-fysisk sikring

Det blir stadig mer vanlig å kople fysiske enheter, som maskiner, roboter o.l., til et cybernettverk.

- Den viktigste standarden for slike system er NEK IEC 62443-serien «Industrial communication networks – IT security for networks and systems».
- NEK IEC 62443 definerer begrepet «security» (dvs. sikring) som:
  - Forebygging av (i) ulovlig eller uønska inntrengning, (ii) forsettlig eller utilsikta inngrep på normal og tiltenkt drift, eller (iii) utilsikta tilgang til konfidensiell informasjon.
- Sikring gjelder datamaskiner, nettverk, operativsystem, applikasjoner og andre programmerbare konfigurerbare komponenter i systemet.

Sikring av personopplysninger

- Regelverket for beskyttelse av personvern forvaltes av Datatilsynet.
- Med personvern meines retten til privatliv og retten til å bestemme over egne personopplysninger.
- EU-forordningen GDPR «General Data Protection Regulation» ble innarbeidd i norske lover fra 2018.
- Du finner en god veiledning til hvordan du skal gjennomføre en risikovurdering av personopplysninger på Datatilsynets nettsider.

Andre metoder

Det er utvikla ei rekke metoder som sikringsrisikoanalyse i ulike land f.eks:

- Threat, vulnerability risk analysis» (TVRA) er utvikla for ETSI og er retta mot sikringsrisikoanalyse av IKT-system.
- NIST utgir standarder/veiledninger for bl.a. sikringsrisiko.
- Etter 11. sept. 2001 utvikla ASME en metode kalt RAMCAP for å vurdere hvordan USAs infrastruktur kunne beskyttes mot terroraksjoner.
- OCTAVE er en metode for sikringsrisikoanalyse av informasjonutvikla ved Carnegie-Mellon universitetet.
- FEMA har utviklet «Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings».