Objekt- og informasjonssikkerhet

Metode for risiko- og sårbarhetsanalyse

ROSS

Risiko- og sårbarhetsstudier ved NTNU

Metodikken er utformet på oppdrag fra Nasjonal sikkerhetsmyndighet

Institutt for produksjons- og kvalitetsteknikk

Adresse: N-7491 Trondheim
Besøksadresse: S.P. Andersensvei 5
Telefon: +47 73 59 38 00
Telefaks: +47 73 59 71 17

TITTEL

OBJEKT- OG INFORMASJONSSIKKERHET
METODE FOR RISIKO- OG SÅRBARHETSANALYSE

FORFATTERE

Einar Skavland Idsø og Øyvind Mejdell Jakobsen

SAMMENDRAG

Rapporten presenterer en metode for analyse av objekt- og informasjonssikkerhet. Metoden er en skjemabasert risiko- og sårbarhetsanalyse (ROS-analyse) rettet mot fagfeltet security. Analysen inkluderer kartlegging av skjermingsverdige objekter, trusler, utførende aktører og handlingsmønstre. Systemets sårbarhet blir vurdert, samt eksisterende sikringstiltak. Risiko vurderes på grunnlag av sannsynligheten for, og konsekvensen av de forskjellige handlingsmønstrene. Et eget eksempel illustrerer de ulike arbeidstrinnene og utfyllingen av metodens skjemaer. Rapporten inkluderer i tillegg et sett med sentrale begreper og definisjoner som brukes innenfor ROS-analyse og security.

ARKIVNØKKEL	RAPPORT NR.
1937.2000	ROSS (NTNU) 200027
ISBN	DATO
82-7706-160-9	2000-12-20
SIGNATUR	SIDER/APPEND.
Marvin Rausand (sign)	95
NØKKELORD NORSK	NØKKELORD ENGELSK
SÅRBARHET RISIKO ANALYSE SIKRING METODIKK	VULNERABILITY RISK ANALYSIS SECURITY METHOD

Forord

Denne rapporten er utarbeidet i forbindelse med et samarbeidsprosjekt mellom Sikkerhetsstaben i Forsvarets overkommando (FO/S), Norges teknisk-naturvitenskapelige universitet (NTNU) og Direktoratet for sivilt beredskap (DSB). Arbeidet er utført ved Institutt for produksjons- og kvalitetsteknikk (IPK) ved NTNU, med professor Marvin Rausand som faglig ansvarlig.

Bakgrunnen for prosjektet er et arbeid FO/S startet på grunnlag av sine behov innenfor fagområdet security med fokus på risikohåndtering. I løpet av 1999 utarbeidet sivilingeniør Vidar Evensen, IPK, et forslag til en metode for vurdering av informasjonssikkerhet og objektsikkerhet med fokus på security. Etter ønske fra FO/S, DSB og IPK har dette arbeidet blitt videreutviklet, og det presenteres nå en fullstendig metodikk for risiko- og sårbarhetsanalyse med fokus på security. Denne utgivelsen erstatter den tidligere rapporten med samme navn (Idsø og Jakobsen, 2000).

Rapporten anses som en omfattende dokumentasjon av den nevnte analysemetoden. Som en første introduksjon vil imidlertid en kortere veileder bli utarbeidet av DSB. Rapporten er derfor ment som utfyllende bakgrunnsdokumentasjon til en slik veileder.

Arbeidet har inkludert evalueringer i samarbeid med FO/S, DSB, SINTEF avdeling for sikkerhet og pålitelighet og IPK. Metoden ble også presentert for sikkerhetspersonell ved KNM Tordenskjold ved Haakonsvern orlogsstasjon. Vi ønsker å rette en takk til disse for nyttige diskusjoner og konstruktive kommentarer. Spesielt har vi dradd nytte av en praktisk utprøving av metoden på Forsvarets hovedarsenal på Lillehammer.

Under arbeidet har det vært jevnlig kontakt med FO/S representert ved seniorkonsulent Hans Morten Synstnes og kommandør Tor Arne Moe. Vi takker for nyttige forslag og synspunkter.

Vi vil også få takke professor Marvin Rausand som har fungert som faglig veileder og spilt en essensiell rolle under alle fasene i arbeidet.

Trondheim, 20. desember 2000

Einar Skavland Idsø Øyvind Mejdell Jakobsen

Sammendrag

Rapporten presenterer en metode for analyse av objekt- og informasjonssikkerhet. Dette er en risiko- og sårbarhetsanalyse rettet mot fagfeltet security. Analysen konsentrerer seg om planlagte handlinger som blir utført med overlegg, dvs. såkalte tilsiktede handlinger. Tilfeldige hendelser omfattes ikke av analysen.

Metoden er delt inn i separate trinn og drives fram av utfyllingen av fire skjemaer. Metoden starter etter en organiserings- og planleggingsfase, med kartlegging av skjermingsverdige objekter, det vil si objekter som virksomheten ønsker å beskytte (inkludert informasjonsobjekter). Deretter identifiseres potensielle trusler som kan ramme objektene. Hvem som kan realisere disse truslene og hvordan de kan gjøre det, blir evaluert, og systemets sårbarhet blir vurdert. For hvert av handlingsmønstrene identifiseres eksisterende sikringstiltak, både forebyggende tiltak og skadereduserende og normaliserende tiltak. Risikoen knyttet til hendelsene vurderes på grunnlag av sannsynligheten for, og konsekvensene av de uønskede hendelsene. Til slutt blir rapportering av analyseresultatene gjennomgått.

Metodens skjemaer blir forklart og de forskjellige arbeidstrinnene blir gjennomgått. Et eget, gjennomgående eksempel illustrerer de ulike arbeidstrinnene og utfyllingen av metodens skjemaer.

Risiko- og sårbarhetsforskningen inneholder et mangfold av ord og begreper, og uklarhet i hva som menes med de ulike definisjonene forekommer. Det er derfor utarbeidet et sett med sentrale begreper og definisjoner i rapporten, noe som kan bidra til et mest mulig ensartet begrepsapparat i forbindelse med arbeidet med den presenterte risiko- og sårbarhetsanalysen.

Innholdsfortegnelse

Forord ..... **iii**
Sammendrag ..... **v**
Innholdsfortegnelse **1**
1 Innledning **3**
1.1 Bakgrunn 3
1.2 Tidligere arbeid 3
1.3 Introduksjon til ROS-analyse og security 6
1.4 Hvorfor utføre en risiko- og sårbarhetsanalyse? 10
1.5 Målsettinger for arbeidet med analysemetoden 10
1.6 Begrensninger 11
2 Presentasjon av metoden **13**
2.1 Begrepsavklaring 13
2.2 Generelt 14
2.3 Analysens struktur 16
2.4 Oppstartsfasen: Organisering og planlegging 18
2.4.1 Organisering av arbeidet 18
2.4.2 Planlegging av analysen 19
2.5 Utfylling av skjema "Beskrivelse av objekt" (O-skjema) 24
2.5.1 Beskrivelse av skjermingsverdige objekter 26
2.6 Utfylling av skjema "Identifikasjon av trusselbilde" (T-skjema) 28
2.6.1 Identifikasjon av potensielle trusler 29
2.6.2 Identifikasjon av utførende aktører 32
2.6.3 Identifikasjon av handlingsmønstre 33
2.6.4 Vurdering av sårbarhet 33
2.7 Utfylling av skjema "Analyse av sikringstiltak" (S-skjema) 34
2.7.1 Beskrivelse av uønskede hendelser 35
2.7.2 Kartlegging av eksisterende forebyggende tiltak 36
2.7.3 Kartlegging av skadereduserende og normaliserende tiltak 37
2.8 Utfylling av skjema "Risikovurdering" (R-skjema) 38
2.8.1 Risikovurdering 39
2.9 Rapportering 41
2.9.1 Presentasjonsmetoder 43

3 Brukerveiledning 49
3.1 Beskrivelse av analyseobjektet 49
3.2 Organisering av arbeidet 52
3.3 Planlegging av analyse 53
3.4 Beskrivelse av skjermingsverdige objekter 55
3.5 Identifikasjon av trusselbilde 59
3.5.1 Identifikasjon av potensielle trusler 59
3.5.2 Identifikasjon av utførende aktører 60
3.5.3 Identifikasjon av handlingsmønstre og svakheter 60
3.6 Analyse av sikringstiltak 63
3.7 Vurdering av konsekvens og sannsynlighet 66
3.8 Rapportering 70
4 Konklusjon og anbefalinger 75
Referanser 77
A Sentrale begreper og definisjoner 81
B Systembeskrivelse 83
B.1 IDEF0 83
B.2 Hierarkisk nedbryting 86
C Sikkerhetsgradering av informasjon 89
D Skjemaer 92

1 Innledning

1.1 Bakgrunn

Sikkerhetsforskningen i Norge startet hovedsakelig for 15 til 20 år siden med utspring i analyse og forebyggelse av storulykkerisiko primært knyttet til offshore petroleumsvirksomhet. Selv om Norge fortsatt høster fra denne forskningen, står samfunnet og næringslivet ovenfor endringer og utfordringer som krever ytterligere satsing på sikkerhetsforskningen. Den raske teknologiske utviklingen skaper hele tiden nye muligheter, men gjør samtidig samfunnet mer sårbart. År 2000-problematikken har satt et viktig søkelys på samfunnets avhengighet av informasjonsteknologi, men er imidlertid bare et lite eksempel på samfunnets sårbarhet for svikt i IT-systemer eller annen kritisk infrastruktur. Willoch-utvalgets rapport "Et sårbart samfunn" (Norges offentlige utredninger nr. 24, 2000) har rettet søkelyset mot samfunnets sårbarhet og beredskap, og konkluderer med at utfordringene innenfor dette området er betydelige.

Sårbarheten i samfunnsviktige funksjoner må også sees i sammenheng med trussel-situasjonen, som i dag er helt annerledes enn for bare noen år siden. Et økt internasjonalt engasjement fra Norges side innebærer at vi kan bli mer utsatt for fiendtlige anslag, terrorisme og sabotasje fra enkeltpersoner, grupper, organisasjoner og nasjoner. I tillegg fører økt bruk og avhengighet av informasjonsteknologi og telekommunikasjon til at samfunnet blir mer sårbart. Det er ikke lenger utenkelig at en fiende raskt kan lamme store deler av samfunnet uten at en eneste soldat har krysset den norske grensen. Behovet for å kunne analysere mulighetene for bevisste fiendtlige operasjoner, og samtidig kunne vurdere konsekvensene av disse, er derfor til stede. Også i privat sektor øker behovet for sikring og dermed analyse av sannsynligheter og konsekvenser i forhold til tilsiktede handlinger.

1.2 Tidligere arbeid

I 1983 ble det gjennom kongelig resolusjon satt ned et utvalg som skulle utrede sårbarheten i vårt datateknologi-avhengige samfunn (Norges offentlige utredninger nr. 12, 1986). Utvalget skulle blant annet utrede hvilke samfunnsviktige funksjoner som hadde blitt avhengig av elektronisk databehandling, og hvilke forhold som kunne føre til forstyrrelser og avbrudd i viktige datatjenester. Utvalget kom

fram til en rekke forslag og konklusjoner, blant annet for sikker strømtilførsel og teletjeneste. Oppmerksomheten ble også rettet mot behovet for tiltak mot sabotasje, terrorhandlinger og spionasje, samt undervisning innenfor EDB og EDB-sikkerhet.

Innenfor fagfeltet som omhandler risiko- og sårbarhetsanalyser ga Norges Standardiseringsforbund i 1991 ut Norsk Standard 5814, "Krav til risikoanalyser", som beskriver retningslinjer for planlegging og gjennomføring av risikoanalyser (Norges Standardiseringsforbund, 1991).

Norges forskningsråd (NFR) startet i 1993 et program for risiko- og sårbarhetsforskning innenfor helse, miljø og sikkerhet som fikk navnet ROS-programmet (Programstyret for risiko- og sårbarhetsforskning, 1997). Programmet som pågikk i perioden 1993-97, fokuserte på faren for akutte hendelser som kan medføre skade på mennesker, ytre miljø eller materielle verdier. ROS-programmet ble utarbeidet for å utvikle og omsette resultater fra risiko- og sårbarhetsforskning til systemer, metoder og verktøy for beslutningsstøtte, risikoreduksjon og heving av kompetansen på dette området i industrien, spesielt med hensyn på anvendelse i små og mellomstore bedrifter.

Året etter at ROS-programmet ble startet, ga Direktoratet for sivilt beredskap (DSB) ut en veileder for kommunale risiko- og sårbarhetsanalyser (Direktoratet for sivilt beredskap, 1994) som ble grunnleggende for gjennomføringen av ROS-programmet. Veilederen fra DSB beskriver en av flere mulige framgangsmåter for å systematisere og organisere arbeidet med risiko- og sårbarhets-analyser.

Gjennom et samarbeid mellom Forsvarets forskningsinstitutt (FFI) og Direktoratet for sivilt beredskap ble det såkalte BAS-prosjektet ("Beskyttelse av samfunnet") gjennomført (FFI, 1997). Her blir samfunnets sårbarhet og aktuelle beskyttelsestiltak gjennomgått for bedre å kunne opprettholde samfunnets funksjonsdyktighet ved unormale påkjenninger i fred og krig. Som en fortsettelse på dette prosjektet ble det senere gitt ut en rapport med spesiell fokus på offentlig telekommunikasjon (FFI, 1999).

Den hittil siste nasjonale innsatsen innenfor risiko- og sårbarhetsutredninger startet høsten 1999. Regjeringen opprettet et hurtigarbeidende utvalg som hadde som hovedoppgave å utrede

samfunnets sårbarhet og beredskap. Utvalget, som ble ledet av fylkesmann Kåre Willoch, la i juli 2000 fram sin utredning "Et sårbart samfunn" (Norges offentlige utredninger nr. 24, 2000). Her gjennomgår utvalget dagens sikkerhets- og beredskapsarbeid og peker på eksisterende og kommende utfordringer for samfunnssikkerheten. Utvalget behandler og oppsummerer utfordringer og tiltak innenfor hver sektor i samfunnet. I tillegg gis det generelle og prinsipielle råd til regjeringens videre arbeid med beredskap og tiltak mot samfunnets sårbarhet.

I tillegg til de nevnte arbeidene, bør nasjonale aktører som Næringslivets sikkerhetsorganisasjon (NSO), Sikkerhetsstaben i Forsvarets overkommando (FO/S) og Datatilsynet nevnes i denne sammenheng. NSO har med utgangspunkt i NS 5814 gitt ut et faghefte som omhandler risikoanalyse (Næringslivets sikkerhetsorganisasjon, 1998). FO/S er nasjonal sikkerhetsmyndighet, og skal i henhold til den nye sikkerhetsloven (Ot prp nr. 12, 1997-1998) koordinere forebyggende sikkerhetstiltak og kontrollere sikkerhetstilstanden i Norge. FO/S skal også være utøvende organ i forhold til andre land og internasjonale organisasjoner. Sikkerhetsloven skal regulere forebyggende sikkerhetstjeneste både i militær og sivil forvaltning. Datatilsynet har blant annet gitt ut en veileder i risikoanalyse (Datatilsynet, 1998), som gir en innføring i prinsippene for å gjennomføre en risikoanalyse av et informasjonssystem

Utredninger innenfor risiko- og sårbarhetsanalyse har også blitt utført i andre land. I 1996 satte den amerikanske presidenten ned en kommisjon for å vurdere sårbarheten knyttet til kritisk infrastruktur i USA, samt foreslå strategier for å beskytte kritisk infrastruktur i framtiden. Resultatet kom i rapportform i oktober 1997 (Critical Foundations, 1997). Områdene som ble vurdert var informasjonssystemer og telekommunikasjon, kraftforsyning, vannforsyning, oljerelatert virksomhet, transportsystemer, bankvesen, offentlige tjenester, og øyeblikkelig hjelp slik som lege, brannvesen og politi. Rapporten viste også til et behov for utvikling av metodikk for vurdering av informasjonssikkerhet.

I Canada ga Royal Canadian Mounted Police ut ”Guide to Threat and Risk Assessment for Information Technology Systems” i 1994 (Royal Canadian Mounted Police, 1994). To år senere ga den canadiske regjeringen ut retningslinjer for risikovurdering av et IT-system og dets livssyklus. Retningslinjene er fordelt på tre dokumenter der det første

(Government of Canada, 1996a) tar for seg veiledning i risikostyring, det andre (Government of Canada, 1996b) gir veiledning for systemdesignere ved risikovurdering og valg av tiltak, mens det tredje dokumentet (Government of Canada, 1996c) tar for seg sertifiseringsdokumentasjon ved akkreditering av IT-systemer.

Dataforeningen i Sverige lanserte i 1997 en programvare for sårbarhetsanalyse som først og fremst er rettet mot IT-systemer og IT-prosjekter. Programvaren, som har fått navnet SBA-metoden (Dataforeningen i Sverige, 1997), omfatter blant annet analyse av risiko i prosjekter, analyse av organisasjonens informasjonssikkerhet, og en analysemodell for å analysere hvilke nøkkelfunksjoner og nøkkelpersoner som finnes i virksomheten.

Den svenske Överstyrelsen för civil beredskap (ÖCB) gav i mars 2000 ut rapporten "Infrastrukturuppdraget" (Överstyrelsen för civil beredskap, 2000). Dette er en utredning som tar for seg sårbarheten av den sivile infrastrukturen, med spesiell fokus på telekommunikasjon, kraftforskyning og IT-systemer.

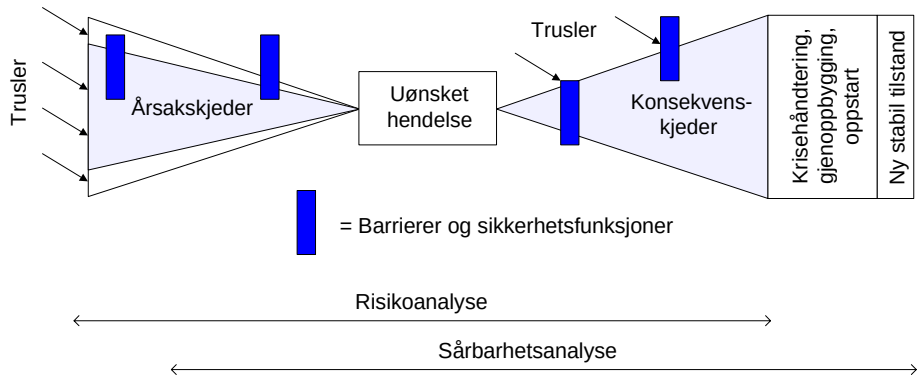
Innenfor NATO arbeides det med å utvikle prinsipper og minimumskrav for å sikre NATO-klassifisert informasjon mot tap av konfidensialitet, integritet og tilgjengelighet, samt å sikre NATO-relaterte ressurser mot tap av integritet og tilgjengelighet. I tilknytning til disse prinsippene og minimumskravene utvikles det også en metode for risikovurdering av gradert informasjon og ressurser (NATO, 1999). I de tilfellene der de gitte minimumskravene for sikring ikke er tilstrekkelige, skal metoden benyttes for å vurdere hvorvidt eventuelle nye sikringstiltak skal implementeres. Metoden og prinsippene for sikring er fortsatt under utarbeidelse.

1.3 Introduksjon til ROS-analyse og security

En årsaks- og konsekvenskjede for et generelt system kan illustreres som vist i Figur 1.1. Figuren illustrerer hvordan uønskede hendelser oppstår som følge av at trusler passerer barrierer og sikkerhetsfunksjoner og hvordan de uønskede hendelsene resulterer i konsekvenser. Etter en viss tid vil systemet gjennom diverse tiltak komme tilbake til en ny stabil tilstand.

I litteraturen skilles det mellom risiko- og sårbarhetsanalyser. En sårbarhetsanalyse er mer omfattende enn en risikoanalyse med hensyn til det som skjer etter at ulykken har inntruffet. Når en uønsket hendelse inntreffer, blir systemet forskjøvet fra den tilstanden det var i. I motsetning til risikoanalyse fokuserer en sårbarhetsanalyse også på avbruddsperioden og hvordan en ny stabil tilstand kan oppstå. En risikoanalyse legger normalt mer vekt på truslene enn en sårbarhetsanalyse. Kort sagt har risikoanalyser fokus på skader som systemet blir utsatt for, mens sårbarhetsanalyser har fokus på overlevelsesevnen til systemet. Sårbarhetsanalyser inkluderer også som oftest et bredere trusselspekter enn risikoanalyser.

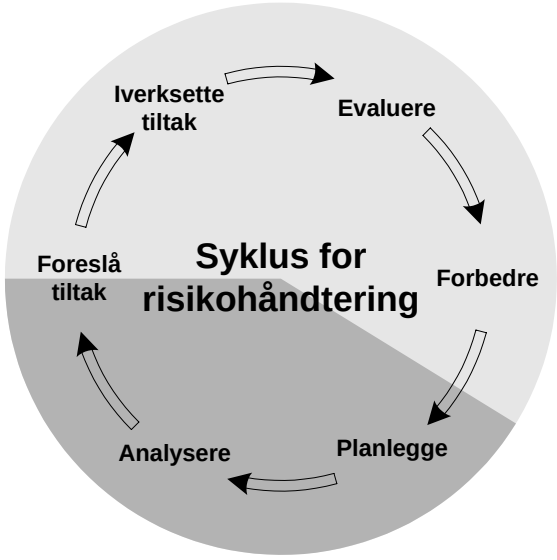
Metoden som blir presentert i kapittel 2, forsøker å dekke hele årsaks- og konsekvenskjeden fra trusler til normaliserende og skadereduserende tiltak. Når det gjelder bredde og dybde i valg av trusler som inkluderes i analysen, settes det ingen absolutte retningslinjer. Det har derfor blitt valgt å kalle metoden for en risiko- og sårbarhetsanalyse.



Figur 1.1. Årsaks- og konsekvenskjeder for risiko- og sårbarhetsanalyser.

Risiko- og sårbarhetsanalyse inngår normalt som en del av en større syklus for risikohåndtering (Figur 1.2). Det mørkeste området i Figur 1.2 indikerer hvilke deler av syklusen som er dekket av metoden som blir presentert i denne rapporten. For at analysen skal være effektiv, bør den først planlegges og organiseres. Dette innebærer å nedsette en arbeidsgruppe, finne bakgrunnen for analysen og beskrive

målsettinger. Når analysen er ferdig, vil det normalt ha kommet fram visse forslag til tiltak. Imidlertid bør tiltakene gjennomgås og kompletteres i etterkant av analysen for å sikre virksomheten mot de potensielle uønskede hendelsene som har blitt identifisert under analysen. Metoden lar arbeidsgruppen som utfører analysen komme med forslag til tiltak i løpet av sitt arbeid, men den legger ikke det totale ansvaret for dette på gruppen. Arbeidsgruppen forventes heller ikke å velge hvilke tiltak som skal iverksettes. Idet tiltak er foreslått, må disse igjennom en utvelgelsesprosess og de viktigste tiltakene iverksettes. Deretter kommer en evalueringsrunde for å se hvor effektive tiltakene viste seg å være, samt for å finne ut om det bør utføres flere analyser. Tiltakene forbedres i neste punkt og en ny analyse, eventuelt med endret bredde og dybde i forhold til den tidligere, kan planlegges. De delene av syklusen som er indikert med lys farge i Figur 1.2 betraktes gjerne som ledelsesverktøy. Disse behandles ikke videre i denne rapporten.



Figur 1.2. Risiko- og sårbarhetsanalyse som del av syklus for risikohåndtering. Det mørkeste området dekkes av analysemetoden som er beskrevet i denne rapporten.

Innenfor risiko- og sårbarhetsanalyse er en *uønsket hendelse* det en ønsker å beskytte seg mot. I vedlegg A defineres en uønsket hendelse

som den første signifikante avvikssituasjonen som har potensialet til å true sikkerheten til et objekt. Uønskede hendelser kan kategoriseres i:

- tilfeldige hendelser
- tilsiktede handlinger

Tilfeldige hendelser opptrer som følge av en eller flere tilfeldigheter, mens tilsiktede handlinger er planlagte og utført med overlegg. For å skille mellom sikkerhetsbegrepet innen de to kategoriene, innføres, av mangel på norske uttrykk, de engelske begrepene *safety* og *security*. Safety omfatter sikkerhet mot tilfeldige hendelser, mens security omfatter sikkerhet mot tilsiktede handlinger.

Før en risiko- og sårbarhetsanalyse utføres, står en gjerne ovenfor valget om å fokusere enten på tilfeldige hendelser, på tilsiktede handlinger, eller forsøke å inkludere begge i analysen. De nødvendige aktivitetene for å analysere de to er imidlertid vesentlig forskjellige, da en analyse av tilsiktede handlinger blant annet krever kartlegging av langt flere faktorer enn en analyse av tilfeldige hendelser. Den presenterte metoden har derfor konsentrert seg kun om tilsiktede handlinger.

Felles for det arbeidet som er lagt ned innenfor risiko- og sårbarhetsforskningen er at innsatsen i all hovedsak er rettet mot safety-området, mens det i liten grad er fokusert på security-delen. Dette går fram av rapporten ”Sikkerhetsforskning” som professor Jan Hovden ved NTNU skrev på oppdrag fra Norges forskningsråd i 1998 (Hovden, 1998). Hovden bruker begrepet *totalsikkerhet* som en målsetting for sikkerhetsarbeidet. Totalsikkerhet oppnås dersom tapsforebyggende tiltak mot tilfeldige ulykkeshendelser (safety), blir sett i sammenheng med tapsforebyggende tiltak mot tilsiktede handlinger (security). Hovden påviser i rapporten at det foreligger et betydelig misforhold siden safety-området har vært gjenstand for omfattende forskning over en 20-30 års periode, mens security-området i liten grad har vært underlagt en slik vitenskapelig tilnærming. Økende avhengighet av informasjonssystemer innenfor samfunnets kritiske infrastruktur, og en endret trusselsituasjon, gjør at sikkerhetsforskningen også bør vektlegge security-området.

1.4 Hvorfor utføre en risiko- og sårbarhetsanalyse?

En risiko- og sårbarhetsanalyse vil i de fleste tilfeller medføre en stor arbeidsmengde og følgelig betydelig ressursbruk for de involverte. Men det finnes flere grunner til at en slik analyse bør gjennomføres. For det første er det av hensyn til egeninteresser. En bedrift vil gjennom en risiko- og sårbarhetsanalyse kunne bedre skjermingen av viktig informasjon og sensitive objekter. Eksempler på dette varierer fra sektor til sektor. Industribedrifter og forskningsinstitusjoner ønsker for eksempel å skjerme forsknings- og utviklingsresultater, og derved redusere sjansene for økonomisk tap som følge av industrispionasje og tyveri. Banker krever for eksempel høy sikring av penger og verdipapirer både i hvelv og under transport, mens blant annet sykehus krever beskyttelse av sensitiv pasientinformasjon. De aller fleste virksomheter vil også ha en generell interesse av å hindre innbrudd og beskytte seg mot datahacking, noe som kan sette hele eller deler av virksomheten ut av spill over kortere eller lengre perioder. Militære virksomheter har blant annet et stort ansvar når det gjelder å sikre informasjon som er av betydning for rikets sikkerhet. Sikkerhetsgradert informasjon utstedes og håndteres også i offentlig virksomhet og i deler av industrien. Et annet og mer ekstremt anvendelsesområde for risiko- og sårbarhetsanalyser, både i militær og sivil sektor, er forebygging av personskader i forbindelse med uønskede handlinger der helse og miljø settes i fare. Enkelte virksomheter er mer utsatt for dette enn andre, og av og til er det spesielle begivenheter som krever økt oppmerksomhet med hensyn til security.

Den andre hovedgrunnen til at risiko- og sårbarhetsanalyser bør utføres, er pålegg gjennom lover og forskrifter. Det foreligger i dag flere forskrifter som omhandler sikkerhet på ulike områder. Metoden som er beskrevet i denne rapporten er utviklet med utgangspunkt i lov av 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven) og dens tilhørende forskrift om organisering og administrasjon av sikkerhetstjenesten i virksomhetene.

1.5 Målsettinger for arbeidet med analysemetoden

Målsettingen for dette prosjektet har vært å utvikle en metode for risiko- og sårbarhetsanalyse av informasjonssikkerhet og objektsikkerhet knyttet til security-området. Det har i den forbindelse ikke vært snakk om ”å finne opp kruttet på nytt”, men om å benytte eksisterende metodikk for risiko- og sårbarhetsanalyse innenfor safety-

området som et utgangspunkt for arbeidet med å utvikle en metode som omfatter de forhold som råder innenfor security.

For selve metodeutviklingen har målet vært å gjøre metoden generell slik at den kan benyttes uavhengig av hvilke systemer eller objekter som analyseres, og at den er anvendbar innenfor både sivil og militær sektor. Metoden er forsøkt utviklet slik at den effektivt kan analysere og vurdere trusler mot virksomhetens sikkerhet.

Metoden kan inngå som et verktøy for virksomhetens ledelse i arbeidet med ressursstyring. Resultater fra risiko- og sårbarhetsanalyser gjennomført i henhold til metoden danner grunnlaget for ledelsens beslutninger og prioriteringer.

Det har også vært en målsetting at prosjektet skal markere starten på en mer vitenskapelig tilnærming til security-området, der behovet for en overgang fra en regelbasert tilnærming til forebyggende sikkerhetstjeneste til en risikobasert tilnærming har stått sentralt. Med risikobasert tilnærming menes at beslutninger om forbedringer og tiltak baseres på en risikoanalyse av aktiviteten, mens det i en regelbasert tilnærming fokuseres på å sikre at faktisk standard er i henhold til materielle krav i lover og forskrifter. Utvikling av et sett med sentrale begreper og definisjoner, noe som kan bidra til et mest mulig ensartet begrepsapparat i arbeidet med risiko- og sårbarhetsanalyser, har derfor vært et delmål. Den utviklede terminologien er beskrevet i vedlegg A.

1.6 Begrensninger

Bruk av metoden krever visse kunnskaper om sikkerhetsrelatert arbeid og terminologi, og det vil derfor være virksomhetens sikkerhetspersonell som vil ha best forutsetninger for å sette seg inn i metoden, og å benytte den på riktig måte.

Metoden er generell, og kan benyttes på ulike typer virksomheter. Imidlertid er det en forutsetning at de uønskede hendelsene som kan ramme virksomheten, er tilsiktede handlinger. For analyse av tilfeldige hendelser henvises det til eksisterende metodikk innenfor safety-området. Metoden er utviklet for analyse av informasjonssikkerhet og objektsikkerhet, og er utviklet med tanke på eksisterende systemer.

Ved analyse av nye systemer blir ikke sikkerheten under selve oppbyggingsfasen spesielt omhandlet.

Metoden er utviklet for å være et kvalitativt verktøy. Under en risikoanalyse estimeres sannsynligheten for at en uønsket hendelse inntreffer. Når det gjelder analyse av tilsiktede handlinger, er det imidlertid svært vanskelig å vurdere hvor sannsynlig en uønsket hendelse er. Sannsynlighetsestimeringen bygger derfor på kvalitative vurderinger.

Fra forskning innenfor risiko og sårbarhet kommer det med jevne mellomrom nye ideer om hvordan en risiko- og sårbarhetsanalyse bør utføres. For å sikre et høyt faglig innhold i metoden, vil det være viktig å oppdatere den med ny innsikt og nye måter å løse problemer på, etter hvert som nye erfaringer og resultater blir tilgjengelige.

2 Presentasjon av metoden

2.1 Begrepsavklaring

I forbindelse med sikkerhet og risiko- og sårbarhetsanalyser blir det benyttet et mangfold av ord og begreper. Uklarhet i hva som menes med de ulike definisjonene forekommer, og det er derfor gitt en avklaring av de mest sentrale definisjonene som er benyttet i denne analysemetoden. En større liste over begreper og definisjoner er gitt i vedlegg A. Analysemetoden er ment å være generell og kunne benyttes av ulike virksomheter og etater. Sikkerhetsmessig begrepsbruk i den enkelte virksomhet og etat kan variere og sammenfaller derfor ikke nødvendigvis med hva som benyttes her.

Metoden dekker både objekter og informasjon. I det følgende blir imidlertid begge disse gruppene omtalt som objekt, da informasjon oppfattes som et "informasjonsobjekt".

Objekt
Materiell, utstyr, personell, informasjon, infrastruktur og andre verdier.

Risiko
Uttrykk for den fare som uønskede hendelser representerer for informasjon/objekter av skjermingsverdig karakter. Risikoen uttrykkes ved sannsynligheten for og konsekvensene av de uønskede hendelsene.

Sårbarhet
En svakhet som reduserer eller begrenser et systems evne til å motstå en uønsket hendelse, eller til å gjenopprette en ny stabil tilstand etter hendelsen har inntruffet.

Risikoanalyse
En systematisk gjennomgang av et system i den hensikt å beregne systemets evne til å motstå trusler ved å identifisere trusler og kvantifisere risiko.

Sårbarhetsanalyse
En systematisk gjennomgang av et system i den hensikt å beregne systemets evne til å motstå trusler og overleve uønskede hendelser, ved å identifisere trusler, kvantifisere risiko og evaluere evne til stabilisering av systemet.

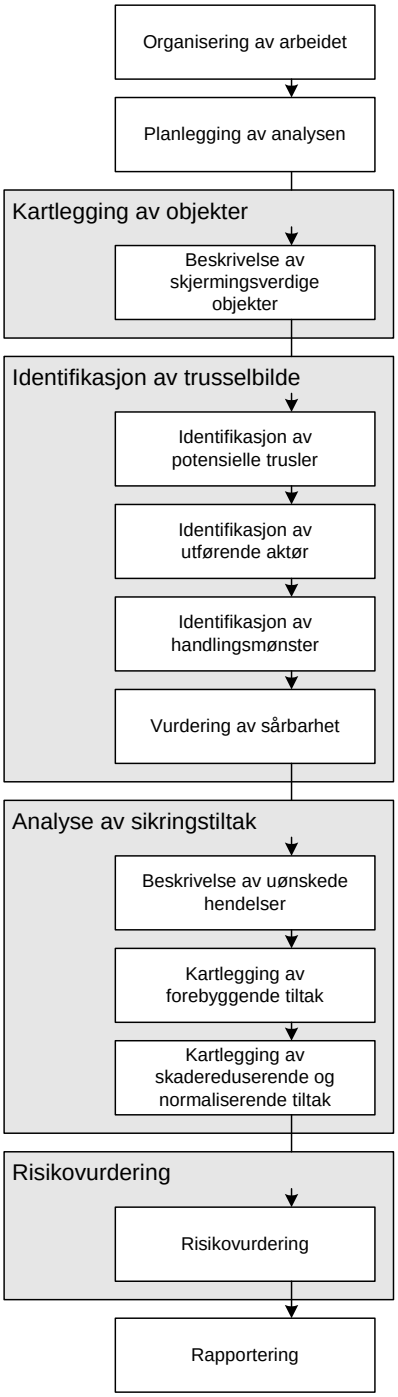
2.2 Generelt

Er sikringen av systemet mot tilsiktede handlinger tilfredsstillende? Metoden som presenteres i dette kapittelet omhandler en analyse som hovedsakelig forsøker å svare på dette spørsmålet.

Analysen er en risiko- og sårbarhetsanalyse som fokuserer på tilsiktede handlinger og fagområdet som omtales som security. Tilfeldige hendelser blir ikke behandlet.

Målgruppen for denne metoden omfatter alt fra store militære anlegg til små private bedrifter, og er derfor svært stor og blandet. Intensjonen er at metoden skal foreligge som et rammeverk for hvordan en securitybasert risiko- og sårbarhetsanalyse kan utføres. Den er ikke ment som en detaljert oppskrift som slavisk må følges av alle. Enkelte vil forhåpentligvis kunne ta i bruk metoden slik den her blir presentert, men hovedhensikten med metoden er å presentere retningslinjer for en risiko- og sårbarhetsanalyse med fokus på tilsiktede handlinger.

Analysen er hovedsakelig bygget opp rundt fire skjema, der hvert skjema omfavner ett eller flere arbeidspunkter. En skisse av analysens skjema og arbeidspunkter er gitt i Figur 2.1. Etter organisering og planlegging av arbeidet drives analysen fram ved hjelp av utfylling av de fire skjemaene. Skjermingsverdige objekter identifiseres, trusselbildet disse står ovenfor kartlegges og de eksisterende sikringstiltakene evalueres. En vurdering av konsekvens og sannsynlighet utgjør deretter risikovurderingen som markerer slutten på selve analysen. Til slutt blir forslag til rapporteringen fra analysen gjennomgått. Skjemaene og arbeidstrinnene blir detaljert beskrevet fra og med avsnitt 2.4.

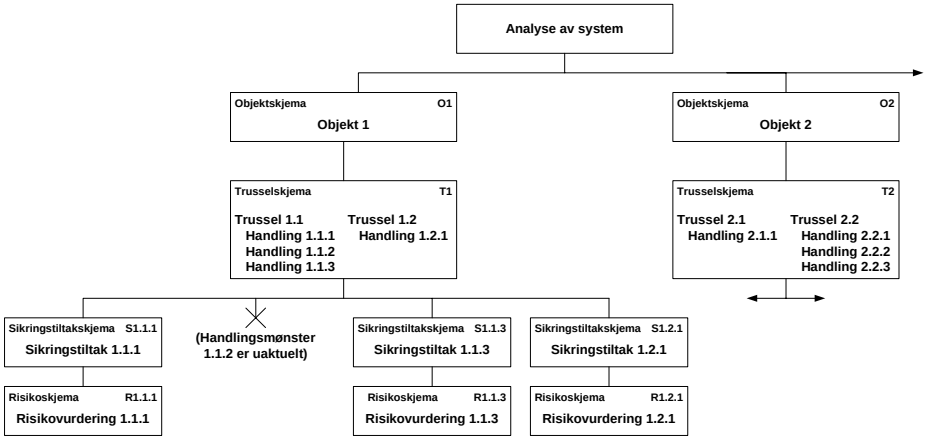


Figur 2.1. Skjematisk illustrasjon av analysens skjemaer (grå felt) og arbeidspunkter (hvite felt)

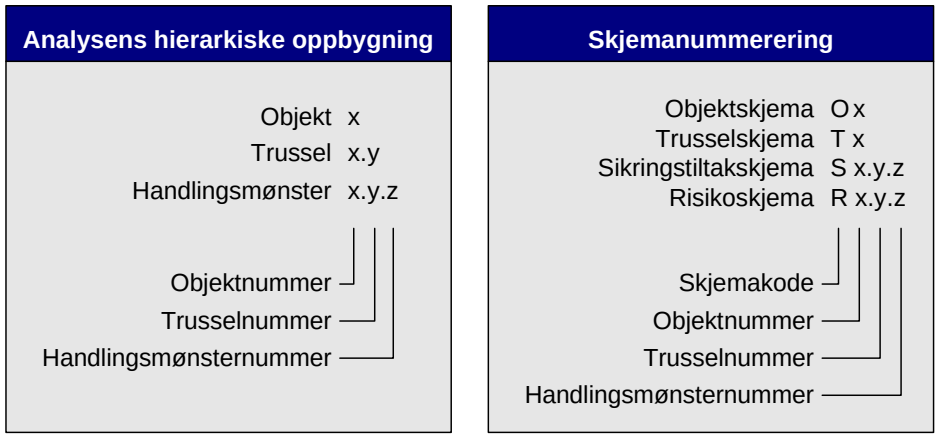
2.3 Analysens struktur

Utgangspunktet under analysen er de skjermingsverdige objektene. Til hvert objekt er det knyttet flere trusler, og for hver trussel kan det være tilknyttet flere handlingsmønstre.

De fire skjematypene utgjør en hierarkisk struktur, som er illustrert i Figur 2.2. Skjemaene gis nummer i samsvar med denne strukturen. Numrene består av én bokstav som gjenspeiler den aktuelle skjematypen, etterfulgt av et hierarkisk nummer, som illustrert i Figur 2.3.



Figur 2.2. Illustrasjon av analysens skjemastruktur.



Figur 2.3. Illustrasjon av analysens hierarkiske oppbygning og skjemanummerering.

Innledningsvis i analysen brytes systemet ned i verdier, eller såkalte *skjermingsverdige objekter*. Objektene nummereres løpende og representerer det første hierarkiske nivået. Objektene blir beskrevet på et *objektskjema*.

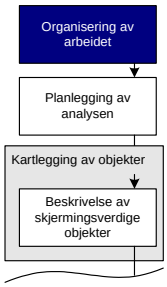
Idet trusselbildet evalueres blir én eller flere *trusler* knyttet til hvert objekt. Truslene nummereres løpende og representerer det andre hierarkiske nivået. Alle trusler knyttet til ett objekt føres på det samme *trusselskjemaet*. For hver trussel finnes flere *handlingsmønstre*. Handlingsmønstre knyttes derfor opp mot den aktuelle trusselen, og markerer det tredje hierarkiske nivået. Handlingsmønstrene nedtegnes på trusselskjemaet sammen med truslene.

For handlingsmønstre som anses som reelle, utføres en evaluering av eksisterende *sikringstiltak* på et eget *sikringstiltakskjema*. Sikringstiltak knyttet til hvert enkelt handlingsmønster evalueres på et separat skjema.

Til slutt evalueres *risikoen* forbundet med det enkelte handlingsmønsteret ved å vurdere sannsynlighet og konsekvens. Dette nedtegnes på et *risikoskjema*. Også her fylles det ut ett skjema per handlingsmønster.

Analysemetoden, strukturen og utfyllingen av de ulike skjemaene blir detaljert forklart i de påfølgende avsnittene. Et relativt utfyllende eksempel som illustrerer hvert trinn i analysen, gis i kapittel **Feil! Fant ikke referansekilden.**.

2.4 Oppstartsfasen: Organisering og planlegging



2.4.1 Organisering av arbeidet

Arbeidet med risiko- og sårbarhetsanalysen utføres av en arbeidsgruppe under ledelse av en gruppeleder. Gruppelederen velger ut deltakere til arbeidsgruppen, men disse må godkjennes av ledelsen. Arbeidsgruppen omfatter personer som har nødvendig kjennskap til analyseobjektet og hvordan sikkerheten blir opprettholdt. Før arbeidet settes i gang, er det viktig å kartlegge kompetanseområdene til de forskjellige gruppemedlemmene. Gruppeleder bør ha god kjennskap til metodikken som skal benyttes.

Gruppelederen har ansvar for oppfølging og kommunikasjon mellom de aktuelle partene under arbeidet med analysen. En tidsplan for gjennomføringen av analysen bør utarbeides. Gruppelederen bør også identifisere tids- og ressursbehov, slik at den økonomiske rammen for analysen kan bestemmes og godkjennes av ledelsen.

Det er viktig å være klar over at når skjemaene som benyttes i analysen er ferdig utfylte, vil disse inneholde mye sensitiv informasjon. Skjemaene må derfor gis nødvendig gradering og skjermes for offentligheten.

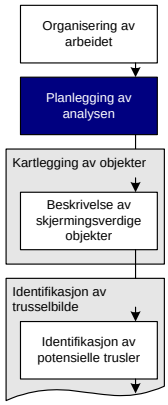
2.4.1.1 Regelmessig oppdatering av risiko- og sårbarhetsanalyser

Virksomheten som skal analyseres, må betraktes som et dynamisk system. I enhver virksomhet forekommer det fra tid til annen større og mindre endringer. Analyseresultatene er viktig og levende informasjon som er essensiell for risikohåndteringen ved virksomheten. For å sikre at analysen ikke blir foreldet, bør virksomheten ha et bevisst forhold til hvordan og hvor ofte en risiko- og sårbarhetsanalyse skal utføres. Selv om slike analyser er ressurskrevende, bør et slikt arbeid ses på som en fornuftig investering for å sikre virksomheten mot eventuelle uønskede hendelser.

Dersom ikke retningslinjer for oppdatering av analyseresultatene allerede foreligger, bør slike retningslinjer fastsettes slik at en ny analyse utføres med jevne mellomrom. Et forslag er å utføre en ny analyse hvert andre år i tillegg til løpende oppdateringer etter eventuelle mindre endringer som medfører mangler eller unøyaktigheter i de eksisterende analyseresultatene. En kompletterende

analyse bør også utføres før markante endringer av systemet eller dets omgivelser inntreffer eller blir utført.

2.4.2 Planlegging av analysen



Planleggingsarbeidet utføres i utgangspunktet av gruppeleder, men det kan være fordelaktig med aktiv deltakelse fra arbeidsgruppen. En slik deltakelse vil føre til økt forståelse for hva som skal analyseres og for nødvendigheten av analysen.

2.4.2.1 Bakgrunn og målsetting

Gruppeleder beskriver bakgrunnen for analysen: *Hvorfor utføres analysen?* I tillegg beskriver gruppeleder og arbeidsgruppen målsettinger for analysen: *Hva ønsker vi å oppnå med analysen?*

En god målformulering er viktig for at analysen skal kunne fokusere på kjernen i problemet og utføres effektivt. Dersom målformuleringen er presis og dekkende, vil analysen bli effektivt utført og gi svar på spørsmålene som har blitt stilt. Det er viktig at små og store beslutninger som en blir møtt med i løpet av analysens gang, blir tatt korrekt i forhold til analysens hensikt.

Siden risiko- og sårbarhetsanalysen er et ledd i virksomhetens sikkerhetsarbeid, må arbeidsgruppen påse at analysen blir utført i tråd med intensjonen bak det generelle sikkerhetsarbeidet i virksomheten. Målsettingen for analysen bør derfor inngå som en del av den overordnede målsettingen for virksomhetens generelle risikohåndtering.

I de fleste tilfeller vil det være en fordel å etablere flere delmål som støtter opp under og fokuserer på hovedmålet. Delmålene vil utgjøre en detaljering av hovedmålet. Dersom hovedmålet for eksempel dekker et helt anlegg, kan delmålene ta for seg enkelte bygninger eller avdelinger. På de laveste nivåene er det ikke alltid nødvendig at målsettingen skrives ned og formaliseres, men det kan likevel være lurt å tenke gjennom målsettinger for mindre delelementer av analysen.

Det bør også etableres kriterier som kan illustrere om hovedmålet og de enkelte delmålene er oppnådd eller ikke. Som kriterier benyttes gjerne såkalte måltall. Et måltall er en verdi som viser om en målsetting er oppnådd eller ikke, evt. i hvor stor grad målsettingen er

oppnådd. For én målsetting kan det være flere måltall som avgjør grad av suksess. Som et eksempel kan målformuleringen for en analyse bestå i å analysere sårbarheten av alle objekter som vurderes til å ha *middels* eller *høy betydning*. Da vil et intuitivt valg av kriterium være hvor mange av disse objektene som har blitt analysert. Et mer generelt og enklere kriterium vil kunne være om analysen er utført innen tidsfrister og kostnadsrammer.

En kort sjekkliste for en god målformulering er:

- Avgrenser målsettingen oppgaven? Spesifiseres hva som skal gjøres eller hva som skal oppnås?
- Beskriver målsettingen spesifikt hvilke spørsmål som skal besvares, og hvordan disse skal besvares?
- Er målet etterprøvbart? På hvilken måte kan en si om målet er nådd eller ikke?
- Er målsettingen realistisk? Er det mulig å oppnå målsettingen?

For mange virksomheter foreligger det overordnede bestemmelser på visse områder innenfor sikkerhet som danner *minimumskrav*. En del av målsettingen for analysen kan derfor være å kontrollere at eventuelle minimumskrav til sikkerheten er oppfylt. Slike krav blir for eksempel stilt i Sikkerhetsloven med forskrifter og Personopplysningsloven med forskrifter, for virksomheter som blir berørt av disse lovene.

En komplett risiko- og sårbarhetsanalyse er tidkrevende å utføre, særlig om ikke virksomheten allerede sitter inne med erfaring fra slikt arbeid. Det bør derfor presiseres at en analyse ikke nødvendigvis trenger å bli utført etter en detaljert og omfattende metodikk første gang. I mange tilfeller kan det være lønnsomt å starte med en mer udetaljert analyse, for eksempel en såkalt grovanalyse. Slik kan arbeidsgruppen, eller deler av gruppen, relativt rask danne seg en oversikt over de viktigste risikoene de forskjellige delene av virksomheten står ovenfor. Når den detaljerte ROS-analysen så skal gjennomføres, kan arbeidsgruppen hente resultater og erfaringer fra grovanalysen og trekke dette inn i planleggingsarbeidet. For eksempel kan arbeidsgruppen i første omgang velge å konsentrere seg om spesifikke områder eller aktiviteter i virksomheten de ønsker å analysere.

2.4.2.2 Beskrivelse av systemet

Å beskrive systemet (det generelle analyseobjektet) kan være en stor og vanskelig oppgave. Imidlertid viser erfaring at ressursene som nedlegges i å beskrive systemet er en god investering: Analysen utføres raskere og kvaliteten blir bedre hvis systemet på forhånd er beskrevet i detalj. Arbeidsgruppen ser da klarere hva de står ovenfor, og får lettere en lik oppfatning om hvilke forhold som er vesentlige for systemets drift, sikkerhet og overlevelse.

For å beskrive systemet er det mange forhold som detaljert må besvares. Imidlertid er det visse fundamentale spørsmål som arbeidsgruppen så tidlig som mulig bør besvare:

- Hva er systemet avhengig av (input)?
- Hvilke arbeidsoppgaver utøves i systemet (funksjoner)?
- Hvilke tjenester leverer systemet (output)?

Disse spørsmålene kan gjerne besvares ved å visualisere systemet ved hjelp av en eller flere ulike representasjonsteknikker. Et organisasjonskart kan være et utgangspunkt, men det kan være en stor fordel å få en oversikt over hvilke objekter og funksjoner som utgjør virksomheten. Noen av de mest brukte teknikkene er omtalt i vedlegg B. Arbeidsgruppen kan velge å visualisere hele systemet eller enkelte funksjoner eller objekter i systemet.

Etter at de mer fundamentale forholdene er gjennomgått, beskrives systemet detaljert og presist i tekstform for å gi arbeidsgruppen det nødvendige innblikket i virksomheten og dens omgivelser. Alle tekniske, organisatoriske og menneskelige forhold som er aktuelle for virksomheten angis i nødvendig detalj. Spesielt bør det framgå hvilke forhold som har betydning for sikkerheten.

Virksomheten kan være pålagt formelle krav om tiltak med tanke på sikkerhet. Slike juridiske pålegg (som må ses i sammenheng med eventuelle minimumskrav stilt i lover og forskrifter) bør nevnes i systembeskrivelsen. Eventuelle politiske, sosiale og økonomiske relasjoner knyttet opp mot virksomheten bør også beskrives. Det er nødvendig å angi hvilke operasjonelle tilstander eller driftstilstander som skal gjelde for analysen.

Gruppeleder må også angi klare avgrensninger for analysen. Dette omfatter fysiske og organisatoriske grenser mot omgivelsene. Det

angis her spesielt hva som blir tatt med i analysen, og hva som blir holdt utenfor.

Det første punktet i selve analysearbeidet vil være å bryte ned systemet som skal analyseres i objekter som skal vurderes i detalj. Alle objektene som ligger innenfor analysens rammer (som virksomheten ønsker å beskytte) skal identifiseres. Dette er et stort og krevende arbeid, og detaljeringsgraden bør fastlegges i planleggingsarbeidet på en slik måte at en hensiktsmessig analyse kan utføres. Detaljeringsgraden kan variere mye: Et objekt kan for eksempel være én enkelt telefaks, avdelingens kommunikasjonsutstyr generelt, eller hele avdelingen sett under ett. "Informasjonsobjekter" kan blant annet representere håndfast, avgrenset informasjon som en dokumentmappe, avgrenset elektronisk informasjon som en harddisk med dens innhold, eller mer omfattende kategorier tilsvarende hovedkategoriene av sikkerhetsgradert informasjon (Se vedlegg C).

En for detaljert analyse kan kreve for mye ressurser, men analysen bør heller ikke utføres for generelt, slik at blant annet sjeldne, men viktige spesialtilfeller blir glemt eller oversett. Mulige retningslinjer kan være å velge detaljeringsnivå på bakgrunn av objektenes fellestrekk. To objekter som står ovenfor de samme truslene, utfører den samme funksjonen, og ellers er mer eller mindre identiske, kan sannsynligvis analyseres under en fellesbetegnelse uten store vanskeligheter. Hvis derimot detaljeringsgraden velges så grov at ett analyseobjekt for eksempel inneholder flere gjenstander med ulike trusler og ulike funksjoner, vil en komplett analyse være vanskeligere å utføre.

Dersom analyser skal utføres av flere underavdelinger, bør en styringsgruppe i ledelsen avklare detaljeringsgraden og analyserammene slik at de ulike avdelingene blir analysert ut fra de samme premissene.

2.4.2.3 Generelle retningslinjer for avgrensning av analysen

Avgrensning og generelle spørsmål som ”*Hva skal inkluderes i analysen, og hva kan en neglisjere?*” er vanskelig å besvare. Dette er spørsmål som særlig vil bli stilt ved identifikasjon av objekter, trusler, utførende aktør og handlingsmønstre. Selv om det er et vanskelig spørsmål å ta stilling til, anbefales det at arbeidsgruppen tenker gjennom problemstillingen og har en bevisst holdning når disse spørsmålene avdekkes.

Feil valg i forbindelse med hva som skal inkluderes i analysen og hva som kan neglisjeres, kan medføre at potensielle uønskede hendelser blir oversett og viktige tiltak ikke blir iverksatt. Disse valgene handler derfor om hvilken risiko systemet frivillig eller ufrivillig blir stilt ovenfor.

Som generelle retningslinjer i slike spørsmål benyttes ofte det såkalte ALARP-prinsippet, som sier at risiko skal være As Low As Reasonably Practicable. Kort fortalt defineres tre risikonivåer. Risiko over et bestemt nivå er utolererbart og må umiddelbart reduseres. På den andre siden av skalaen finnes et risikonivå så lavt at det er neglisjerbart. Mellom disse områdene er risikoen akseptabel såfremt det er bevist eller sannsynliggjort at kostnadene (”in time, trouble and expense”) i forbindelse med en reduksjon av risiko er uforholdsmessig høy i forhold til selve reduksjonen. En videre forklaring av ALARP-prinsippet finnes blant annet i The Engineering Council (1993).

ALARP-tankegangen kan gjerne foreligge som retningslinjer idet spørsmålene om hva som kan neglisjeres i en analyse skal besvares. Imidlertid gir den ingen umiddelbare svar, og det vil hele tiden kunne stilles spørsmål om hvilken risiko som er neglisjerbar, og hvordan denne risikoen estimeres. En står igjen med det faktum at analysegruppen må bruke fornuft i bestemmelsen av ”cut-off”-kriterier.

Spørsmålet en kan ha i bakhodet er ”*Medfører dette objektet, trusselen, aktøren eller handlingsmønsteret kun en neglisjerbar risiko?*”. Om dette er tilfellet, bestemt av usannsynlige hendelser eller ubetydelige konsekvenser, utelates elementet fra analysen. Arbeidsgruppen analyserer derimot alle elementer som ligger over dette neglisjerbare nivået. Resultatene fra denne analysen vil deretter ligge til grunn for å avgjøre om nye tiltak skal iverksettes, eller om risikoen kan aksepteres slik den foreligger i dag på grunn av at eventuelle tiltak medfører en kostnad som er ”uforholdsmessig høy” i forhold til reduksjonen av risiko.

De tilgjengelige ressursene for å utføre en analyse er ofte begrensede. Imidlertid vil naturligvis det sikreste utvelgelseskriteriet alltid være å inkludere tvilstilfeller.



2.5 Utfylling av skjema ”Beskrivelse av objekt” (O-skjema)

Som første punkt i selve analysearbeidet står identifikasjon og vurdering av de objektene som ligger innenfor analysens rammer og som virksomheten ønsker å beskytte, såkalte skjermingsverdige objekter. For hvert objekt identifiseres sikkerhetsansvaret, anvendelse eller funksjon samt muligheter for erstatning og reserveløsninger. I tillegg vurderes objektets sensitivitet og viktighet for systemet.

Hvert objekt gis et nummer for at en senere i analysen skal kunne referere til objektet, og for å sikre sporbarheten av den nedtegnede informasjonen. Disse objektnumrene gis løpende fra 1 og opp til det totale antall objekter.

Informasjonen nedtegnes på skjemaet ”Beskrivelse av objekt” som er vist i Figur 2.4. For hvert skjermingsverdig objekt benyttes det ett skjema.

Som en innledning nedtegnes navnet på systemet som analyseres, og det aktuelle objektet som analyseres. Navnet på systemet vil stå som en overskrift for hele analysen. Dette vil være virksomhetens navn eller en fellesbetegnelse på de delene som arbeidsgruppen har valgt å analysere, for eksempel ”Utforsk A/S - lagerbygning”. Objektnavnet er nummeret og navnet på det enkelte analyseobjektet i tillegg til eventuell annen, kortfattet informasjon, eksempelvis ”3, Dataserver på rom 2.11”.

I tillegg registreres dato arbeidet utføres samt hvem analysen utføres av (navn eller eventuell referanse til arbeidsgruppens medlemmer). Det nedtegnes også et revisjonsnummer som representerer hvilken versjon arbeidsgruppen arbeider med. Revisjonsnummer kan angis med ”A” for første revisjon, ”B” for andre revisjon, og så videre.

Beskrivelse av skjermingsverdig objekt			Skjema nummer: O
System:	Dato:	Utført av:	Revisjon:
Skjermingsverdig objekt (nr. x, navn):			
Daglig ansvarlig for objektets sikkerhet:			
Anvendelse eller funksjon:			
Hvordan kan objektet erstattes?		Kan erstattes innen:	
		Erstatningskostnad:	
Beskrivelse av eksisterende reserveløsning(er):			
Sensitivitet	Ytterste konsekvens hvis tap av konfidensialitet:		
	Ytterste konsekvens hvis tap av integritet:		
	Ytterste konsekvens hvis tap av tilgjengelighet:		
Kommentar:		Objektets betydning: ☐ Høy ☐ Middels ☐ Lav ☐ Lav, ingen videre analyse	

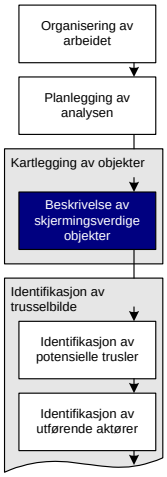
Skjemanummerering

Beskrivelse av skj.verdig objekt *"O-skjema"*

Skjemanummer:
"O"
+ objektnummer

Eksempel:
"O3"
(skjema for objekt 3)

Figur 2.4. Skjema for beskrivelse av skjermingsverdig objekt. Skjemaet er forminsket i forhold til original størrelse. Originalskjema er gitt i vedlegg A.



2.5.1 Beskrivelse av skjermingsverdige objekter

Alle objektene som ligger innenfor analysens rammer, identifiseres og listes opp. Dette er et stort og krevende arbeid, og detaljeringsgraden bør, som nevnt i avsnitt 2.4, ha blitt fastlagt i planleggingsarbeidet på en slik måte at en hensiktsmessig analyse kan utføres. Systemet som analyseres, brytes ned i objekter etter den valgte detaljeringsgraden. Et O-skjema (Figur 2.4) fylles ut for hvert objekt.

Navnet på den daglige ansvarlige for objektets sikkerhet nedtegnes på skjemaet i rubrikken ”Daglig ansvarlig for objektets sikkerhet”. Her menes det ikke den rent juridisk ansvarlige, som normalt er virksomhetens leder, men personen som på operativt nivå har det daglige ansvaret for og muligheten til å iverksette eventuelle sikkerhetstiltak. Objektets anvendelse eller funksjon forklares i rubrikken ”Anvendelse eller funksjon”. Anvendelse og funksjon kan i mange tilfeller være opplagt, og arbeidsgruppen bør selv vurdere hvor detaljert dette feltet skal fylles ut. Hensikten er å få arbeidsgruppen til å tenke gjennom alle anvendelser og funksjoner som er forbundet med objektet, for blant annet lettere å kunne vurdere sensitivitet og hvor viktig objektet er for virksomheten.

Opplysninger om erstatning og reserveløsninger nedtegnes på O-skjemaet. Hvordan objektet erstattes skrives ned i rubrikken ”Hvordan kan objektet erstattes?”, mens den antatte tiden det tar før objektet er erstattet skrives i feltet ”Erstattes innen”. Med erstatning menes her prosessen med å skaffe til veie et nytt objekt slik at systemet kan returnere til en tilnærmet normal tilstand. Kostnaden som er forbundet med erstatningen anslås i rubrikken ”Erstatningskostnad”. Eksisterende reserveløsninger beskrives i feltet ”Beskrivelse av eksisterende reserveløsning(er)”. Det bør her påpekes hvordan eventuelle reserveløsninger vil virke, hvor raskt de kan være operative, kostnader, og annen relevant informasjon. Med reserveløsning menes en midlertidig løsning som kan virke i tidsrommet før objektet er endelig erstattet.

Sensitiviteten forbundet med objektet skal nå vurderes. Arbeidsgruppen skal evaluere konsekvensene forbundet med tap av konfidensialitet, integritet og tilgjengelighet. Med tilgjengelighet menes både tilgjengeligheten av det fysiske objektet, og tilgjengeligheten av objektets funksjon. Siden skjemaet benyttes til både fysiske objekter og informasjonsobjekter, kan en eller flere av rubrikkene være lite relevante i visse tilfeller, og kan las stå ubesvart. I

tillegg til en generell beskrivelse av sårbarheten, er en av hovedhensiktene med å vurdere disse konsekvensene å få en gradering av objektets generelle betydning for systemet. Senere i analysen vil det da være mulig å prioritere hvilke objekter som først skal analyseres videre. Ved vurdering av konsekvens ved tap av konfidensialitet, integritet og tilgjengelighet, vurderes derfor den ytterste konsekvens. En må da ta i betraktning både umiddelbare konsekvenser og konsekvenser som først gir seg til kjenne etter en viss tid. Det er også viktig å vurdere eventuelle konsekvenser tap av konfidensialitet, integritet og tilgjengelighet kan få for andre objekter. Ved vurdering av de ulike konsekvensene skal arbeidsgruppen ikke ta erstatningsmuligheter og reserveløsninger med i betraktningen. Selv om en ofte kan trekke *ytterste* konsekvens nærmest til verdens undergang, menes det i disse tilfellene et realistisk worst-case scenario.

Eventuelle kommentarer til objektet skrives inn i ”Kommentar”-rubrikken, før objektets generelle betydning oppsummeres. Betydningen graderes etter *høy*, *middels*, *lav* og *lav, ingen videre analyse* i feltet ”Objektet betydning”.

Objektets betydning må ses på som en total vurdering av anvendelse og funksjon, muligheter for erstatning, mulige reserveløsninger og sensitivitet (ytterste konsekvens ved tap av konfidensialitet, integritet og tilgjengelighet). For informasjonsobjekter bør en i tillegg ta eventuell sikkerhetsgradering i betraktning (se for øvrig vedlegg C).

Et forslag til mulige kriterier ved gradering av objektets betydning er følgende:

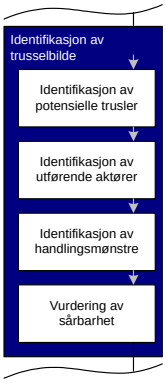
- *høy*: Tap av konfidensialitet, integritet og/eller tilgjengelighet medfører bortfall av en eller flere av systemets hovedfunksjoner (ingen output)
  eller
  informasjonsobjektet har høy sikkerhetsgradering eller høy sensitivitet.

- *middels*: Tap av konfidensialitet, integritet og/eller tilgjengelighet medfører svekkelse av en eller flere av systemets hovedfunksjoner (forringet output)
  eller
  informasjonsobjektet har lav sikkerhetsgradering eller lav sensitivitet.

- *lav*: Systemets hovedfunksjoner opprettholdes, men tap av konfidensialitet, integritet og/eller tilgjengelighet medfører at en eller flere enheter settes i en ufullkommen tilstand (normal output)
  eller
  informasjonsobjektet er ugradert eller ikke sensitivt.
- *lav, ingen videre analyse*: Som lav, men endringen fra normal tilstand vurderes som ubetydelig og en videre analyse vurderes som unødvendig (normal output).

I de fleste tilfellene vil arbeidsgruppen ha begrensede ressurser og ønsker gjerne å prioritere hvilke objekter som detaljert skal behandles i det videre arbeidet. I henhold til analysens målsetting kan nå en prioritering utføres på grunnlag av ”Objektets betydning”.

2.6 Utfylling av skjema ”Identifikasjon av trusselbilde” (T-skjema)



En liste over skjermingsverdige objekter er nå utarbeidet. De neste arbeidspunktene består i å analysere trusselbildet mot hvert enkelt objekt. Dette gjøres ved å identifisere mulige trusler, se på hvem som kan realisere truslene, og hvordan de kan bli realisert.

En filtreringsprosess sørger for at trusler, aktører eller handlingsmønstre kan vurderes som uaktuelle. Slik kan kortfattet informasjon bli nedtegnet for å dokumentere at arbeidsgruppen har vurdert et tilfelle, men anslått risikoen som så liten at en videre analyse ikke har blitt utført.

I tillegg til selve trusselbildet, identifiseres svakheter som svekker muligheten til å motstå en trussel, eller hindrer eller begrenser mulighet til normalisering etter at en uønsket hendelse har inntruffet.

Informasjonen nedtegnes på skjemaet ”Identifikasjon av trusselbilde” som er vist i Figur 2.5. For hvert skjermingsverdig objekt benyttes det ett skjema eller flere skjema. Dersom det trengs flere skjema for ett objekt, indikeres rekkefølgen av disse med bokstav som vist i figuren i margen.

Skjemaet innledes med navn på systemet som analyseres, dato, hvem analysen utføres av, revisjonsnummer og objektets navn og nummer.

For hver trussel identifiseres det normalt flere utførende aktører, og for hver aktør sannsynligvis flere handlingsmønstre. Informasjonen på skjemaet vil derfor utgjøre en trekantstruktur (se eksempel i kapittel 3).

Identifikasjon av trusselbilde			Skjema nummer: T
System:	Dato:	Utført av:	Revisjon:
Skjermingsverdig objekt (nr. x, navn):			
Trussel (nr. x.x, navn)	Utførende aktør	Handlingsmønster (nr. x.x.x, navn)	Svakheter
Kommentar:			

Skjemanummerering

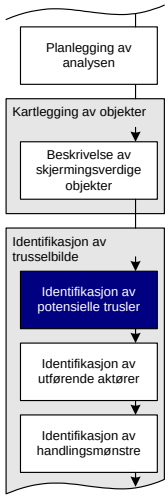
Identifikasjon av trusselbilde
"T-skjema"

Skjemanummer:
"T"
+ objektnummer

Eksempel:
"T3"
(skjema for objekt 3)
"T3-a", "T3-b", osv.
(hvis skjemaet går over flere sider)

Figur 2.5. Skjema for identifikasjon av trusselbilde. Skjemaet er forminsket i forhold til original størrelse. Originalskjema er gitt i vedlegg A.

2.6.1 Identifikasjon av potensielle trusler



Ut fra listen over skjermingsverdige objekter, identifiserer arbeidsgruppen nå alle potensielle trusler mot hvert enkelt element i denne listen. Det er viktig å se på trusler rettet mot kravene til både konfidensialitet, integritet og tilgjengelighet.

En slik identifikasjonsprosess vil normalt utføres som en idédugnad rundt spørsmålet "*Hvilke trusler står de aktuelle objektene eller den aktuelle informasjonen ovenfor?*".

I en slik prosess kan det være nyttig å ta utgangspunkt i ulike kategorier over potensielle trusler, som for eksempel kategoriene gitt i Tabell 2.1. Ut fra disse eller egendefinerte kategorier, setter arbeidsgruppen opp en liste over potensielle trusler. Eksempler på trusler er gitt i Tabell 2.2. Arbeidsgruppen oppfordres først til å sette opp sin egen trusselliste ved hjelp av en idédugnad, for deretter å

komplettere denne ved å sammenligne med andre allerede eksisterende lister. Om en tar utgangspunkt i en eksisterende liste, er det lett å bli overbevist om at listen ser komplett ut, og dermed overse viktige trusler. En ny idédugnad vil også medføre at etter hvert som ytterligere analyser utføres på det samme objektet, vil analysen bli mer og mer komplett. En kan godt starte med en idédugnad for truslene mot hele virksomheten først, for så å ta for seg spesialiserte trusler mot de enkelte objektene.

Det er viktig å være klar over at sjekklisten i Tabell 2.2 er ment som et forslag og kan ikke anses som komplett.

Under idédugnaden kan det også være lønnsomt å se på virksomhetens målsettinger og delmål. Hvis det aktuelle objektet er av betydning for virksomhetens suksess, kan det være nyttig å spørre: ”*Hvilke trusler kan medføre at virksomheten ikke når sin målsetting?* ”

Truslene som arbeidsgruppen har identifisert som realistiske føres inn i skjemaet ”Identifikasjon av trusselbilde” (Figur 2.5), under kolonnen ”Trussel”. Trusselnummeret gis som *Objektnummer.Trusselnummer* med fortløpende *Trusselnummer*. For eksempel får den tredje trusselen under objekt nummer *2* nummeret *2.3*.

Under identifiseringen av trusler kan arbeidsgruppen ønske å dokumentere at de har vurdert en trussel, men anslått at den representerer en så liten risiko at de ikke ønsker å arbeide videre med den. Dette gjøres ved at trusselen som vanlig nedtegnes i "Trussel"-kolonnen, for så å skrive et "÷"-tegn i den smale kolonnen like til høyre. Hvis trusselen markeres med et "÷"-tegn, går ikke arbeidsgruppen videre for å identifisere aktører eller handlingsmønstre for denne trusselen.

Tabell 2.1. Eksempler på kategorier over potensielle trusler.

Kategori	Forklaring
Tyveri	Ulovlig tilegnelse av utstyr, materiell eller informasjon for egen eller andres vinnings skyld.
Alminnelig skadeverk	Umotivert ødeleggelse av utstyr, materiell, informasjon eller aktiviteter.
Spionasje	Innsamling av informasjon ved hjelp av fordekte midler i etterretningsmessig hensikt.
Sabotasje	Tilsiktet ødeleggelse, lammelse eller driftsstopp av utstyr, materiell, informasjon eller aktiviteter, eller uskadeliggjøring av personer, utført av eller for en fremmed stat, organisasjon eller gruppering.
Terrorhandlinger	Ulovlig bruk av, eller trussel om bruk av, makt eller vold mot personer eller eiendom, i et forsøk på å legge press på landets myndigheter, befolkning eller samfunnet for øvrig for å oppnå politiske, religiøse eller ideologiske mål.

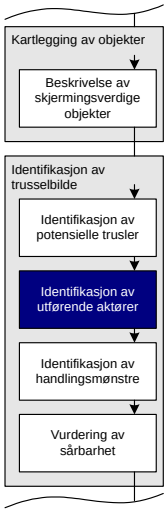
Tabell 2.2. Eksempler på potensielle trusler.

Potensielle trusler	
Datavirus	Endring av informasjon
Kompromittering av informasjon	EMP[1] og HPM[2]
Monitorering av nettverk	Bombeattentat
Avlytting ved hjelp av TEMPEST[3]	Påført strømbrudd
Telefonavlytting	Påført driftsstans
Innbrudd	Ryktespredning
Tyveri av informasjon	Brannstifting
Tyveri av utstyr og inventar	Hærverk
Hacking	Eliminering eller skadepåføring av personell

[1] En elektromagnetisk puls (EMP) er et bredbåndet, kortvarig utbrudd av elektromagnetisk energi med høy intensitet. Det elektromagnetiske feltet som oppstår, kan virke forstyrrende eller ødeleggende på elektronisk utstyr.

[2] I den senere tid er det utviklet utstyr som kan sende ut mikrobølger med meget høy effekt, High Power Microwave (HPM). Pulsens energimengde avhenger av kilden, men kan så stor at betydelige ødeleggelser kan forekomme på elektronisk utstyr.

[3] Elektromagnetisk stråling fra telekommunikasjons- og dataprosesseringsutstyr kan inneholde informasjon som kan fanges opp ved bruk av dertil egnet utstyr. TEMPEST betegner studiet av og kontrollen med denne kompromitterende utstrålingen.



2.6.2 Identifikasjon av utførende aktører

På basis av de identifiserte truslene i foregående punkt skal arbeidsgruppen identifisere såkalt utførende aktør. Utførende aktør kan være enkeltpersoner, grupper eller organisasjoner i samfunnet som har kapasitet og intensjon til å realisere trusselen. Identifikasjon av utførende aktør gjennomføres gjennom en idédugnad ved å stille spørsmålet *"Hvem har kapasitet og intensjon til å realisere trusselen?"*.

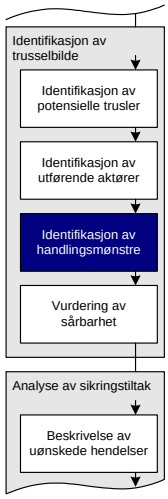
Bruk av en sjekkliste kan også i dette punktet være til hjelp. Eksempler på utførende aktører er gitt i Tabell 2.3. Denne listen er ikke komplett, og kun ment som et forslag til en sjekkliste. Hvilke aktører som velges, vil være avhengig av virksomheten eller de deler av virksomheten som analyseres.

Tabell 2.3. Eksempler på utførende aktør.

Utførende aktører	
Datakriminelle	Industri
Besøkende	Fremmed etterretning
"Pøbel"	Stoffmisbrukere
Innleid personell	Personer påvirket av alkohol
Egne ansatte	Utro tjener
Vinningsforbrytere	Fremmede makter eller organisasjoner

Etter hvert som arbeidsgruppen identifiserer utførende aktør for de ulike truslene, føres disse inn i T-skjemaet (Figur 2.5) under kolonnen "Utførende aktør". Hver trussel kan ha flere ulike typer utførende aktør. Tilsvarende som ved identifikasjonen av trusler, kan arbeidsgruppen dokumentere at en aktør er vurdert, men sette et "÷"-tegn i kolonnen til høyre for å markere at det ikke vil bli arbeidet videre med denne aktøren.

2.6.3 Identifikasjon av handlingsmønstre

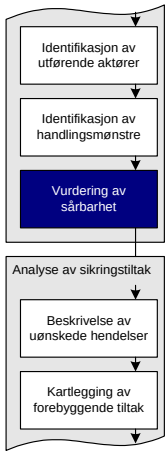


Når utførende aktør er identifisert, må det vurderes hvordan utførende aktør vil utføre trusselen. Arbeidsgruppen identifiserer derfor hvilke potensielle handlingsmønstre som utførende aktør kan tenkes å følge. Et utgangspunkt er å stille spørsmålet: *"Hvordan ville du som utførende aktør gå til verks?"*.

Mulige handlingsmønstre føres inn i T-skjemaet (Figur 2.5) under kolonnen "Handlingsmønster". Hvert handlingsmønster får et nummer av typen *Objekt.Trusselnummer.Handlingsmønsternummer*. De ulike handlingsmønstrene under hver trussel gis fortløpende numre. Eksempelvis får det første handlingsmønsteret under trussel *2.3* nummeret *2.3.1*.

Også her kan arbeidsgruppen filtrere bort uaktuelle handlingsmønstre ved å sette et "÷"-tegn i kolonnen til høyre.

2.6.4 Vurdering av sårbarhet



For hvert handlingsmønster skal arbeidsgruppen analysere systemet for å identifisere svakheter som svekker eller begrenser muligheten til å hindre at det aktuelle handlingsmønsteret blir utført. Slike svakheter kan eksempelvis være en ulåst dør eller en PC uten passordbeskyttelse.

I tillegg identifiseres svakheter som kan hindre eller begrense virksomhetens mulighet til skadereduksjon og normalisering etter at en uønsket hendelse har inntruffet, for eksempel mangel på brannslukningsutstyr eller nødaggregat.

De enkelte svakhetene føres inn i T-skjemaet (Figur 2.5) under kolonnen "Svakheter", til høyre for de aktuelle handlingsmønstrene.



2.7 Utfylling av skjema ”Analyse av sikringstiltak” (S-skjema)

Når trusselbildet er identifisert, vendes fokus mot de eksisterende sikringstiltakene. For hvert handlingsmønster fra T-skjemaet fyller arbeidsgruppen ut ett skjema av typen ”Analyse av sikringstiltak”.

Som det foregående innledes også dette skjemaet med ”System”, ”Dato”, ”Utført av” og ”Revisjon”. I tillegg påføres nummer og navn på det aktuelle handlingsmønsteret, hentet fra kolonnen ”Handlingsmønster” i T-skjemaet.

Arbeidsgruppen oppsummerer først det aktuelle handlingsmønsteret. Dette er en beskrivelse av handlingsmønsteret av typen *hva*, *hvem*, *hvordan*, *hvorfor*, osv.

Eksisterende sikringstiltak i forbindelse med det aktuelle handlingsmønsteret skal så vurderes. Dette er tiltak virksomheten har innført for å redusere sannsynligheten for at handlingsmønsteret skal inntreffe, eller for å redusere eventuelle konsekvenser av dette. Eventuelle lovfestede minimumskrav setter også ofte retningslinjer for tiltak som virksomheten må innføre.

Sikringstiltakene deles inn i to grupper:

- *Forebyggende tiltak*: Begrenser mulighetene for at en uønsket hendelse skal inntreffe. Fokuserer på tidsrommet før hendelsen inntreffer.
- *Skadereduserende og normaliserende tiltak*: Begrenser skaden en uønsket hendelse påfører systemet, og bidrar til at systemet kommer tilbake til tilnærmet normal tilstand. Fokuserer på tidsrommet etter at en hendelse har inntruffet.

Tiltak i begge gruppene identifiseres og vurderes. Dersom arbeidsgruppen ser umiddelbare alternativer for nye tiltak, kommenteres dette.

Informasjonen nedtegnes i skjema ”Analyse av sikringstiltak”, som vist i Figur 2.6.

Analyse av sikringstiltak			Skjema nummer: S . .
System:	Dato:	Utført av:	Revisjon:
Handlingsmønster (nr. x.x.x, navn):			
Beskrivelse av den uønskede hendelsen:			
Eksisterende forebyggende tiltak:		Tilfredsstillende?	
Eksisterende skadereduserende og normaliserende tiltak:		Tilfredsstillende?	
Forslag til nye og endrede tiltak:			
Kommentar:			

Skjemanummerering

Analyse av sikringstiltak
"S-skjema"

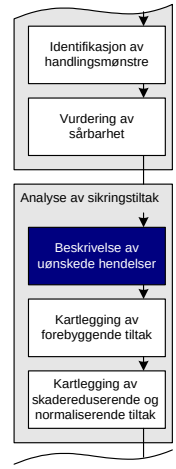
Skjemanummer:
"S"
+ objektnummer
+ trusselnummer
+ h.mønsternummer

Eksempel:
"S3.2.5"
(skjema for h.mønster 3.2.5)

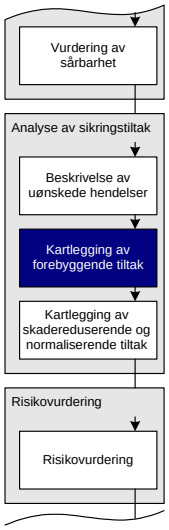
Figur 2.6. Skjema for analyse av sikringstiltak. Skjemaet er forminsket i forhold til original størrelse. Originalskjema er gitt i vedlegg A.

2.7.1 Beskrivelse av uønskede hendelser

Som et sammendrag av punktene i avsnitt 2.6, beskriver arbeidsgruppen hver enkelt uønsket hendelse. Dette er en beskrivelse av trusselen, den utførende aktøren, handlingsmønsteret og svakhetene i systemet. Beskrivelsen bør være så detaljert som mulig, og føres inn i S-skjemaet i rubrikken ”Beskrivelse av den uønskede hendelsen”.



Antall uønskede hendelser kan bli svært stort, og en del av disse vil kanskje virke meningsløse. Som tidligere påpekt er det derfor hensiktsmessig å filtrere bort uønskede hendelser som representerer svært lave risiki. Handlingsmønstre som har blitt markert med et "÷"-tegn på trusselbilde-skjemaet blir ikke inkludert videre i analysen.



2.7.2 Kartlegging av eksisterende forebyggende tiltak

I dette arbeidspunktet evaluerer arbeidsgruppen alle eksisterende forebyggende sikringstiltak som er etablert for å hindre realiseringen av en gitt trussel.

Ved kartlegging av de eksisterende forebyggende tiltakene, identifiserer arbeidsgruppen både fysiske tiltak (for eksempel en lås) og operasjonelle tiltak (for eksempel vakthold).

Arbeidsgruppen vurderer videre alle de identifiserte forebyggende tiltakene for å finne ut om disse er tilfredsstillende eller ikke. Vurderingen gjennomføres ved å betrakte de forebyggende tiltakenes grad av:

- beskyttende virkning
- detekterende virkning
- avskrekkende virkning

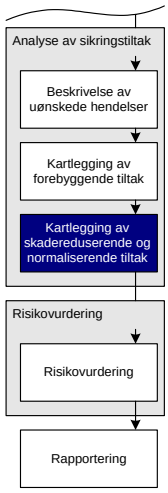
Mot enkelte trusler er det ofte satt i verk flere tiltak samtidig. Vurderingen av et aktuelt tiltak er ikke et svar på om det enkelte tiltaket alene er godt nok til å beskytte virksomheten. Om tiltaket er tilfredsstillende eller ikke, peker derimot på om det enkelte tiltaket er satt i verk på en tilfredsstillende måte, isolert sett. (For eksempel: Er backupen omfangsrik nok? Tas det backup ofte nok? Er backupinstruksen god nok? Her kan svarene være 'ja' selv om backup alene ikke er tilfredsstillende for å sikre seg mot tap av data.)

Samtidig er det viktig å gjøre en kost-nyttevurdering av de eksisterende tiltakene. Et kritikkverdig tiltak er normalt for dårlig, men i visse tilfeller kan et tiltak også være for bra eller rett og slett unødvendig. Det er viktig at analysen også fanger opp slike momenter slik at de tilmålte ressursene kan benyttes på en effektiv måte.

De forebyggende tiltakene som arbeidsgruppen har identifisert og analysert, føres inn i S-skjemaet i rubrikken ”Eksisterende forebyggende tiltak”. Evalueringen av tiltakene oppsummeres i rubrikken ”Tilfredsstillende?” ved å svare "Ja"/"Nei" i tillegg til en kommentar.

Når de eksisterende tiltakene identifiseres og evalueres, kommer det gjerne fram ideer om nye tiltak, eller mulige endringer av de eksisterende tiltakene. Dette kan arbeidsgruppen notere i rubrikken ”Forslag til nye og endrede tiltak”.

2.7.3 Kartlegging av skadereduserende og normaliserende tiltak



Arbeidsgruppen begynner nå på arbeidet med å identifisere og vurdere sikringstiltakene som fokuserer på perioden *etter* at en uønsket hendelse har blitt realisert.

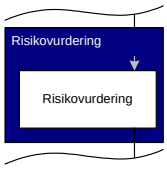
Slike tiltak kan deles inn i to grupper:

- tiltak for reduksjon av påført skade (skadereduserende)
- tiltak for å bringe systemet tilbake til normal tilstand (normaliserende)

Arbeidsgruppen kartlegger de eksisterende tiltakene i begge disse gruppene. Tiltakene evalueres, og det vurderes om de er tilfredsstillende eller ikke. Inkludert i dette er en kost-nyttevurdering for å se hvor effektive de eksisterende tiltakene er.

De skadereduserende og normaliserende tiltakene som arbeidsgruppen identifiserer, føres inn i S-skjemaet i rubrikken ”Eksisterende skadereduserende og normaliserende tiltak”. Evalueringen av tiltakene oppsummeres i rubrikken ”Tilfredsstillende?” ved å svare "Ja"/"Nei" i tillegg til en kommentar.

Igjen kan arbeidsgruppen notere forslag til nye og endrede tiltak, både skadereduserende og normaliserende, i rubrikken ”Forslag til nye og endrede tiltak”.



2.8 Utfylling av skjema ”Risikovurdering” (R-skjema)

I de to foregående skjemaene har trusler og sikringstiltak blitt evaluert. En ønsker nå å analysere konsekvens av og sannsynlighet for hvert handlingsmønster. Basert på informasjonen fra de foregående skjemaene vil en slik analyse gi et bilde av hvilken risiko systemet utsettes for.

For hvert handlingsmønster fra S-skjemaet vurderes sannsynligheten for at trusselen blir realisert i tillegg til den forventede konsekvensen. Informasjonen nedtegnes i skjema ”Risikovurdering”, som vist i Figur 2.7. Hvert R-skjema omhandler ett enkelt handlingsmønster. Når man først jobber med et handlingsmønster, vil det i mange tilfeller være hensiktsmessig å foreta en risikovurdering like etter. Det anbefales derfor at analysegruppen ferdigstiller både S- og R-skjema for det samme handlingsmønsteret, før arbeidsgruppen går over til å arbeide med neste handlingsmønster.

Som for det foregående skjemaet påføres systemets navn, dato, hvem analysen utføres av, revisjonsnummer, samt nummer og navn på handlingsmønsteret.

Risikovurdering | Skjema nummer: R . .

System:	Dato:	Utført av:	Revisjon:

Handlingsmønster (nr. x.x.x, navn):

Beskrivelse av konsekvens:

	Lite farlig	Farlig	Kritisk	Katastrofalt
Virksomheten				
Økonomi				
Anseelse				
Nasjonen				
Allierte				

Beskrivelse av sannsynlighet:

- ☐ Svært sannsynlig
- ☐ Meget sannsynlig
- ☐ Sannsynlig
- ☐ Lite sannsynlig

Kommentar:

Skjemanummerering

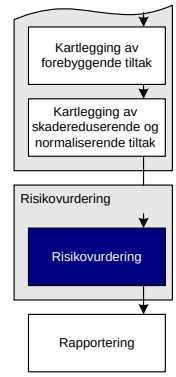
Risikovurdering
"R-skjema"

Skjemanummer:
"R"
+ objektnummer
+ trusselnummer
+ h.mønsternummer

Eksempel:
"R3.2.5"
(skjema for h.mønster 3.2.5)

Figur 2.7. Skjema for risikovurdering. Skjemaet er forminsket i forhold til original størrelse. Originalskjema er gitt i vedlegg A.

2.8.1 Risikovurdering



I selve analysens siste arbeidspunkt vurderer arbeidsgruppen hvilke konsekvenser en uønsket hendelse kan få, samt sannsynligheten for at hendelsen skal inntreffe.

Ved vurdering av konsekvens tar arbeidsgruppen utgangspunkt i det skjermingsverdige objektet som vurderes. Det bør tas hensyn til objektets funksjon, muligheter for erstatning, eventuelle reserveløsninger, og eksisterende skadereduserende og normaliserende tiltak. Vurderingen beskriver både umiddelbare konsekvenser og konsekvenser som først gir seg til kjenne etter en viss tid. Det er også viktig å vurdere eventuelle konsekvenser den uønskede hendelsen kan få for andre objekter. Eksempelvis kan tap av et objekts tilgjengelighet medføre at et annet objekt ikke lenger kan utøve sin funksjon. Et annet eksempel er et redundant system der to objekter kan utføre den samme

funksjonen. Tap av ett objekt kan ha ingen eller liten direkte konsekvens, men medføre at systemet kun stoler på det andre gjenlevende objektet. En bør i slike tilfeller vurdere konsekvensen av en hendelse utover den direkte konsekvensen, og vurdere hvilken tilstand systemet som helhet blir satt i. Arbeidsgruppen må derfor vurdere umiddelbare og forsinkede konsekvenser samt direkte og indirekte konsekvenser. Konsekvensvurderingen nedtegnes i rubrikken ”Beskrivelse av konsekvens” i R-skjemaet.

For å få et mer strukturert bilde av konsekvens kan det gjerne benyttes en matrise som vist i R-skjemaet i Figur 2.7. Her kan konsekvensen kategoriseres etter hvilke områder den uønskede hendelsen kan påvirke. For hvert område angis en tilhørende konsekvensgrad. De foreslåtte områdene er eksempler aktuelle for et militært anlegg, og må endres avhengig av systemet som analyseres. Andre eksempler kan være ”Miljø”, ”Personers liv og helse”, ”Virksomhetens operativitet”, ”Bedriftens konkurranseegenskaper”, ”Selskapets markedsandel”, og så videre. En kan på denne måten sette fokus på områder som er viktige i den enkelte analysen.

Konsekvensen kan kategoriseres etter *lite farlig*, *farlig*, *kritisk* og *katastrofalt*. Kategoriene kan byttes ut dersom arbeidsgruppen finner det hensiktsmessig. Det er også åpent for å innføre tre eller fem kategorier i motsetning til de foreslåtte fire. Konsekvenskategoriene bør på forhånd defineres slik at det eksisterer kriterier for hvilken konsekvens som tilsvarer de ulike kategoriene. Dersom det er mulig bør definisjonene inkludere ett eller flere måltall. Det bør defineres kriterier for alle de ulike konsekvens-områdene. Det henvises til kapittel 0 for eksempler på mulige kriterier.

Sannsynligheten for at den uønskede hendelsen skal bli realisert, evalueres basert på opplysninger om trusselbildet og de eksisterende forebyggende tiltakene. Vurderingen gjøres ved å se på sammenhenger mellom utførende aktør og den anstrengelse som er nødvendig for å kunne realisere en trussel. Forhold som bør betraktes er:

- motiv
- tilgjengelige muligheter
- ressurser og kompetanse utførende aktør besitter
- nødvendige ressurser og kompetanse for å realisere en trussel

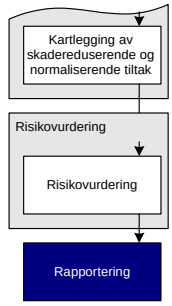
Arbeidsgruppa bør også se på hvor ofte det aktuelle handlingsmønsteret eller lignende handlingsmønstre har skjedd i løpet av virksomhetens eller tilsvarende virksomheters historie.

I tillegg til den mer detaljerte beskrivelsen av sannsynligheten, oppsummeres vurderingen av sannsynlighet med å kategorisere etter *lite sannsynlig*, *sannsynlig*, *meget sannsynlig*, og *svært sannsynlig*. Igjen påpekes det at kategoriene kan byttes ut dersom arbeidsgruppen finner det hensiktsmessig, eventuelt innføre tre eller fem kategorier i stedet for de foreslåtte fire. Tilsvarende som for konsekvenskategoriene bør det defineres kriterier for hva arbeidsgruppen mener med de ulike kategoriene. Kriteriene kan gjerne baseres på antall hendelser i løpet av et gitt tidsrom. Det henvises igjen til kapittel 0 for eksempler på mulige kriterier.

Vurderingen av sannsynlighet og konsekvens gjøres uten hensyn til de foreslåtte, nye tiltakene (som ennå ikke er satt i verk).

Sannsynlighetsvurderingen nedtegnes i rubrikken ”Beskrivelse av sannsynlighet” i R-skjemaet. Eventuelle kommentarer kan noteres i rubrikken ”Kommentar”.

2.9 Rapportering



I løpet av analysen har skjermingsverdige objekter blitt identifisert og evaluert i forhold til hvilke potensielle trusler de står ovenfor. Eksisterende sikringstiltak har blitt gjennomgått, og risikobildet hvert enkelt objekt står ovenfor har blitt oppsummert.

I de fleste tilfeller skal resultatene og erfaringene fra analysen rapporteres til ledelse, sikkerhetspersonell eller andre personer utenfor arbeidsgruppen, slik at analysearbeidet kan legge grunnlaget for styringen av det videre sikkerhetsarbeidet ved virksomheten. Rapporteringen bør være kortfattet og effektiv, men likevel viderebringe den nødvendige informasjonen.

Etter analysearbeidet sitter arbeidsgruppen hovedsakelig med følgende informasjon:

- Liste over skjermingsverdige objekter, vurdert med hensyn til funksjon, mulighet for erstatning, reserveløsninger og

sensitivitet, gradert etter den generelle betydningen for virksomheten.
- Trusselbildet som hvert objekt står ovenfor: Potensielle trusler, utførende aktører, handlingsmønstre og eksisterende svakheter utførende aktører kan dra nytte av.
- Identifikasjon og vurdering av eksisterende forebyggende tiltak i tillegg til eksisterende skadereduserende og normaliserende tiltak for hver uønsket hendelse med behov for videre analyse.
- Beskrivelse av konsekvens og sannsynlighet for hver uønsket hendelse med behov for videre analyse. Konsekvens har blitt vurdert i forhold til ulike områder.

Forslag til hvordan denne informasjonen kan presenteres er gitt nedenfor. Det finnes naturligvis flere alternativer for hvordan arbeidsgruppen kan formidle resultatene fra analysen. Rapporteringen må i hvert tilfelle vurderes i forhold til analysens målsetting, rapportens målgruppe, virksomhetens behov og ikke minst analyseresultatene. Det anbefales imidlertid at rapporten inneholder følgende informasjon (enkelte punkter blir forklart i neste avsnitt):

- Bakgrunn for analysen og dens målsetting.
- Systemets tilstand: Relativt kort oppsummering av den generelle sikkerheten.
- Risikomatriser (vist i Figur 2.8) for hvert konsekvensområde. Risikomatrisene kan inneholde handlingsmønstre knyttet til én enkelt trussel, ett enkelt analyseobjekt, flere analyseobjekter, eller systemet generelt. Detaljeringen av matrisene avhenger av analysens størrelse og hva analysegruppen ønsker å sette fokus på. Imidlertid kan det i de fleste tilfeller utarbeides egne risikomatriser for spesielt viktige objekter (klassifisert som *høy betydning*).
- Oppsummering av hendelser med *høy* og *middels* risiko. R- og S-skjema for de aktuelle handlingsmønstrene i tillegg til O-skjema for aktuelle objekter vedlegges. Oppsummeringen gir en oversikt over handlingsmønstre som medfører så stor risiko at tiltak straks bør iverksettes, eller at tiltak bør vurderes iverksatt.
- Vurdering av tiltak. Ikke tilfredsstillende tiltak listes opp og kommenteres. Tilsvarende påpekes arbeidsgruppens forslag til nye og endrede tiltak.
- Konklusjon.

Det er også en fordel om rapporten oppsummerer mer generelle forhold som organisering, interne prosedyrer og instrukser, ledelsens engasjement og ansvar, samt eksisterende og ønsket kompetanse innenfor sikkerhet.

Siden antall skjemaer i en analyse lett blir meget høyt, bør arbeidsgruppen vurdere om det er nødvendig å inkludere alle skjemaer i rapporten. En viss andel av skjemaene bør legges ved som vedlegg, men en komplett dokumentasjon (alle skjemaer og vurderinger) er sjelden nødvendig i en rapporteringssammenheng.

Som nevnt i avsnitt 2.4 bør virksomheten ha en bevisst holdning til regelmessig oppdatering av analyseresultatene. I rapporten kan analysegruppen gjerne påpeke en veiledende frist for utførelsen av en ny analyse, og anbefale løpende oppdateringer etter eventuelle mindre endringer som medfører mangler eller unøyaktigheter i de eksisterende analyseresultatene.

Igjen påpekes viktigheten av å skjerme informasjonen fra analysen. Om ikke dokumentasjonen fra analysen og rapporten gis den nødvendige gradering, kan den utførte risiko- og sårbarhetsanalysen føre til at virksomheten blir mer sårbar.

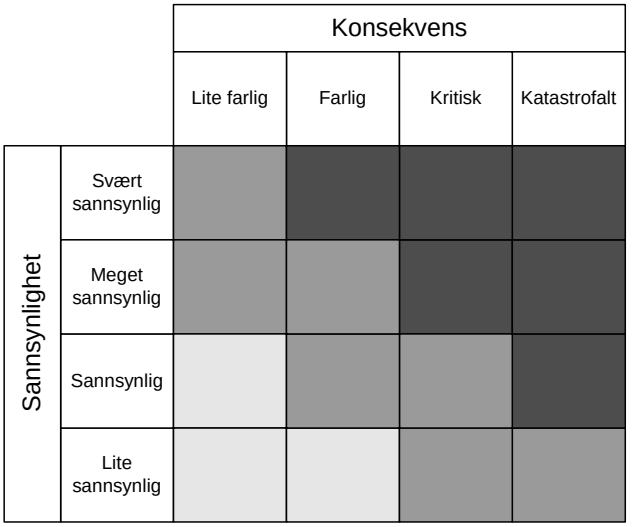
2.9.1 Presentasjonsmetoder

2.9.1.1 Risikomatrise

Risiko defineres gjerne som en funksjon av en uønsket hendelses sannsynlighet og konsekvens. Risikoen stiger i takt med økende sannsynlighet for hendelsen og økende konsekvens hendelsen kan medføre. En risikomatrise forsøker å illustrere risikoen knyttet til en hendelse ved å presentere sannsynlighet og konsekvens i en matrise. Et eksempel på en risikomatrise er gitt i Figur 2.8.

Uønskede hendelser plasseres i matrisen, og plasseringen avhenger av de vurderingene som er gjort i henhold til hendelsens konsekvens og sannsynlighet. Risikoen knyttet til en uønsket hendelse øker jo lenger til høyre og høyere opp i matrisen en uønsket hendelse plasseres. Matrisen benyttes hovedsakelig til å rangere ulike uønskede hendelser etter hvor stor risiko de medfører. Om ønskelig kan risikomatrisen i tillegg benyttes til å illustrere forskjellen i risiko med og uten sikringstiltak. Dette krever imidlertid at konsekvens og sannsynlighet

vurderes uten å ta sikringstiltak (nye eller eksisterende) i betraktning, noe som ikke blir gjort i den presenterte metodikken.



Figur 2.8. Risikomatrise. Risikoen øker til høyre og oppover i matrisen. Basert på et handlingsmønsters sannsynlighet og konsekvens, kan handlingsmønsteret plasseres i en av rubrikkene i matrisen. Risikomatrisen er delt inn i tre områder (□ lav, ▒ middels og ■ høy risiko) som enklere kan illustrere hvilken risiko en aktuell hendelse representerer.

Risikomatrisen deles gjerne inn i flere områder som beskriver ulik grad av risiko. Dette gjøres for enklere å illustrere risikoen knyttet til en hendelse og rangere dem mot hverandre, slik at det blir enklere å prioritere hvor risikoreduserende tiltak skal settes inn. For eksempel kan en risikomatrise deles inn i tre områder (som i Figur 2.8):

- *Høy risiko:* Risikoreduserende tiltak skal iverksettes umiddelbart.
- *Middels risiko:* Risikoreduserende tiltak skal vurderes.
- *Lav risiko:* Ikke nødvendig å iverksette risikoreduserende tiltak, så fremt ikke formelle krav til sikkerheten krever dette.

Hvor stort areal de forskjellige risikonivåene representerer i matrisen kan varierer fra analyse til analyse, og fra konsekvensområde til konsekvensområde. For eksempel kan arealet som representerer høy risiko (og umiddelbare tiltak) være definert større i matrisen for "Virksomheten" enn i matrisen for "Allierte".

Hvordan risikomatrisen benyttes vil være avhengig av den enkelte analysen. Antall handlingsmønstre som fylles inn i en enkelt matrise vil avhenge av analysens størrelse og organisering. En risikomatrise kan for eksempel inneholde alle hendelsene knyttet til én enkelt trussel, ett enkelt analyseobjekt, flere analyseobjekter, eller systemet generelt. Egne risikomatriser kan utarbeides for hvert konsekvensområde (jamfør områdene foreslått i R-skjemaet, Figur 2.7).

Kategoriene som er vist for konsekvens og sannsynlighet i Figur 2.8 er identiske med kategoriene foreslått i R-skjemaet. Disse kategoriene er ment som forslag og kan byttes ut dersom arbeidsgruppen finner det hensiktsmessig. Det er også åpent for å innføre tre eller fem kategorier for konsekvens og sannsynlighet i motsetning til de foreslåtte fire. Eventuelle endringer må i så fall gjøres i samsvar med endring av sannsynlighets- og konsekvenskategoriene i R-skjemaet.

Risikomatriser kan i tillegg benyttes for å gi en oppsummerende oversikt over systemets tilstand. Som et alternativ til å skrive inn handlingsmønsternummer i aktuelle rubrikker i matrisen, kan antallet handlingsmønstre som hører til hver rubrikk skrives inn i den aktuelle rubrikken. Det er særlig tre måter dette kan gjøres på:

- Én oppsummerende risikomatrise for hvert konsekvensområde. List opp antall handlingsmønstre i hver rubrikk. For eksempel 7 handlingsmønstre klassifiseres som *sannsynlig* og *kritisk* for virksomheten.
- Kun én oppsummerende risikomatrise. For alle konsekvensområdene summeres antallet handlingsmønstre i hver rubrikk i matrisen. For eksempel 13 handlingsmønstre klassifiseres som sannsynlig og kritisk totalt for virksomheten, økonomi, anseelse, nasjonen og allierte.
- Kun én oppsummerende risikomatrise. For alle handlingsmønstre velges den høyeste avkryssede konsekvensen. Risikomatrisen lages på grunnlag av handlingsmønstrenes oppgitte sannsynlighet og den høyeste avkryssede konsekvensen blant de fem kategoriene. For eksempel 16 handlingsmønstre klassifiseres som *sannsynlig* og med *kritisk* som den høyeste avkryssede konsekvensen.

2.9.1.2 Oppsummering av hendelser med høy og middels risiko

For at rapporten effektivt skal virke som et utgangspunkt for det videre arbeidet med sikkerheten, bør hendelsene i de høyeste risikokategoriene oppsummeres. Rapporten bør derfor inneholde en oversikt over hvilke hendelser som har blitt klassifisert under kategoriene *høy risiko* og *middels risiko*.

En enkel oppsummering kan være en tabell med oversikt over de aktuelle handlingsmønstrene med tilhørende objekt, trussel og utførende aktør. Et eksempel på et rammeverk for en slik tabell er gitt i Tabell 2.4. Hendelser klassifisert under *lav risiko* kan normalt utelates fra rapporten.

Tabell 2.4. Oppsummering av uønskede hendelser. Separate tabeller utarbeides for *høy risiko* og *middels risiko*.

Objekt (nr. x, navn)	Trussel (nr. x.x, navn)	Utførende aktør og handlingsmønster (nr. x.x.x, navn)

Som vedlegg til denne oversikten inkluderes S-skjema og R-skjema for de aktuelle handlingsmønstrene, samt O-skjema for de aktuelle objektene.

Tabellene over handlingsmønstre som medfører høy og middels risiko, gir leseren en oversikt over hvilke uønskede hendelser virksomheten står ovenfor. I forbindelse med det videre sikkerhetsarbeidet ligger S-, R- og O-skjemaene tilgjengelige som bakgrunnsinformasjon.

2.9.1.3 Vurdering av tiltak

Arbeidsgruppen har for hvert handlingsmønster vurdert eksisterende sikringstiltak, både forebyggende tiltak og skadereduserende og normaliserende tiltak. Tiltak som har blitt vurdert som ikke tilfredsstillende bør rapporteres slik at disse kan utbedres i forbindelse med det videre sikkerhetsarbeidet. En oppsummering over ikke tilfredsstillende tiltak kan gis i tabellform, som forslaget i Tabell 2.5.

Tilsvarende oppsummeringen av ikke tilfredsstillende tiltak bør også forslag til nye og endrede tiltak oppsummeres. Til dette kan det gjerne benyttes en tabell lik forslaget vist i Tabell 2.5.

Tabell 2.5. Oppsummering av ikke tilfredsstillende tiltak.

Tiltak	Beskrivelse

3 Brukerveiledning

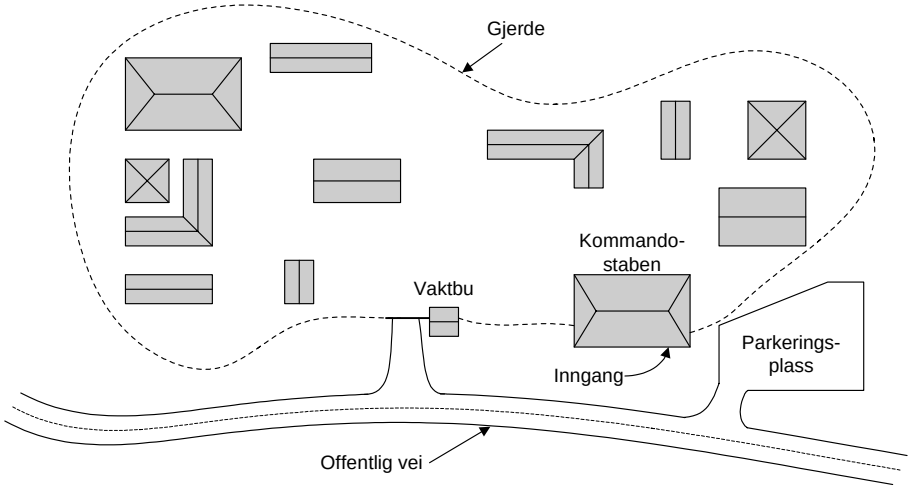
Dette kapittelet beskriver en brukerveiledning for metoden som er forklart i kapittel 2. Brukerveiledningen tar utgangspunkt i konkrete eksempler, og viser hvordan metoden kan anvendes i praksis.

Det vil først bli gitt en beskrivelse av virksomheten som skal analyseres, og deretter anvendes metoden slik den er beskrevet i kapittel 2. Virksomheten som blir analysert i denne rapporten er et tenkt tilfelle.

2.10 Beskrivelse av analyseobjektet

Virksomheten som skal gjennomføre en risiko- og sårbarhetsanalyse i denne brukerveiledningen er en avdeling innenfor Forsvaret. Avdelingen er en administrativ virksomhet med ca. 200 ansatte, og omfatter ledelse, IT-avdeling, teknisk avdeling, økonomiavdeling, personalavdeling, samt prosjektavdeling. I den videre beskrivelsen kalles virksomheten for ”Kommandostaben”.

Kommandostaben er en del av et større militært inngjerdet område med adgangskontroll og vaktmannskaper. Kommandostaben ligger på grensen mellom åpent og begrenset område. Det går en offentlig vei rett på utsiden av det militære området. Fra denne er det en avkjøring til parkeringsplassen for de ansatte i Kommandostaben. Figur 0.1 gir et oversiktsbilde over Kommandostaben og det militære området i tilknytning til Kommandostaben.



Figur 0.1. Oversiktsbilde av det militære området som Kommandostaben er en del av.

Kommandostaben har egen inngang på utsiden av det militære området. Inn- og utpassering i åpningstiden, dvs. mellom kl. 07.00 og 17.00, kontrolleres ved hjelp av resepsjonist og rotasjonsgrind med kortleser. Resepsjonistjobben betjenes av en vernepliktig soldat. Alle som skal inn i Kommandostaben, må ha eget nøkkelkort som benyttes i kortleseren. Området innenfor rotasjonsgrinden er begrenset område. Etter stengetid er Kommandostaben avlåst, og inn- og utpassering skjer da ved hjelp av nøkkelkortet og en firesifret kode. Besøkende til Kommandostaben registreres i resepsjonen, og må til enhver tid bære et besøkskort og være i følge med en av de ansatte.

Siden Kommandostaben er en avdeling i Forsvaret, oppbevares det sensitiv informasjon både i elektronisk form og i dokumentform. Informasjonen er gradert opp til HEMMELIG, og omfatter både nasjonal informasjon og NATO informasjon. Pr. 1.august 2000 ble det oppbevart 8 dokumenter gradert HEMMELIG og 40 dokumenter gradert KONFIDENSIELT. Oppbevaringen av informasjonen foregår etter de forskrifter som gjelder for de ulike graderingsnivåene. Dokumenter gradert HEMMELIG oppbevares i arkivet for HEMMELIGE dokumenter, som er sperret område. Datanettet er koplet opp for intern bruk, og har ingen eksterne linjer. Informasjon som ligger lagret på det interne datanettet, er ikke gradert høyere enn BEGRENSET. Det finnes PCer med eksterne linjer som er tilkoplet Internett, men disse er frittstående maskiner som ikke er koplet til det

interne datanettet. Det finnes også frittstående PCer for behandling av informasjon gradert opp til HEMMELIG.

Det foregår også noe sensitiv informasjonsflyt via datamaskin, telefon og faks, og kryptomateriell er derfor installert. Det er ikke etablert noen egen kryptoavdeling i Kommandostaben, men det er organisert en kryptosikkerhetsorganisasjon med kryptosikkerhetsleder og kryptoforvalter med stedfortredere. Kryptosikkerhetsleder skal blant annet sørge for opplæring av personell som arbeider med kryptomateriell, sørge for at slikt personell er kjent med instruksene til de kryptosystemene som er i bruk, og utarbeide en lokal kryptosikkerhetsinstruks. Kryptoforvalteren skal forvalte kryptomateriell ved Kommandostaben, og skal motta, oppbevare og behandle alt kryptomateriell for å hindre tap eller kompromittering. Han skal også føre kryptoregnskap, distribuere eller overføre kryptomateriell til autoriserte brukere, samt utføre tillintetgjøring og sende tillintetgjøringsrapporter i henhold til pålagte krav.

Som alle andre virksomheter er Kommandostaben avhengig av informasjonsteknologiske hjelpemidler. Det er derfor en egen IT-avdeling med en datasikkerhetsleder, en systemansvarlig og driftsansvarlige. Systemansvarlig har det overordnede ansvaret for at datasystemet fungerer. De driftsansvarlige tar seg av den daglige driften av IT-systemene, sørger for at systemene for backup fungerer, klargjør for nye brukere, og oppdaterer programvare. IT-avdelingen for øvrig driver blant annet med saksbehandling av saker knyttet til datasikkerhet, utfører sikkerhetsmessig godkjenning av datasystemer, underviser i datasikkerhet, utarbeider direktiver og veiledere, og rapporterer sikkerhetsbrudd.

Den tekniske avdelingen i Kommandostaben er relativt liten. Avdelingen har ansvaret for alle tekniske løsninger, slik som strømforsyning, vann og avløp, samt telefonnettet. Teknisk avdeling skal også sørge for at brannvern ivaretas, og derfor følge de branntekniske forskriftene som foreligger.

Økonomiavdelingen og personalavdelingen er stort sett sysselsatt med oppgaver knyttet til de ansatte i Kommandostaben. Økonomiavdelingen har ansvaret for lønn, reiseregninger og fakturering av regninger osv., mens personalavdelingen for eksempel tar seg av alle ansettelser, og oppbevarer derfor til dels store mengder sensitive personalopplysninger. Personalavdelingen fører også oversikt

over sikkerhetsklareringer og autoriseringer av personell, både av de ansatte i Kommandostaben, og av innleid prosjektpersonell.

Prosjektavdelingen er den største avdelingen i Kommandostaben. Prosjektavdelingen jobber både med interne og eksterne prosjekter av ulik art og størrelse. Noen prosjekter krever kompetanse utover det de ansatte i prosjektavdelingen har, og i slike tilfeller må den nødvendige kompetansen leies inn utenfra. Innleid personell må sikkerhetsklareres og autoriseres for å få adgang til Kommandostaben.

Kommandostaben oppfattes som en god arbeidsplass med et hyggelig arbeidsmiljø. Arbeidstakerne har god moral og nyansettelser eller oppsigelser i den faste staben er relativt sjeldne.

Kommandostaben har egen kantine. Dette tilbudet krever tilførsel av råvarer hver dag, og kantinen har en fast leverandør til dette formål. I tillegg er det satt ut drikkeautomater med kildevann flere steder i Kommandostaben. Det er derfor etablert en avtale med en leverandør av kildevann som en gang i uken fyller opp lageret for drikkevannsballonger.

Den øverste ledelsen for hele det militære området er lokalisert i Kommandostaben. Ledelsen har ansvaret for den daglige driften av både det militære området og Kommandostaben, samt å ivareta den totale sikkerheten. Sikkerhetsarbeidet ved Kommandostaben utføres gjennom kontinuerlige sikkerhetsvurderinger, og nå ønsker øverstkommanderende en vurdering av sikkerhetstilstanden i Kommandostaben med fokus på security. Han gir derfor sikkerhetssjefen ansvaret for å gjennomføre en risiko- og sårbarhetsanalyse av Kommandostaben.

2.11 Organisering av arbeidet

Sikkerhetssjefen har sikkerhetsfaglig utdanning, og mange års erfaring med gjennomføring av risiko- og sårbarhetsanalyser. Han er likevel avhengig av å ha med seg en tverrfaglig arbeidsgruppe med nødvendig kunnskap om Kommandostaben, og går derfor i gang med å sette sammen en arbeidsgruppe.

Etter et par dagers jobbing har sikkerhetssjefen klart å samle sammen en arbeidsgruppe der følgende avdelinger og fagområder er representert:

IT	IT-avdelingen er representert ved datasikkerhetslederen i Kommandostaben. Han har oversikt over datasystemene, og har gjennom sin stilling som datasikkerhetsleder ansvaret for at datasikkerheten ivaretas.
Personal	Personalavdelingens representant sitter inne med kunnskap knyttet til alle personalrelaterte problemer. Hun har oversikt over prosedyrer for lagring av personalopplysninger. Hun kjenner også til prosedyrer for sikkerhetssamtaler og autorisasjon.
Krypto	For å dekke problemstillinger knyttet til kryptosikkerhet er kryptosikkerhetslederen i Kommandostaben representert i arbeidsgruppen. Han kjenner sikkerhetsbestemmelsene for kryptotjenesten, og har god kunnskap om kryptomateriellet som benyttes.
Teknisk	Representanten fra den tekniske avdelingen har kjennskap til de tekniske løsningene for vann og avløp, strømforsyning, telefonnettet, samt det branntekniske systemet i Kommandostaben. Han kjenner også til typiske problemer knyttet til den tekniske driften av Kommandostaben.

Sikkerhetssjefen har identifisert tids- og ressursbehovet for analysen, og laget et økonomisk overslag for den totale kostnaden knyttet til analysen av Kommandostaben. De ulike ansvarsområdene fordeles grovt på de enkelte gruppemedlemmene. Det økonomiske overslaget, samt en oversikt over de ulike gruppemedlemmene, legger han fram for øverste sjef for godkjennelse slik at analysen kan starte.

2.12 Planlegging av analyse

Sikkerhetssjefen vil gjerne at gruppedeltakerne skal få forståelse for nødvendigheten av analysen, og foretar derfor planleggingen sammen med arbeidsgruppen.

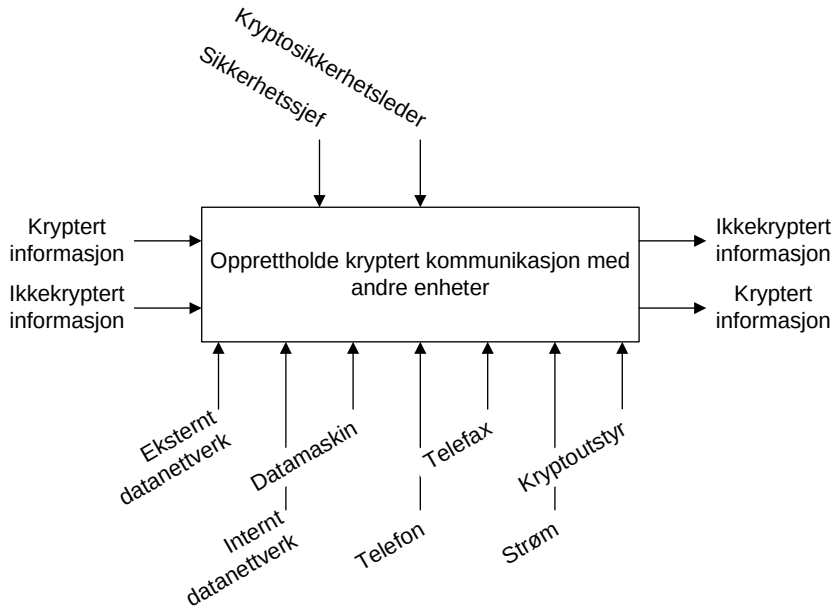
Sikkerhetssjefen forteller hvorfor analysen skal gjennomføres, og hva som er målsettingen med analysen. I dette tilfellet skal analysen gjennomføres fordi det er en del av det kontinuerlige sikkerhetsarbeidet ved Kommandostaben. Dette arbeidet har som overordnet målsetting å ivareta en tilfredsstillende sikkerhet ved anlegget, og etterse at minimumskrav til enhver tid er oppfylt. Målsettingen for analysen fastsettes til:

- En risiko- og sårbarhetsanalyse skal utføres i tråd med analysen foreslått i "Objekt og informasjonssikkerhet. Metode for risiko- og sårbarhetsanalyse".
- Sikkerheten til alle objekter innenfor Kommandostabens bygg som i fredstid har merkbar innvirkning på anleggets, nasjonens eller alliertes sikkerhet eller det norske forsvarets anseelse skal analyseres. Dette innebærer at alle objekter som er klassifisert til å ha *høy*, *middels* eller *lav* betydning skal analyseres. Inkludert i dette er all sikkerhetsgradert informasjon.
- Alle objekter som har betydning klassifisert som *middels* eller *høy* skal være analysert innen to måneder.
- Alle objekter skal være analysert innen fire måneder.
- Det skal kontrolleres at alle minimumskrav i lover og forskrifter er oppfylt.
- Kostnadseffektiviteten av iverksatte tiltak og eventuelt nye tiltak skal vurderes for å påse at avsatte ressurser blir benyttet på en best mulig måte.

Analysegruppen diskuterer seg fram til en begrensning av analysen og en detaljeringsgrad som virker hensiktsmessig i forhold til målsettingen og ressursene gruppen har til rådighet.

Når målsettingen og begrensningen av analysen er formulert, begynner arbeidsgruppen å beskrive Kommandostaben og dens funksjoner. Beskrivelsen som utformes blir en utvidelse av den som er gitt i avsnitt 2.10. En av funksjonene til prosjektavdelingen er å opprettholde kryptert kommunikasjon med andre enheter. Denne funksjonen er det kryptosikkerhetsleder som har best oversikt over. For å få oversikt og kunne formidle funksjonen til de andre på gruppen, tegner han et IDEF0-diagram som er gjengitt i Figur 0.2. Det tegnes også tilsvarende diagrammer for de andre funksjonene som Kommandostaben oppfyller.

Arbeidsgruppen blir enige om at resultatet fra analysen bør foreligge i rapportform med konklusjoner og eventuelle anbefalinger om nødvendige tiltak. De lager også en framdriftsplan for arbeidet som skal utføres. Framdriftsplanen er i henhold til det tids- og ressursbehovet som gjelder for analysen.



Figur 0.2. IDEF0-diagram for en av hovedfunksjonene til Kommandostaben.

2.13 Beskrivelse av skjermingsverdige objekter

Med utgangspunkt i begrensningen for analysen, som ble avklart under planleggingsarbeidet, begynner arbeidsgruppen å lage lister over objekter som skal analyseres. For å identifisere samtlige objekter som er relevante i forhold til analysen, benytter arbeidsgruppen flere IDEF0-diagrammer som lages ut fra funksjonene de ønsker opprettholdt. For hvert objekt fylles det ut ett O-skjema.

I funksjonen 'Opprettholde kryptert kommunikasjon med andre enheter' inngår objektene eksternt kryptonettverk, kryptoutstyr, PC, telefon og telefaks. PCen inneholder to harddisker. Den ene brukes til operativsystem og programvare og er fast montert i PCen. Den andre benyttes til lagring av data og er uttagbar. For å få utført kryptering og dekryptering, kobles PCen til en kryptomodul. Denne inneholder en type smartkort som virker som en nøkkel for å aktivere

kryptomodulen. Smartkortet kan og skal tas ut av PCen når det ikke er i bruk. Det skal da lagres på et sted som er godkjent for HEMMELIG. Det samme gjelder for harddisken som benyttes til lagring av data. En PC som er godkjent til denne typen bruk kalles PBS (PC basert brukersystem). Det er nødvendig med kryptoklarering grad 1 for å kunne hente ut smartkort og harddisk. Både kryptosikkerhetssjef og kryptoforvalter har denne klareringen. Det tas dobbel backup av harddisken i PBS en gang om dagen. De to kopiene legges i separate hvelv. PBS blir objekt nummer *14*, og O-skjemaet fylles ut som vist i Figur 0.3.

Det blir vurdert hvordan en skal beskrive strømforsyningen til Kommandostaben. Et forslag er å beskrive hver fordelingsboks for seg, men representanten for teknisk avdeling synes dette blir for detaljert i et O-skjema og ønsker å se på strømforsyningen til Kommandostaben som et generalisert objekt. Strømforsyningen blir objekt nummer *27*, og tilhørende skjema *O27* er gjengitt i Figur 0.4. Tilsvarende skjemaer som i Figur 0.3 og Figur 0.4 fylles ut for de andre objektene som inngår i analysen.

Beskrivelse av skjermingsverdig objekt			Skjema nummer: O 14
System: Kommandostaben	Dato: 26. mai 00	Utført av: IT ansvarlig H. Acker	Revisjon: A

Skjermingsverdig objekt eller informasjon (nr. x, navn):

14, PBS på rom 3.14

Daglig ansvarlig for objektets sikkerhet:

Kryptosikkerhetsleder K. Oden

Anvendelse eller funksjon:

Sende, lagre og motta kodet informasjon gradert til og med HEMMELIG til og fra andre militære enheter nasjonalt og internasjonalt.

Hvordan kan objektet eller informasjonen erstattes?	Kan erstattes innen:
PC godkjent som PBS kan anskaffes fra leverandør (Defence PC Systems). Dersom kryptoenhet og/eller smartkort forsvinner, kan nye enheter sendes fra kryptoavdelingen ved FO/S.	2 dager
	Erstatningskostnad: NOK 30 - 40.000

Beskrivelse av eksisterende reserveløsning(er):

PC på rom 2.71 har uttagbar harddisk og er ellers godkjent til bruk som PBS. Denne kan fungere som reserve ved å flytte den inn på rom 3.14 og koble den til nødvendig utstyr. PCen må da få installert ny kryptoenhet med tilhørende smartkort fra FO/S. Reserveløsningen vil være operativ innen en dag dersom kryptoutstyret fortsatt er tilgjengelig. Dersom både PC og kryptoutstyr er ødelagt eller forsvunnet, vil reserveløsningen være operativ innen to dager, som er lik tiden det normalt tar å erstatte det originale utstyret.

Sensitivitet

Ytterste konsekvens hvis tap av konfidensialitet:

Informasjonen som er lagret på harddisken er gradert opp til HEMMELIG. Følgelig kan det alvorlig skade Norge eller dets alliertes sikkerhet eller landets forhold til fremmede makter dersom informasjonen blir tilgjengelig for uautoriserte personer.

Ytterste konsekvens hvis tap av integritet:

Feilaktige beslutninger eller vurderinger på grunn av feilaktig eller ufullstendig informasjon på PBS. Mistenkelig informasjon vil normalt kunne dobbeltsjekkes. Informasjon som virker rimelig, men likevel er feilaktig, vil kunne gi grunnlag for vurderinger og beslutninger som i verste fall medfører tap av menneskeliv og/eller viktige ressurser.

Ytterste konsekvens hvis tap av tilgjengelighet:

Informasjon vil ikke kunne sendes, mottas eller hentes fram. Dette kan føre til forsinkelser samt feilaktige beslutninger og vurderinger. I fredstid vil imidlertid kosekvensene være begrensede i forhold til viktige ressurser og personellets sikkerhet.

Kommentar:	Objektets betydning:
Med PBS menes her et funksjonelt PC-basert brukersystem, dvs. PC med kryptoenhet, smartkort, en permanent og en uttagbar harddisk samt monitor. Andre perifere enheter inkluderes ikke.	☒ Høy ☐ Middels ☐ Lav ☐ Lav, ingen videre analyse

Figur 0.3. O-skjema for PC basert brukersystem (PBS).

Beskrivelse av skjermingsverdig objekt			Skjema nummer: O 27
System: Kommandostaben	Dato: 27. mai 00	Utført av: Teknisk assistent R.E. Parer	Revisjon: A

Skjermingsverdig objekt (nr. x, navn):

27, Strømforsyningen til Kommandostaben

Daglig ansvarlig for objektets sikkerhet:

Teknisk ansvarlig P. Ussopp

Anvendelse eller funksjon:

Drive elektrisk utstyr i Kommandostabens bygning.

Hvordan kan objektet eller informasjonen erstattes?

Ingen alternativer. Strømmen må komme tilbake igjen, enten fra samme eller alternativt kraftselskap, eller ved at eventuell feil på strømnettet repareres.

Kan erstattes innen:

Normalt innen 1 dag. Ved større skader innen 1 uke.

Erstatningskostnad:

NOK 0 - 50.000

Beskrivelse av eksisterende reserveløsning(er):

Aggregat i kjelleren kan brukes dersom strømstansen ikke har sitt opphav etter aggregatets innkoblingspunkt. Aggregatet kobles automatisk inn ved strømstans. Det vil følgelig ikke oppstå et merkbart avbrudd i strømtilførselen. Opplagret drivstoff er tilstrekkelig til to døgns uavbrutt drift. Utover denne perioden må drivstoff anskaffes og etterfylles.

Sensitivitet

Ytterste konsekvens hvis tap av konfidensialitet:

-

Ytterste konsekvens hvis tap av integritet:

Endringer i spenning eller frekvens kan medføre at elektrisk/elektronisk utstyr ødelegges. Dette kan særlig skade kryptoutstyr og PCer, noe som kan medføre nedsatt operabilitet i opptil en uke.

Ytterste konsekvens hvis tap av tilgjengelighet:

Elektrisk/elektronisk utstyr kan ikke benyttes. Dette medfører forsinkelser ved bruk av kommunikasjonsutstyr som ikke er batteridrevet. I tillegg fås generelt nedsatt operabilitet i den tiden strømmen er borte.

Kommentar:

Objektets betydning:

- ☐ Høy
- ☒ Middels
- ☐ Lav
- ☐ Lav, ingen videre analyse

Figur 0.4. O-skjema for strømtilførselen til Kommandostaben.

2.14 Identifikasjon av trusselbilde

Når arbeidsgruppen har fylt ut O-skjema for alle skjermingsverdige objekter, begynner de å sette opp lister over truslene mot disse. For å fokusere på de viktigste objektene først, sorteres objektene etter deres anslåtte betydning med de viktigste øverst. Deretter jobber arbeidsgruppen seg nedover i bunken.

2.14.1 Identifikasjon av potensielle trusler

Fra før har sikkerhetssjefen utarbeidet en sjekkliste over potensielle trusler mot virksomheten (tilsvarende **Tabell 2.2**). Istedet for å vise denne sjekklisten til arbeidsgruppen, setter han opp kategorier for trusler (tilsvarende **Tabell 2.1**) og gjennomfører en idédugnad rundt spørsmålet *"Hvilke trusler står de aktuelle objektene ovenfor?*". Når idédugnaden er ferdig, blir trusselbildet for hvert objekt utfylt med aktuelle trusler fra sjekklisten. Dette medfører at noen nye trusler kommer frem som sikkerhetssjefen ikke hadde på sjekklisten fra før. Sjekklisten oppdateres med disse truslene og bevares med tanke på neste gang en tilsvarende analyse skal gjennomføres.

Arbeidsgruppen kommer fram til at det kan være hensiktsmessig å skille mellom tyveri av PC og tyveri av kryptoutstyr siden dette kan ha totalt forskjellig konsekvens. Tyveri av PC kan medføre at harddisken blir stjålet, noe som betyr tyveri av informasjon. I så tilfelle må konsekvensene ved tyveri av informasjon også vurderes, ikke bare PCens kostnad og bruksverdi. Derfor velger arbeidsgruppen å betrakte tap av harddisk som tap av informasjon og ta hensyn til dette når de fyller ut S- og R-skjema ved tap av PC.

Arbeidsgruppen kommer fram til følgende trusler for PBS:

- Hacking
- Datavirus
- Monitorering av nettverk
- Avlytting ved bruk av TEMPEST
- Eliminering og skadepåføring av nøkkelpersonell
- Tyveri av kryptoutstyr
- Tyveri av PC
- Tyveri av informasjon
- Endring av informasjon
- Skade fra EMP eller HPM
- Bombeattentat

- Påført strømbrudd
- Brannstifting

Disse truslene føres inn i første kolonne i T-skjemaet *T14* der de gis fortløpende nummer på formen *14.x*. Et eksempel på hvordan et T-skjema kan fylles ut for PBS er vist i Figur 0.5. Merk at dette er et forenklet eksempel siden det finnes langt flere enn de to truslene som er vist i figuren. I tillegg er bare et utvalg aktører og handlingsmønstre inkludert. I eksempelet jobbes det kun videre med de to oppførte truslene.

2.14.2 Identifikasjon av utførende aktører

For hver trussel skal det nå identifiseres en eller flere utførende aktører. I likhet med identifikasjon av trusler, har sikkerhetssjefen en sjekkliste over mulige aktører. Før han viser denne sjekklisten til arbeidsgruppen, gjennomfører de en idédugnad rundt spørsmålet ”*Hvem har kapasitet og intensjon til å realisere trusselen?*”. Listen med kategorier over potensielle trusler benyttes som hjelp i prosessen. Etterpå oppdateres den tidligere sjekklisten og den nye listen med informasjon fra hverandre.

For trussel *14.2, Tyveri av kryptoutstyr*, velger arbeidsgruppen å skille mellom utro tjener/innleid personell og fremmed etterretning. Dette skyldes at de antar at fremmed etterretning vil ha større midler til disposisjon og mer profesjonelle framgangsmåter enn ansatte. I tillegg benytter de kategorien vinningsforbrytere. De vurderer det som lite trolig at en vinningsforbryter vil bryte seg inn på militært område for å stjele en PC, men vil likevel dokumentere at de har vurdert muligheten. Av den grunn skriver de opp vinningsforbrytere som mulig aktør og setter et "÷"-tegn i kolonnen til høyre. For trussel *14.1, Datavirus*, velger arbeidsgruppen å slå sammen alle typer datakriminelle (for eksempel ansatte, tilfeldige hackere og fremmed etterretning) siden deres framgangsmåter generelt sett vil være like. Aktørene føres inn i kolonnen ”Utførende aktør” i T-skjemaet (Figur 0.5).

2.14.3 Identifikasjon av handlingsmønstre og svakheter

For hver aktør identifiseres det nå ett eller flere handlingsmønstre. Sikkerhetssjefen ber deltakerne i arbeidsgruppen om å forsøke å tenke på samme måte som utførende aktør mest sannsynlig ville gjøre, og

stiller følgende spørsmål: ”*Hvordan ville du som utførende aktør gå til verks?*”. Handlingsmønstrene som kommer fram for PBS skrives inn i kolonnen ”Handlingsmønster” i T-skjemaet. For trussel *14.1* gis handlingsmønstrene fortløpende nummer på formen *14.1.x*. Tilsvarende gjelder for de andre truslene.

Arbeidsgruppen ønsker å inkludere muligheten for at brukere av PBS uforvarende legger virusinfiserte filer på datamaskinen, selv om dette per definisjon ikke er en tilsiktet handling.

For de ulike handlingsmønstrene identifiserer arbeidsgruppen også eventuelle svakheter, dvs. egenskaper som utførende aktør kan dra nytte av og dermed medvirke til at et handlingsmønster blir realisert, eller som kan hindre at systemet lar seg normalisere etter hendelsen. Disse svakhetene fylles inn i kolonnen ”Svakheter” i T-skjemaet.

Identifikasjon av trusselbilde			Skjema nummer: T 14 - a
System: Kommandostaben	Dato: 29. mai 2000	Utført av: IT ansvarlig H. Acker	Revisjon: A

Skjermingsverdig objekt (nr. x, navn):
14, PBS på rom 3.14

Trussel (nr. x.x, navn)		Utførende aktør		Handlingsmønster (nr. x.x.x, navn)		Svakheter
14.1, Datavirus		Datakriminelle		14.1.1, Datakriminelle bryter seg inn og planter datavirus lokalt på PBS.		
				14.1.2, Datakriminelle bruker eget eller tilegnet nøkkelkort og planter datavirus lokalt på PBS.		Ansatte/innleid personell misbruker, mister eller oppbevarer sitt nøkkelkort på et uforsvarlig sted. Mange ansatte/innleid personell har unødvendig adgang til rom 3.14. Dør kan åpnes uten kode.
				14.1.3, Datakriminelle tar seg inn på ulåst rom og planter datavirus lokalt på PBS.		Ansatte/innleid personell glemmer å låse rom 3.14.
				14.1.4, Datakriminelle bryter seg inn på PBS via datanettet og planter virus.		Eksterne tilkoblinger.
		Brukere av PBS		14.1.5, Brukere av PBS legger uforvarende infiserte filer på PBS (via datanett eller lagringsmedia).		Må stole på egne ansatte og andre som har brukerrettigheter på PBS. Mangelfulle datasikkerhetsinstrukser.
14.2, Tyveri av kryptoutstyr		Vinningsforbrytere	÷			
		Utro tjener/innleid personell		14.2.1, Utro tjener/innleid personell bryter seg inn på rom 3.14 og stjeler kryptoutstyr.		Brukere glemmer å fjerne smartkort etter bruk.
				14.2.2, Utro tjener/innleid personell tar seg inn på rom 3.14 ved bruk av eget eller tilegnet nøkkelkort og stjeler kryptoutstyr.		Ansatte/innleid personell misbruker, mister eller oppbevarer sitt nøkkelkort på et uforsvarlig sted. Mange ansatte/innleid personell har unødvendig adgang til rom 3.14. Dør kan åpnes uten kode. Brukere glemmer å fjerne smartkort etter bruk.
				14.2.3, Utro tjener/innleid personell stjeler kryptoutstyr fra ulåst rom 3.14.		Ansatte/innleid personell glemmer å låse rom 3.14. Brukere glemmer å fjerne smartkort etter bruk.

Kommentar:

Med "datakriminelle" menes alle som benytter maskinvare og/eller programvare til å utføre uautoriserte handlinger. Dette kan være tilfeldige besøkende, fremmed etterretning, utro tjener, innleid personell, vinningsforbrytere, organisasjoner, med flere.
Med "kryptoutstyr" menes kryptoenhet og smartkort.

Fortsettelse på skjema T14-b.

Figur 0.5. T-skjema for PBS. Dette er et forenklet eksempel og inneholder kun et lite utvalg av de trusler, aktører og handlingsmønstre som vil være aktuelle.

2.15 Analyse av sikringstiltak

Arbeidsgruppen benytter så informasjonen fra T-skjemaene til å gi en mer utførlig beskrivelse av handlingsmønstrene og deres tilhørende uønskede hendelser. Dette gjøres i S-skjemaet. Blant annet ble handlingsmønstrene *14.1.1* og *14.2.2* vurdert som sannsynlige nok til at de er verdt å jobbe videre med.

For alle aktuelle handlingsmønstre, finner arbeidsgruppen fram til alle eksisterende sikringstiltak og fører disse inn i S-skjemaene. Sikringstiltakene evalueres ved en kost-nytte vurdering, samt ved en vurdering av tiltakenes grad av beskyttende, detekterende og avskrekkende virkning. Resultatet av vurderingen for handlingsmønster *14.1.1, Datakriminelle bryter seg inn og planter datavirus lokalt på PBS* og *14.2.2, Utro tjener/innleid personell bryter seg inn på rom 3.14 ved bruk av eget eller tilegnet nøkkelkort og stjeler kryptoutstyr* er gjengitt i Figur 0.6 og Figur 0.7.

Det er verdt å merke seg at arbeidsgruppen vurderer sikringstiltaket ”Lås på dør til rom 3.14” forskjellig for hendelsene *14.1.1* og *14.2.2*. Dette skyldes at i *14.2.2* betraktes bruk av nøkkelkort, eget eller tilegnet, noe som medfører at bruk av pinkode blir av betydning. I *14.1.1* betraktes innbrudd uten bruk av nøkkelkort, noe som medfører at bruk av pinkode blir uinteressant.

Med hensyn til handlingsmønster *14.1.1* kommer arbeidsgruppen fram til at passordbeskyttelsen på PBS er for svak og lett å knekke. Arbeidsgruppen vurderer at en månedlig oppdatering av antivirusprogramvaren er for sjelden. De foreslår å foreta en automatisk oppdatering hver dag. Vinduene til rommet er fra før av ikke sikret med annet en vanlige vindushasper, noe som arbeidsgruppen ønsker å endre på. Et tiltak som arbeidsgruppen ikke vurderer som utilstrekkelig, men snarere overflødig, er dobbel backup av den uttagbare harddisken. De framlegger derfor forslag om å fjerne ordningen med dobbel backup. Disse forslagene fylles inn i rubrikken "Forslag til nye og endrede tiltak" i skjemaet *S14.1.1*. Tilsvarende utfyllinger gjøres for alle de andre nedtegnede handlingsmønstrene som vurderes sannsynlige nok til å arbeide videre med.

Analyse av sikringstiltak		Skjema nummer: S 14 . 1 . 1	
System: Kommandostaben	Dato: 29. mai 2000	Utført av: IT ansvarlig H. Acker	Revisjon: A

Handlingsmønster (nr. x.x.x, navn):

14.1.1, Datakriminelle bryter seg inn og planter datavirus lokalt på PBS.

Beskrivelse av den uønskede hendelsen:

Datakriminelle tar seg inn på rom 3.14 ved innbrudd. Innbrudd kan utføres ved å bryte opp inngangsdør eller vindu (vindu i tredje etasje, vender ut mot sivilt område).

Utro tjener eller innleid personell kan benytte seg av sine brukerrettigheter for å få adgang til PCen og dermed plante datavirus fra medbragte lagringsmedia (diskett, CD eller lignende). Datakriminelle uten brukerrettigheter eller utro tjener/innleid personell som ikke vil benytte egne brukerrettigheter, må bryte seg gjennom brukernavn/passordbeskyttelse.

Virus kan lagres på den permanente harddisken som sitter i PCen, og kan siden spres til den uttagbare harddisken med gradert informasjon.

Eksisterende forebyggende tiltak:	Tilfredsstillende?
- Sikkerhetssamtale med personer som autoriseres med brukerrettigheter.	- Ja.
- Lås på dør til rom 3.14.	- Ja, åpnes med adgangskort.
- Instrukser for fjerning av uttagbar harddisk med gradert informasjon etter bruk.	- Ja.
- Brukernavn/passordbeskyttelse av PBS.	- Nei, passordbeskyttelsen er for enkel.

Eksisterende skadereduserende og normaliserende tiltak:	Tilfredsstillende?
- Backup av lagret informasjon.	- Ja, men ikke kostnadseffektivt. Backup utføres daglig, kopieres og de to kopiene legges i separate hvelv.
- Antivirusprogramvare.	- Nei, dårlig oppdatering (hver måned).
- Periodisk viruskontroll med antivirusprogramvare.	- Ja, fast kontroll hver dag, samt dynamisk beskyttelse.
- PC på rom 2.71 kan benyttes som reserveløsning (se O14).	- Ja.

Forslag til nye og endrede tiltak:

- Brukernavn/passordbeskyttelsen på PBS bør forbedres.
- Backup av lagret informasjon på PBS blir hver dag kopiert, og de to kopiene lagres i separate hvelv. Det antas som forsvarlig og mer kostnadeffektivt å kun oppbevare en kopi av backupen.
- Antivirusprogramvaren bør oppdateres hver dag (kan gjøres automatisk).
- Sikring av vindu på rom 3.14 med alarm og kraftigere lås.

Kommentar:

Med "datakriminelle" menes alle som benytter maskinvare og/eller programvare til å utføre uautoriserte handlinger. Dette kan være tilfeldige besøkende, fremmed etterretning, utro tjener, innleid personell, vinningsforbrytere, organisasjoner, med flere.

Figur 0.6. S-skjema for handlingsmønster *14.1.1*.

Analyse av sikringstiltak			Skjema nummer: S 14 . 2 . 2
System: Kommandostaben	Dato: 29. mai 2000	Utført av: IT ansvarlig H. Acker	Revisjon: A

Handlingsmønster (nr. x.x.x, navn):

14.2.2, Utro tjener/innleid personell tar seg inn på rom 3.14 ved bruk av eget eller tilegnet nøkkelkort og stjeler kryptoutstyr.

Beskrivelse av den uønskede hendelsen:

Utro tjener/innleid personell benytter eget nøkkelkort eller tilegner seg et annet nøkkelkort og tar seg inn på rom 3.14. Kryptoutstyr (smartkort og/eller kryptoenhet) blir fjernet fra rommet. Kryptoenheten oppbevares til en hver tid på rom 3.14, mens smartkortet normalt fjernes fra rom 3.14 etter at brukeren av PBS er ferdig med oppgaven. Når brukere forlater rommet ved mindre pauser forekommer det imidlertid at kun døren til rom 3.14 blir låst, og smartkortet forblir på rommet.
Sikkerheten er avhengig av hvor forsvarlig smartkortet blir oppbevart, hvordan innehavere av nøkkelkort oppbevarer disse, samt hvor fort nøkkelkortene blir deaktivert ved eventuelle tap. Rutiner som sikrer at nøkkelkort blir deaktivert så fort de blir savnet, eksisterer ikke. Mange ansatte og innleid personell har unødvendig adgang til rom 3.14. Dette medfører økt sannsynlighet for at utro tjener/innleid personell i utgangspunktet har nødvendige rettigheter, samt økt sannsynlighet for at et tilegnet nøkkelkort har de nødvendige rettighetene. Et tilegnet nøkkelkort med riktige rettigheter kan benyttes uten pinkode.

Eksisterende forebyggende tiltak:	Tilfredsstillende?
- Sikkerhetssamtale med personer som skal ansettes eller jobbe midlertidig ved Kommandostaben. - Lås på dør til rom 3.14.	- Ja. - Nei, kun nøkkelkort er nødvendig (ikke kode).

Eksisterende skadereduserende og normaliserende tiltak:	Tilfredsstillende?
- Rutine for å deaktivere stjålet smartkort. - Rutine for å fjerne smartkort fra rom 3.14 etter bruk og oppbevare dette i hvelv.	- Ja, kontroll av smartkort hver dag. - Nei, smartkortet fjernes normalt ikke dersom brukeren er borte fra rom 3.14 for kun en kort periode.

Forslag til nye og endrede tiltak:

- Adgangskontroll til rom 3.14 forsterkes slik at det i tillegg til nøkkelkort blir nødvendig med adgangskode.
- Adgang til rom 3.14 gis kun til de personene som har reelle og nødvendige arbeidsoppgaver på rom 3.14.
- Sett i verk rutiner slik at tapte nøkkelkort blir deaktivert så fort som mulig etter tapet.
- Forbedre rutinene for fjerning av smartkort fra rom 3.14. Smartkortet bør fjernes fra rommet og oppbevares i hvelv hver gang brukeren forlater rommet.

Kommentar:

Figur 0.7. S-skjema for handlingsmønster *14.2.2*.

2.16 Vurdering av konsekvens og sannsynlighet

Arbeidsgruppen har nå beskrevet eksisterende sikringstiltak, og er klare til å starte med risikovurdering av de uønskede hendelsene. Dette gjøres ved at de vurderer hvilke konsekvenser hendelsene kan få, samt hvor sannsynlig det er at de inntreffer. Sikkerhetssjefen påpeker at det er viktig at arbeidsgruppen tar hensyn til eksisterende sikringstiltak ved disse vurderingene.

Sikkerhetssjefen anbefaler at de benytter fire konsekvenskategorier og fem konsekvensområder. Han spesifiserer hva de enkelte kategoriene skal kalles og kommer med et forslag til hva de skal bety for hvert område. Han lager en oversikt som vist i Tabell 0.1.

For sannsynlighet anbefaler sikkerhetssjefen at de benytter fire kategorier basert på frekvens (antall hendelser over et gitt tidsrom). Hva de kalles og hva de betyr lister han opp som vist i Tabell 0.2.

Med utgangspunkt i Tabell 0.1 begynner arbeidsgruppen å vurdere konsekvenser for hver enkelt hendelse. Konsekvensene av hendelsene vurderes med tanke på alle de fem områdene og beskrives i detalj i R-skjemaer. I tillegg foretas en beskrivelse av sannsynligheten for at hver enkelt hendelse skal inntreffe. Beskrivelsen oppsummeres ved å krysse av for en valgt sannsynlighetskategori.

For hendelsene *14.1.1* og *14.2.2* fylles R-skjemaene ut som vist i Figur 0.8 og Figur 0.9.

Tabell 0.1. Konsekvenskategorier.

	Lite farlig	Farlig	Kritisk	Katastrofalt
Virksomheten	Ingen påvirkning	Redusert operativitet inntil en dag	Redusert operativitet inntil en uke	Bortfall av operativitet mer enn en uke
Økonomi	Inntil NOK 50.000	Inntil NOK 500.000	Inntil NOK 5.000.000	Over NOK 5.000.000
Allmenn anseelse	Påvirker ikke troverdighet og respekt	Svekket troverdighet og respekt	Betydelig svekket troverdighet og respekt	All troverdighet og respekt borte
Nasjonen	Ingen påvirkning	Redusert operativitet, kan skade rikets sikkerhet	Betydelig redusert operativitet, kan skade rikets sikkerhet alvorlig	Satt ut av spill, kan få avgjørende følger for rikets sikkerhet
Allierte	Ingen påvirkning	Kan skade alliertes sikkerhet	Kan alvorlig skade alliertes sikkerhet	Kan få helt avgjørende følger for alliertes sikkerhet

Tabell 0.2. Sannsynlighetskategorier.

Kategori	Forklaring
Lite sannsynlig	Mindre enn en hendelse hvert 10. år
Sannsynlig	Mellom en hendelse hvert år og en hendelse hvert 10. år
Meget sannsynlig	Mellom en hendelse hvert år og en hendelse hver måned
Svært sannsynlig	Mer enn en hendelse hver måned

Risikovurdering			Skjema nummer: R 14 . 1 . 1
System: Kommandostaben	Dato: 29. mai 2000	Utført av: IT ansvarlig H. Acker	Revisjon: A

Handlingsmønster (nr. x.x.x, navn):

14.1.1, Datakriminelle bryter seg inn og planter datavirus lokalt på PBS.

Beskrivelse av konsekvens:

Virus blir plantet på PBS og kan derfor skade informasjon og programvare som ligger både lokalt på PBS og på datanettet ved at viruset sprer seg. Antivirusprogramvaren sørger normalt for at viruset oppdages og elimineres, men nye virus vil ha muligheten til å trenge gjennom viruskontrollen. Selv om harddisken med gradert informasjon fjernes fra maskinen når den ikke er i bruk, kan virus legges inn på den permanente harddisken og spres videre ved senere bruk.

Konfidensialitet vil normalt ikke kunne bli truet siden datanettet er lukket for uvedkommende (krever smartkort og kryptoenhet for å lese gradert informasjon), men integriteten og tilgjengeligheten av informasjon og programvare kan tapes. Etter at skaden er oppdaget kan det gå opp til ett døgn før skaden er rettet opp ved hjelp av backup. PBS vil i denne tiden være utilgjengelig eller ha svekket operabilitet. Backuprutiner sørger for at ikke mer enn en dags arbeid med informasjon og programvare lagret lokalt blir ødelagt.

Anseelse vil kunne bli svekket, særlig dersom viruset sprer seg til andre nasjonale eller internasjonale militære enheter.

Konsekvenser ovenfor nasjonen eller allierte anses ikke som signifikant ettersom andre anlegg følger gjeldende sikkerhetsrutiner og utfører regelmessig backup.

	Lite farlig	Farlig	Kritisk	Katastrofalt
Virksomheten		X		
Økonomi	X			
Anseelse		X		
Nasjonen	X			
Allierte	X			

Beskrivelse av sannsynlighet:

Sjansen for at utro tjenere eller innleid personell skal bryte seg inn på rom 3.14 anses som liten på grunn av grundig sikkerhetsklarering.

Innbrudd av utenforstående kan utføres ved å bryte seg inn gjennom døren eller vinduet. Døren er beskyttet med godkjent nøkkelkortlås. For at døren til rom 3.14 skal kunne benyttes, må vedkommende først komme seg inn i kommandostab-bygget og opp i tredje etasje. Innbrudd via døren til rom 3.14 anses derfor som lite sannsynlig. Imidlertid synes vinduet relativt dårlig beskyttet, da en fra sivilt område kan klatre opp med en stige og bryte seg inn gjennom vinduet. Vinduet er ikke tilkoblet alarm, og er ikke låst utenom vanlige vindushasper.

For å plante virus lokalt på PBS må uvedkommende bryte seg gjennom brukernavn/passordbeskyttelse. Passordbeskyttelsen er imidlertid et relativt enkelt system som uvedkommende med gode datakunnskaper kan bryte gjennom. Eventuelt kan uvedkommende dra nytte av at den forrige brukeren ikke har logget seg ut.

- ☐ Svært sannsynlig
- ☐ Meget sannsynlig
- ☒ Sannsynlig
- ☐ Lite sannsynlig

Kommentar:

Figur 0.8. R-skjema for handlingsmønster *14.1.1*.

Risikovurdering			Skjema nummer: V 14 . 2 . 2
System: Kommandostaben	Dato: 29. mai 2000	Utført av: IT ansvarlig H. Acker	Revisjon: A

Handlingsmønster (nr. x.x.x, navn):

14.2.2, Utro tjener/innleid personell tar seg inn på rom 3.14 ved bruk av eget eller tilegnet nøkkelkort og stjeler kryptoutstyr.

Beskrivelse av konsekvens:

Dersom et smartkort blir meldt stjålet deaktiveres kortet slik at innehaveren(e) ikke er i stand til å sende eller lese kodet informasjon. Rutiner ved kommandostaben sørger for at det hver dag blir kontrollert at smartkortet er forsvarlig oppbevart eller i autorisert bruk. Smartkortet kan derfor kun bli uautorisert benyttet i underkant av en dag. Konsekvensene blir derfor at uvedkommende kan sende eller lese kodet informasjon gradert opp til HEMMELIG i underkant av en dag. Selv om tidsperioden er begrenset, kan dette få alvorlige konsekvenser.

Tyveri av kun kryptoenhet anses som mindre farlig da denne ikke kan benyttes uten et smartkort.

Ved tap av smartkort og/eller kryptoenhet må disse erstattes. Dette gjøres relativt enkelt fra kryptoavdelingen på FO/S, men det kan ta opp til to dager før nytt utstyr er operativt.

	Lite farlig	Farlig	Kritisk	Katastrofalt
Virksomheten			X	
Økonomi		X		
Anseelse			X	
Nasjonen			X	
Allierte			X	

Beskrivelse av sannsynlighet:

På grunn av grundige rutiner for sikkerhetsklarering anses mulighetene for at utro tjener eller innleid personell skal misbruke sine privilegier som små. I tillegg oppbevares normalt smartkortet i hvelv når det ikke er i autorisert bruk. Selv om smartkortet i visse tilfeller forblir på rom 3.14 ved kortere pauser i pågående arbeid, anses likevel sannsynligheten for at en ansatt eller annet personell skal benytte muligheten som liten.

- ☐ Svært sannsynlig
- ☐ Meget sannsynlig
- ☐ Sannsynlig
- ☒ Lite sannsynlig

Kommentar:

Figur 0.9. R-skjema for handlingsmønster *14.2.2*.

2.17 Rapportering

Når vurderingen av konsekvens og sannsynlighet er ferdig, er det klart for å få en oversikt over resultatene fra analysen, og rapportere disse.

Arbeidsgruppen velger å benytte risikomatriser i stor grad i rapporteringen. Sikkerhetssjefen anbefaler å dele risikokategoriene inn som vist i Tabell 0.3.

Tabell 0.3. Risikokategorier

Kategori	Forklaring
Høy risiko	Risikoreduserende tiltak skal iverksettes umiddelbart
Middels risiko	Risikoreduserende tiltak skal vurderes
Lav risiko	Ikke nødvendig å iverksette risikoreduserende tiltak, så fremt ikke formelle krav til sikkerheten krever dette.

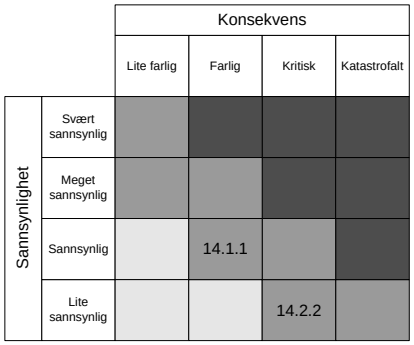
Som innledende del av rapporten skriver sikkerhetssjefen en kort beskrivelse av hva som var hensikten med analysen og gjengir dens målsetting som gitt i avsnitt 2.12. Han lar hvert medlem av analysegruppen kort beskrive deres inntrykk av sikkerheten ved Kommandostaben. Deretter setter han de ulike utkastene sammen til et dokument som beskriver analysegruppens generelle inntrykk av sikkerheten.

For å sette tall på og grafisk framstille Kommandostabens sikkerhetstilstand, lager analysegruppen en sammensatt risikomatrise for hver av de fem konsekvensområdene. I hver rute i disse matrisene står det totale antall hendelser som hører til i ruten. Et eksempel på hvordan denne kunne sett ut for området *nasjonen* er vist i Figur 0.10. Her inngår hendelse *14.1.1* blant de 43 hendelsene som er sannsynlige og lite farlige. Hendelse *14.2.2* inngår blant de 15 hendelsene som er lite sannsynlige og kritiske. Det framgår av Figur 0.10 at det er 28 identifiserte uønskede hendelser som har *høy risiko*, 150 med *middels risiko* og 155 med *lav risiko*.

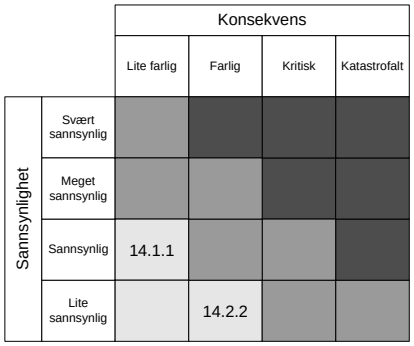
		Konsekvens			
		Lite farlig	Farlig	Kritisk	Katastrofalt
Sannsynlighet	Svært sannsynlig	22	9	1	2
	Meget sannsynlig	27	19	5	4
	Sannsynlig	43	34	21	7
	Lite sannsynlig	87	25	15	12

Figur 0.10. Samlet risiko for hele Kommandostaben for konsekvensområdet *nasjonen*. I tillegg til de to eksemplene med handlingsmønster *14.1.1* og *14.2.2* har eksempeldata blitt satt inn i matrisen for å illustrere hvordan matrisen kan se ut etter en komplett analyse.

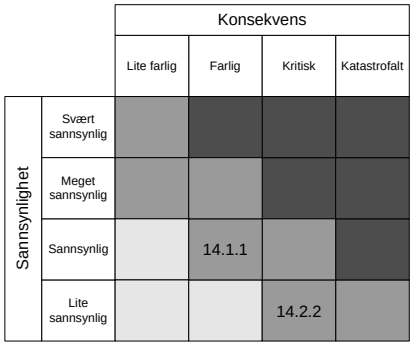
Arbeidsgruppen velger videre å sette opp risikomatriser for de fem konsekvensområdene for hver enkelt avdeling i Kommandostaben. I risikomatrisenes ruter fylles handlingsnummer inn. Dersom det blir for mange hendelser i forhold til rutestørrelsen i noen av rutene, skrives det istedenfor i de rutene antall hendelser som inngår samt en henvisning til en liste over alle hendelsene som hører til i rutene. For enkelte viktige objekter lages det egne risikomatriser. Her benyttes objektet PBS for å vise et eksempel på hvordan risikomatriser kan fylles ut. I Figur 0.11 til Figur 0.15 er det vist risikomatriser for hendelsene som er knyttet til PBS. I virkeligheten ville flere hendelser blitt analysert og presentert, men her blir bare de hendelsene som er gjennomgått i eksempelet inkludert.



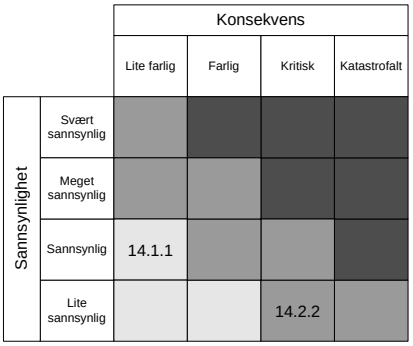
Figur 0.11. Risikomatrise for uønskede hendelser knyttet til virksomheten.



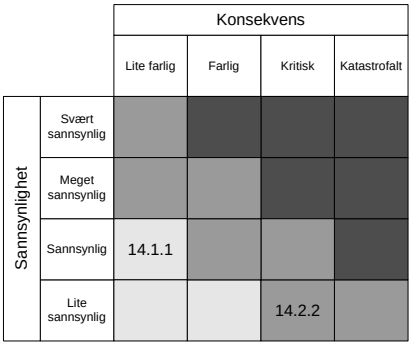
Figur 0.12. Risikomatrise for uønskede hendelser knyttet til økonomi.



Figur 0.13. Risikomatrise for uønskede hendelser knyttet til allmenn anseelse.



Figur 0.14. Risikomatrise for uønskede hendelser knyttet til nasjonen.



Figur 0.15. Risikomatrise for uønskede hendelser knyttet til de allierte.

I rapporten inkluderes også en tabell over uønskede hendelser klassifisert under kategorien *høy risiko* og en tilsvarende tabell under kategorien *middels risiko*. Siden det kun er to hendelser som er gjennomgått i eksempelet og begge faller under *middels risiko*, inkluderes kun disse to i Tabell 0.4.

Som vedlegg til de to tabellene følger alle aktuelle R-, S- og O-skjema. Tabellene brukes som oversikt over handlingsmønstre som medfører så stor risiko at tiltak må iverksettes umiddelbart (*høy risiko*) eller at tiltak bør vurderes iverksatt (*middels risiko*).

Tabell 0.4. Oppsummering av uønskede hendelser klassifisert under kategorien *middels risiko*. Risikoreduserende tiltak skal vurderes.

Objekt (nr. x, navn)	Trussel (nr. x.x, navn)	Utførende aktør og handlingsmønster (nr. x.x.x, navn)
14, PBS på rom 3.14	14.1, Datavirus	14.1.1, Datakriminelle bryter seg inn og planter datavirus lokalt på PBS.
	14.2, Tyveri av kryptoutstyr	14.2.2, Utro tjener/innleid personell tar seg inn på rom 3.14 ved bruk av eget eller tilegnet nøkkelkort og stjeler kryptoutstyr.

Tabell 0.5: Oppsummering av tiltak som ikke er tilfredsstillende.

Tiltak	Beskrivelse
Brukernavn/passordbeskyttelse av PBS.	Passordbeskyttelsen er for enkel. Dagens passordbeskyttelse bør analyseres og utbedres.
Antivirusprogramvare på PBS.	Programvaren oppdateres for sjelden (hver måned). Signaturfiler bør oppdateres hver dag (dette kan gjøres automatisk).
Lås på dør til rom 3.14.	Låsen er tilfredsstillende med hensyn på fysisk innbrudd, men for å bedre sikringen mot misbruk av nøkkelkort, bør kode bli nødvendig for å åpne døren.
Rutine for å fjerne smartkort fra rom 3.14 etter bruk og oppbevare dette i hvelv.	Det forekommer at brukere av PBS (rom 3.14) lar smartkortet forbli på rommet når brukeren forlater rommet for en kort periode. Rutinene bør forbedres slik at hver gang en bruker av PBS forlater rommet fjernes smartkortet og oppbevares i hvelv, selv om brukeren forlater rommet for kun en kort periode.

Rapporten avsluttes med en oppsummerende konklusjon og forslag til videreføring av arbeidet. Arbeidsgruppen påpeker at det bør gjennomføres en ny analyse innen tre år, men ved større endringer av sikkerhetsmessig betydning ved Kommandostaben, bør analysen oppdateres.

Rapporten stemples HEMMELIG grunnet sin svært sensitive informasjon og leveres til øverstkommanderende ved Kommandostaben.

3 Konklusjon og anbefalinger

Nasjonale virksomheter og organisasjoner retter fokus mot framtidige konsepter for risikohåndtering, og behovet for overgangen fra en regelbasert sikkerhetstjeneste til en risikobasert tilnærming står sentralt.

Risiko- og sårbarhetsforskningen står sterkt i Norge, og det finnes mange retningslinjer og metoder for risiko- og sårbarhetsanalyse, både nasjonalt og internasjonalt. Imidlertid er arbeidet som er lagt ned innenfor risiko- og sårbarhetsforskningen, og de retningslinjer og metoder som foreligger for risiko- og sårbarhetsanalyser, i all hovedsak rettet mot safety. Det er hittil lagt lite vekt på security-delen av sikkerhet.

Metoden som dokumenteres i denne rapporten er utviklet for analyse av objekt- og informasjonssikkerhet med fokus på de forhold som råder innenfor security. Metoden er generell, og kan anvendes uavhengig av hvilke systemer og objekter som skal analyseres.

Brukerveiledningen som er utarbeidet tar utgangspunkt i en oppdiktet virksomhet. Veiledningen viser gjennom et konkret eksempel hvordan metoden kan anvendes steg for steg, og hvordan skjemaene fylles ut.

Det er utarbeidet en oversikt over sentrale begreper og definisjoner. Denne oversikten kan forhåpentligvis bidra til økt forståelse og forbedret kommunikasjon i arbeidet med risiko- og sårbarhetsanalyser.

Metoden inneholder to sjekklister. Den ene sjekklisten omfatter ulike trusler som kan ramme en virksomhet, mens den andre gir oversikt over ulike typer av utførende aktører. Sjekklister er generelt anvendbare, og kan bidra til å kartlegge trusselbildet mot en virksomhet. Sjekklistene i denne rapporten er imidlertid satt opp som et forslag, og det anbefales derfor å jobbe videre med komplettering av sjekklistene.

Denne rapporten anses å være en omfattende dokumentasjon av den presenterte analysemetoden. Som en første introduksjon til en analysemetode, bør en kortere veileder bli utarbeidet. Rapporten er ment som bakgrunnsdokumentasjon til en slik veileder som på sikt vil gis ut av Direktoratet for sivilt beredskap (DSB).

En risiko- og sårbarhetsanalyse utført etter den presenterte metoden, vil i de fleste tilfeller medføre et høyt antall utfylte skjemaer. Under utarbeidelsen av metoden har kravet om fyldig dokumentasjon etter en risiko- og sårbarhetsanalyse stått sentralt. På grunn av metodens detaljeringsgrad og skjemabaserte struktur, bør det derfor utvikles programvare for behandling av informasjonen som framkommer under analysen. En slik programvare kan forenkle innskriving, søking, framhenting og rapportering av informasjon.

Fra pågående forskning innenfor risiko og sårbarhet kommer det med jevne mellomrom nye ideer om hvordan risiko- og sårbarhetsanalyser kan utføres. Det anses som en fordel at det opprettes en faggruppe som kan stå for videreutvikling og oppfølging av en allment akseptert analysemetode. En slik faggruppe kan for eksempel forankres i miljøet ved Institutt for produksjons- og kvalitetsteknikk (IPK) ved NTNU hvor det i dag finnes gode ressurser innenfor fagfeltet risiko og sårbarhet.

Referanser

Beskyttelsesinstruksen (1988), Statens fellesblankett X-0076B, fastsatt ved kgl.res. av 17. mars 1972 og trådte i kraft fra 1. juli 1972, endret ved kgl.res. av 14. mai 1982 og 7. oktober 1988

Critical Foundations (1997), *Protecting America's Infrastructure, The Report of the President's Commission on Critical Infrastructure Protection*, Washington DC

Dataforeningen i Sverige (1997), *SBA-metoden*, http://www.dfs.se/sba.htm

Datatilsynet (1998), *Veiledning i risikoanalyse av informasjonssystem*, TV-201

Direktoratet for sivilt beredskap (1994), *Veileder for kommunale risiko- og sårbarhetsanalyser*

Evensen, Vidar (2000), *Metode for analyse av informasjonssikkerhet og objektsikkerhet*, Institutt for produksjons- og kvalitetsteknikk, NTNU, Trondheim

Forsvarets forskningsinstitutt (1997), *Beskyttelse av samfunnet (BAS) : sluttrapport*, Kjeller

Forsvarets forskningsinstitutt (1999), *Beskyttelse av samfunnet med vekt på offentlig telekommunikasjon*, Kjeller

Forsvarets Overkommando/Sikkerhetsstaben (1998), *Datasikkerhetsdirektivet, Direktiv for sikring av datasystemer gradert etter Sikkerhetsinstruksen eller Beskyttelsesinstruksen*

Government of Canada (1996a), *A Guide to Security Risk Management for Information Technology Systems*, Communications Security Establishment, Ontario, Canada

Government of Canada (1996b), *A Guide to Risk Assessment and Safeguard Selection for Information Technology Systems*, Communications Security Establishment, Ontario, Canada

Government of Canada (1996c), *A Guide to Certification and Accreditation of Information Technology Systems*, Communications Security Establishment, Ontario, Canada

Hovden, Jan (1998), *Sikkerhetsforskning, en utredning for Norges forskningsråd*, NTNU, Trondheim

Idsø, Einar S. og Jakobsen, Øyvind M. (2000), Objekt- og informasjonssikkerhet. Metode for risiko- og sårbarhetsanalyse, Institutt for produksjons- og kvalitetsteknikk, NTNU, Trondheim

National Institute of Standards and Technology (1993), *Federal Information Processing Standards Publication 183: Announcing the standard for Integration Definition for Function Modeling (IDEF0)*

NATO (1999), *Fundamental review of NATO security policy - CM(55)15 Final, Enclosure C, The NATO Security Risk Management Process*

Norges offentlige utredninger nr. 12 (1986), *Datateknikk og samfunnets sårbarhet*, Forbruker- og administrasjonsdepartementet, Universitetsforlaget A/S

Norges Standardiseringsforbund, *Norsk Standard 5814, Krav til risikoanalyser*, 1. utg 1991

Næringslivets sikkerhetsorganisasjon (1998), *Faghefte 3, Risikoanalyse*

Næringslivets sikkerhetsorganisasjon (2000), *Faghefte 23, Dokumentsikkerhet - Sikker behandling av sensitive dokumenter*

Ot prp nr. 12 (1997-98), *Om lov om forebyggende sikkerhetstjeneste (sikkerhetsloven), Forsvarsdepartementet*

Överstyrelsen för civil beredskap (2000), *Infrastrukturoppdraget*, Stockholm, Sverige

Programstyret for risiko- og sårbarhetsforskning (1997), Norges forskningsråd, *Risikostyring Helse, miljø og sikkerhet, En kort innføring i risikostyring i din virksomhet*, Tapir forlag, Trondheim

Royal Canadian Mounted Police (1994), *Guide to Threat and Risk Assessment for Information Technology*, Information Technology Security Branch

The Engineering Council (1993), *Guidelines on Risk Issues*, London, England

A Sentrale begreper og definisjoner

Integritet
Informasjon og objekters nøyaktighet og fullstendighet, samt pålitelighet av transaksjoner.

Intensjon
Personers eller organisasjoners vilje og motivasjon til å realisere en trussel.

Kapasitet
De ressurser og den kompetanse som er nødvendig for å realisere en trussel.

Kompromittering
Når det ikke kan utelukkes tap av konfidensialitet, integritet eller tilgjengelighet for skjermingsverdig objekt eller sikkerhetsgradert informasjon.

Konfidensialitet
Det at informasjonen ikke er tilgjengelig for uautoriserte personer eller ikke-godkjente systemer (Forsvarets Overkommando/Sikkerhetsstaben, 1998).

Konsekvens
Mulig følge av en uønsket hendelse. Konsekvenser kan uttrykkes med ord eller som en tallverdi for omfanget av skader på informasjon/objekter (Norsk Standard 5814).

Objekt
Materiell, utstyr, personell, informasjon, infrastruktur og andre verdier.

Risiko
Uttrykk for den fare som uønskede hendelser representerer for informasjon/objekter av skjermingsverdig karakter. Risikoen uttrykkes ved sannsynligheten for og konsekvensene av de uønskede hendelsene (Norsk Standard 5814).

Risikoanalyse
En systematisk gjennomgang av et system i den hensikt å beregne systemets evne til å motstå trusler ved å identifisere trusler og kvantifisere risiko.

Safety
Sikkerhet mot uønskede hendelser som opptrer som følge av en eller flere tilfeldigheter.

Security
Sikkerhet mot uønskede hendelser som er et resultat av overlegg og planlegging.

Sårbarhet
En svakhet som reduserer eller begrenser et systems evne til å motstå en uønsket hendelse, eller til å gjenopprette en ny stabil tilstand etter hendelsen har inntruffet.

Sårbarhetsanalyse
En systematisk gjennomgang av et system i den hensikt å beregne systemets evne til å motstå trusler og overleve uønskede hendelser, ved å identifisere trusler, kvantifisere risiko og evaluere evne til stabilisering av systemet.

Tilgjengelighet
Tilgang til objekter, tjenester og informasjon ved behov og uten unødvendig forsinkelse.

Trussel
Ethvert forhold eller enhver enhet med potensiale til å forårsake en uønsket hendelse.

Utførende aktør
En person, organisasjon eller et objekt som ønsker og er i stand til å utløse en uønsket hendelse.

Uønsket hendelse
Den første signifikante avvikssituasjonen som har potensialet til å true sikkerheten til et objekt eller informasjon.

Tilsiktede handlinger
Handlinger som er planlagte og utført med overlegg.

B Systembeskrivelse

Ofte vil det å beskrive et system være en stor og tung oppgave. Det er mange faktorer som er viktige når en skal foreta en slik beskrivelse. For det første må en avgrense systemet, både i bredde og i dybde. Denne avgrensningen må gjøres så vid at den dekker hele systemet og dets relevante omgivelser, men den bør samtidig være så smal at det ikke blir unødvendig store arbeidsmengder i forhold til utbyttet av beskrivelsen.

Når en har beskrevet et system på en hensiktsmessig måte, oppnås en modell som kan kommuniseres til andre. Det blir enklere, både for en selv og for andre, å se helheten i systemet, men også å se sammenhengene mellom de enkelte delene som systemet består av. Erfaring viser at det kan være en fordel å gjøre en god innsats under systembeskrivelsen for å lette det videre arbeidet. Det tar selvsagt lengre tid før selve analysearbeidet kommer i gang, men på den annen side vil dette arbeidet kunne utføres med større effektivitet og kvalitet enn uten en god systembeskrivelse.

En god systembeskrivelse bør kunne besvare i minste fall følgende tre spørsmål:

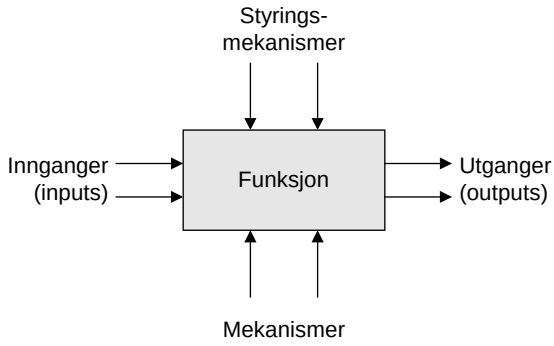
- Hva er systemet avhengig av for å funksjonere (input)?
- Hvilke funksjoner og oppgaver utføres av systemet?
- Hvilke tjenester eller produkter leverer system (output)?

I de følgende underkapitlene vil noen kjente og velbrukte metoder bli presentert.

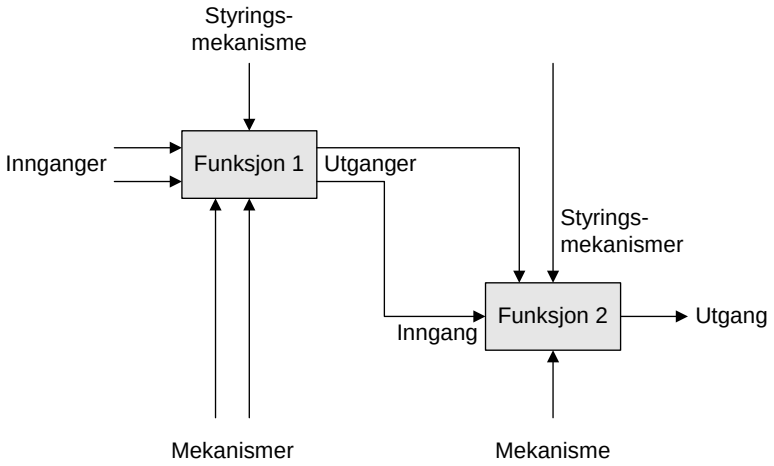
B.1 IDEF0

IDEF (Integration Definition for Function Modeling) er en metode som ble designet for å modellere avgjørelser, handlinger og aktiviteter i en organisasjon eller et system. Metoden er en avlegger av det grafiske språket Structured Analysis and Design Technique (SADT). IDEF ble til ved at United States Air Force ga de opprinnelige utviklerne av SADT i oppgave å utvikle en metode for funksjonsmodellering som kan brukes til analyse og kommunisering av funksjonene til et system. IDEF består av to modelleringstyper: IDEF0 omhandler prosesser og IDEF1 omhandler data. IDEF0 er hensiktsmessig å benytte for å etablere omfanget av en analyse, særlig funksjonsanalyse. Metoden hjelper analytikeren til å identifisere forutsetningene for at en funksjon

skal kunne utføres, samt hva som er resultatet av funksjonen. Enkle grafiske symboler forenkler beslutningstaking og letter involvering av flere parter på alle nivå innenfor organisasjonen.



Figur B.1. En grunnleggende IDEF0-celle med innganger, styringsmekanismer, mekanismer og utganger.



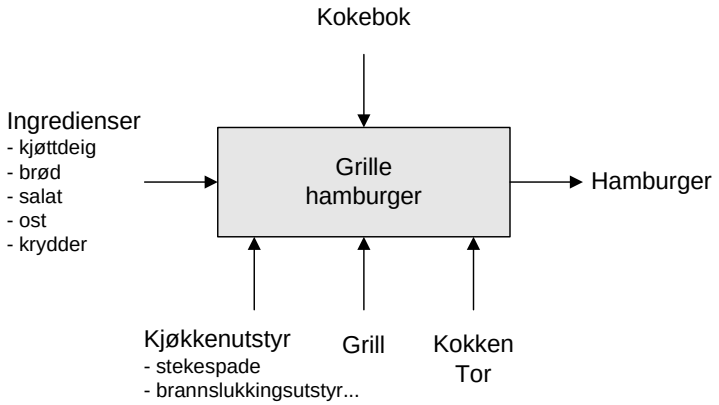
Figur B.2. Sammenkobling av IDEF0-celler.

IDEF0 benytter enkle diagrammer basert på bokser og piler. Boksene symboliserer funksjonene mens grensesnittet til og fra funksjonene indikeres med piler til og fra boksene. Overordnede funksjoner kan deles opp i mindre funksjoner og en kan følgelig oppnå et hierarki av bokser som indikerer funksjoner på ulike detaljeringsnivå. En funksjonsboks med tilhørende piler kalles gjerne for en celle. Pilene og boksene påsettes merkelapper som gir en indikasjon om hva den enkelte boks eller pil er. En grunnleggende IDEF0 celle er vist i Figur

B.1. For funksjoner som er avhengige av andre funksjoner, indikeres koblingene med piler. Cellene tegnes vanligvis diagonalt fra øverste venstre hjørne til nederste høyre hjørne som vist i Figur B.2.

Prosesser har normalt tre faktorer som influerer på funksjonen. Den mest grunnleggende faktoren er materialer og data som indikeres ved piler fra venstre inn i boksen. For at prosessen eller funksjonen skal få starte eller opprettholde aktivitet, trengs styringssignaler. Disse kan være alt fra mekaniske brytere til underskrifter fra en ansvarlig person. Styringssignaler indikeres ved piler til toppen av boksen. I tillegg trengs også andre mekanismer som utstyr og arbeidskraft. Disse mekanismene indikeres ved piler til bunnen av boksen. Resultatet eller resultatene av en funksjon eller prosess indikeres med en pil ut fra boksens høyre side. Disse resultatene kan igjen benyttes som inngang eller styringssignal for en annen prosess.

Et banalt, men illustrerende eksempel er vist i figur B.3.



Figur B.3. Et enkelt eksempel på bruk av IDEF0 for funksjonen "Grille hamburger".

Ved bruk av IDEF0 benyttes følgende retningslinjer:

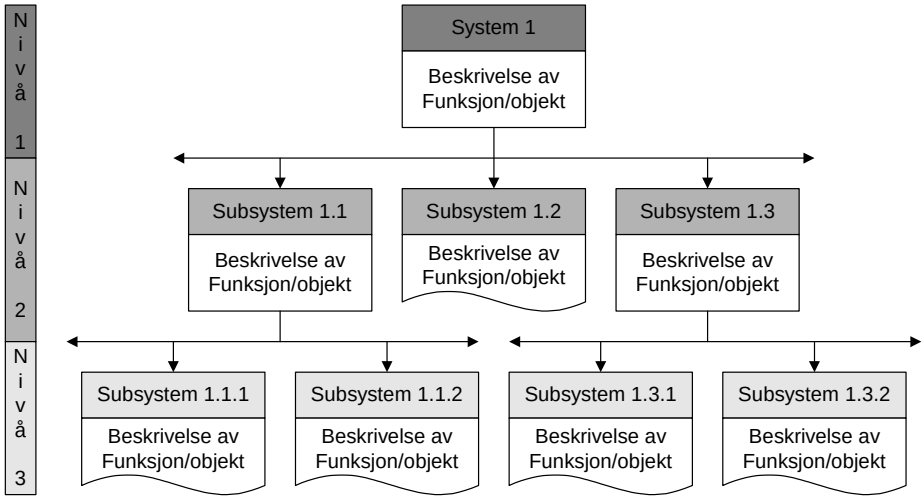
- Hver merkelapp skal være unik, dvs. at det skal ikke forekomme duplikater av merkelappene.
- Dersom merkelappene som benyttes til å beskrive pilene eller boksene er upresise eller tvetydige, kan en benytte en ordbok som nærmere spesifiserer hva hver enkelt merkelapp betyr.

- Ved oppdeling av funksjoner i mindre underfunksjoner, benyttes generelt ikke mer enn seks underfunksjoner per overfunksjon. Dette gjøres for å lette lesbarheten.
- Alle funksjoner skal ha minst ett styringssignal.
- Styringssignaler og innganger må være klart adskilt.

For en mer detaljert beskrivelse av IDEF0 henvises det til National Institute of Standards and Technology (1993).

B.2 Hierarkisk nedbryting

Ofte vil en oppdage at det ikke er nødvendig med det relativt grundige analyseunderlaget som IDEF0 resulterer i. For å få en oversikt over funksjoner og generaliserte objekter, som for eksempel en bygning, kan det ofte være mer hensiktsmessig å benytte en enkel hierarkisk oppbygging. Grunntanken er at en starter med et overordnet system, objekt eller funksjon, og undersøker hvilke funksjoner og objekter som er underordnet dette. Denne prosessen gjentas for underliggende nivåer inntil en har oppnådd en tilfredsstillende detaljeringsgrad. Dette kalles gjerne topp-bunn tilnærming.

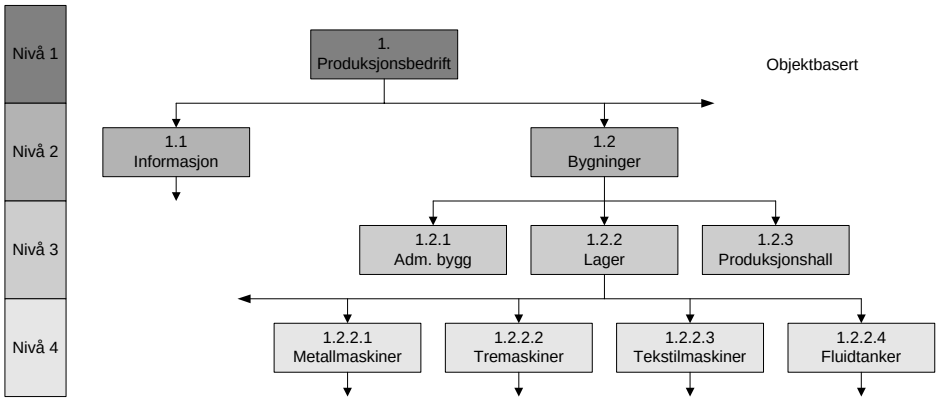


Figur B.4. Eksempel på en hierarkisk nedbryting av et objekt eller en funksjon. Merk at den hierarkiske nummereringen av de forskjellige subsystemene ikke har sammenheng med nummereringen av objekter, trusler og handlingsmønstre i beskrivelsen av risiko- og sårbarhetsanalysen.

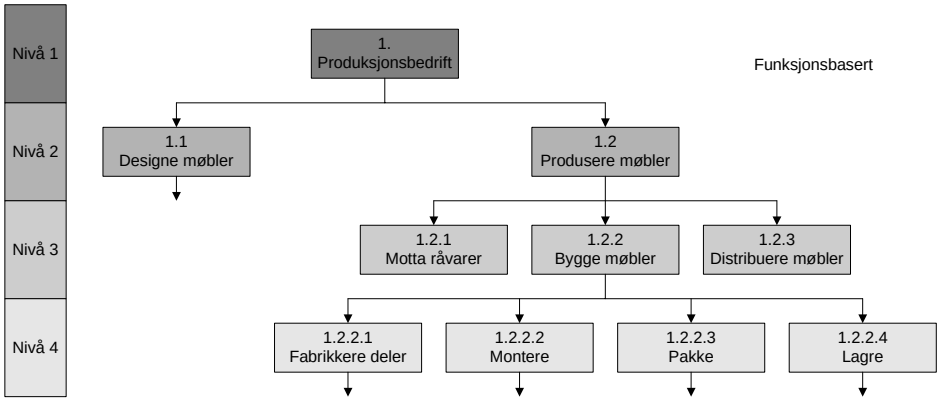
I enkelte tilfeller er det hensiktsmessig å fokusere på funksjon, mens det i andre tilfeller er mer hensiktsmessig å fokusere på objekt. I Figur B.4 er det illustrert hvordan et system kan tenkes inndelt i objekter som hvert har en funksjon. Det gjøres oppmerksom på at en hierarkisk oppbygging ikke er en formalisert metode, som for eksempel IDEF0, og metoden som benyttes her er bare et eksempel på hvordan det kan gjøres. Figuren illustrerer hvordan en starter med et overliggende system og dets funksjon. Deretter foretas en vurdering av hvilke objekter som er nødvendige for å opprettholde denne funksjonen. Disse objektenes funksjoner er igjen opprettholdelse av andre objekter. Figuren viser også at det ikke nødvendigvis kreves at en når samme detaljeringsnivå for hvert enkelt objekt, men at en kan stanse oppdelingen når en måtte ønske.

En diagram over et systems hierarkiske oppbygging vil kunne gi en god oversikt over analyseobjektet på en intuitiv og enkel måte. På grunn av diagrammets enkle struktur ligger det imidlertid begrensninger i fleksibiliteten. Et eksempel på en slik begrensning er at det i utgangspunktet ikke kan tas høyde for innvirkning mellom funksjoner og objekter på samme nivå. Dette kan imidlertid bøtes på ved å utføre små endringer i den grafiske representasjonen. For eksempel kan det innføres piler mellom funksjoner og objekter som har innvirkning på hverandre, der en forklaring på interaksjonen følger pilene.

Eksempeler på objektbasert og funksjonsbasert hierarkisk nedbryting av en produksjonsbedrift er gitt i henholdsvis Figur B.5 og Figur B.6.



Figur B.5. Eksempel på en noe forenklet objektbasert hierarkisk nedbryting av en produksjonsbedrift. Beskrivelser av hvert enkelt objekt er utelatt.



Figur B.6. Eksempel på en noe forenklet funksjonsbasert hierarkisk nedbryting av en produksjonsbedrift. Beskrivelser av hvert enkelt objekt er utelatt.

C Sikkerhetsgradering av informasjon

Sikkerhetsloven av 20. mars 1998 gir bestemmelser for behandling av dokumenter som av sikkerhetsmessige grunner må beskyttes. Disse bestemmelsene benyttes av militære og offentlige virksomheter, på fylkes- og kommunenivå, og i deler av industrien der sikkerhetsgradert informasjon utstedes og håndteres.

Det opereres med fire beskyttelsesgrader:

> *Når informasjon må beskyttes av sikkerhetsmessige grunner, skal en av følgende beskyttelsesgrader benyttes:*
>
> *STRENGT HEMMELIG*
>
> *HEMMELIG*
>
> *KONFIDENSIELT*
>
> *BEGRENSET*

Til de fire beskyttelsesgradene stilles følgende kriterier:

> *STRENGT HEMMELIG nyttes dersom det kan få helt avgjørende skadefølger for Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.*
>
> *HEMMELIG nyttes dersom det alvorlig kan skade Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.*
>
> *KONFIDENSIELT nyttes dersom det kan skade Norges etter dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.*
>
> *BEGRENSET nyttes dersom det i noen grad kan medføre skadefølger for Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.*

For behandling av dokumenter som trenger beskyttelse av andre grunner enn de som er nevnt i Sikkerhetsloven, kan Beskyttelsesinstruksen (1988) benyttes. Denne kan benyttes av blant annet private virksomheter og stats- og kommuneforvaltning ved behandling av informasjon som ikke er underlagt Sikkerhetsloven.

Beskyttelsesinstruksen opererer med to beskyttelsesgrader:

> *For å beskytte innholdet av et dokument, skal en av følgende beskyttelsesgrader nyttes:*
>
> *STRENGT FORTROLIG*
>
> *FORTROLIG*

Til de to beskyttelsesgradene stilles følgende kriterier:

> *STRENGT FORTROLIG nyttes dersom det vil kunne forårsake betydelig skade for offentlige interesser, en bedrift, institusjon eller enkeltperson at dokumentets innhold blir kjent for uvedkommende.*
>
> *FORTROLIG nyttes dersom det vil kunne skade offentlige interesser, en bedrift, institusjon eller enkeltperson at dokumentets innhold blir kjent for uvedkommende.*

Dette graderingssystemet blir blant annet omtalt i NSOs faghefte om Dokumentsikkerhet (Næringslivets sikkerhetsorganisasjon, 2000).

D Skjemaer

De fire skjemaene som blir benyttet under analysen er gjengitt i full størrelse på de neste sidene. Skjemaene kan kopieres og benyttes under analysen, eller tilsvarende skjemaer med eventuelle endringer kan utarbeides av analysegruppen.

Beskrivelse av skjermingsverdig objekt			Skjema nummer: O
System:	Dato:	Utført av:	Revisjon:
Skjermingsverdig objekt (nr. x, navn):			
Daglig ansvarlig for objektets sikkerhet:			
Anvendelse eller funksjon:			
Hvordan kan objektet erstattes?		Kan erstattes innen:	
		Erstatningskostnad:	
Beskrivelse av eksisterende reserveløsning(er):			
Sensitivitet	Ytterste konsekvens hvis tap av konfidensialitet:		
	Ytterste konsekvens hvis tap av integritet:		
	Ytterste konsekvens hvis tap av tilgjengelighet:		
Kommentar:		Objektets betydning: ☐ Høy ☐ Middels ☐ Lav ☐ Lav, ingen videre analyse	

Identifikasjon av trusselbilde				Skjema nummer:	T
System:		Dato:	Utført av:		Revisjon:
Skjermingsverdig objekt (nr. x, navn):					

Trussel (nr. x.x, navn)		Utførende aktør		Handlingsmønster (nr. x.x.x, navn)		Svakheter	

Kommentar:

Analyse av sikringstiltak			Skjema nummer: S . .
System:	Dato:	Utført av:	Revisjon:
Handlingsmønster (nr. x.x.x, navn):			
Beskrivelse av den uønskede hendelsen:			
Eksisterende forebyggende tiltak:		Tilfredsstillende?	
Eksisterende skadereduserende og normaliserende tiltak:		Tilfredsstillende?	
Forslag til nye og endrede tiltak:			
Kommentar:			

Risikovurdering			Skjema nummer: R . .
System:	Dato:	Utført av:	Revisjon:

Handlingsmønster (nr. x.x.x, navn):

Beskrivelse av konsekvens:

	Lite farlig	Farlig	Kritisk	Katastrofalt
Virksomheten				
Økonomi				
Anseelse				
Nasjonen				
Allierte				

Beskrivelse av sannsynlighet:

- ☐ Svært sannsynlig
- ☐ Meget sannsynlig
- ☐ Sannsynlig
- ☐ Lite sannsynlig

Kommentar: