FFI-rapport 2007/01204

Beskyttelse av samfunnet 5: Sårbarhet i kritiske IKT-systemer – sluttrapport

Håvard Fridheim og Janne Hagen

Forsvarets forskningsinstitutt/Norwegian Defence Research Establishment (FFI)

30. mars 2007

FFI-rapport 2007/01204

1014

ISBN 978-82-464-1222-1

Emneord

IKT

Kritisk infrastruktur

Risikoanalyse

Effektivitet

Godkjent av

Håvard Fridheim	Prosjektleder
Jan Erik Torp	Avdelingssjef

Sammendrag

BAS5 har vært et samarbeidsprosjekt mellom flere forskningsinstitusjoner, akademia, myndigheter og offentlige og private virksomheter. Prosjektets hovedtema har vært metoder for analyser av samfunnskritiske IKT-systemer.

Det er BAS5-prosjektets oppfatning at arbeidet med IKT-sikkerhet blir best dersom det legges strukturerte arbeidsprosesser med klare rammebetingelser til grunn for arbeidet, uavhengig av om arbeidet gjøres på nasjonalt -, sektor- eller virksomhetsnivå. Viktige steg i slike prosesser er å konkretisere hvilket ambisjonsnivå sikkerhetsarbeidet skal ha, spesifisere hva slags roller ulike aktører skal ha og å utvikle gode metoder som kan understøtte arbeidet.

BAS5 har i første rekke sett på det siste punktet: å utvikle metoder med relevans for IKT-sikkerhetsarbeidet i Norge. Målgruppen for de utviklede metodene er dels myndigheter som arbeider med nasjonal IKT-sikkerhet, dels virksomheter som eier og drifter samfunnskritiske IKT-systemer.

Det metodiske arbeidet i BAS5 har vært gjennomført for å understøtte tre hovedmål i prosjektet:

1. Utvikle og anvende metodikk for identifisering og rangering av kritiske samfunnsfunksjoner og IKT-systemer.
2. Utvikle og anvende metodikk for risikoanalyse av samfunnskritiske IKT-systemer.
3. Utvikle og anvende metodikk for effektivitetsvurderinger av tiltak som kan redusere sårbarheter i IKT-systemer.

Knyttet til det første målet har prosjektet utviklet en metodikk og en prosess for identifisering og prioritering. Denne er foreløpig ikke testet ut, men det anbefales at dette gjøres i etterkant av prosjektet.

Knyttet til det andre målet har prosjektet utviklet en prosess for risikoanalyser av samfunnskritisk IKT som ivaretar både tilsiktede og ikke-tilsiktede hendelser, et rammeverk som understøtter valg av analysemetoder og en veileder for støtte til personer som skal gjennomføre risikoanalyser.

Det tredje målet er i hovedsak koblet til prosjektets doktorgradsarbeid, som foreløpig ikke er avsluttet. De innledende arbeidene er likevel presentert som et vedlegg til denne rapporten.

Prosjektet har ikke har foreslått konkrete kostnads- og effektivitetsberegnede tiltak for det nasjonale sikkerhetsarbeidet, men pekt på behovet for nytenkning rundt det offentliges rolle i IKT-sikkerhetsarbeidet. Historisk sett har det ikke vært mangel på forslag til tiltak innen IT-sikkerhetsområdet, men heller manglende rammebetingelser for at tiltak kan utvikles og inngå i en helhetlig og kontinuerlig arbeidsprosess. Et forslag til nødvendige avklaringer og overordnede tiltak er derfor presentert som en del av denne rapporten.

English summary

BAS5 has been a project of collaboration between several research and academic institutions, public authorities and private and public enterprises. The primary goal of the project has been to develop methodologies for analysis of information systems critical to society.

The participants in this project is clear in its opinion that the work with information security will benefit greatly from structured work processes with specific frame conditions, regardless of whether the work is to be done on a national, sector or local level. Important conditions for the security work are specific objectives, clear roles for all involved and solid methodologies to support the work.

BAS5 has primarily worked with methodological issues. Possible users of the methodologies include public authorities and enterprises operating information systems critical to society.

The project has focused on three main areas:

1. Develop and apply methodologies to identify and prioritise critical societal functions and information systems.
2. Develop and apply methodologies for risk analysis of critical information systems.
3. Develop and apply methodologies for measurements of effectiveness of information security measures

Related to the first goal, the project has developed a methodology and a process for identification and prioritisation. The methodology has not been formally tested, and it is recommended that such tests are done subsequently to this project.

To meet the second goal, the project has developed a process for risk analysis of critical information systems addressing both intentional and non-intentional events, a framework supporting the process of choosing the methodological approach for a given analysis, and a user-guide for persons who will perform risk analyses.

The third goal is mainly related to a PhD-study in the project. This study is not yet finished, but the preliminary work is presented in the report.

BAS5 has not proposed measures with cost and effectiveness calculations associated. Instead, the project points to the need for new approaches in the public authorities work with national information security. Historically, several information security measures have been proposed in Norway, but a key problem is to allow such measures to be developed as a part of a holistic, continuous work process. Suggestions and recommendations for necessary clarifications and principal measures for the national work with information security are presented as part of the report

Innhold

Forord

Denne sluttrapporten er i første rekke skrevet for å gi en oversikt over arbeidet som er gjennomført i løpet av BAS5-prosjektet. Den baserer seg tungt på og henviser til alle rapporter og publikasjoner som har blitt skrevet i løpet av prosjektet. Som listen i appendiks D viser, inkluderer dette innsats fra mange personer.

Selv om bare de to prosjektlederne for BAS5 står som ansvarlige forfattere av denne rapporten, hadde det selvfølgelig ikke vært mulig å utarbeide den uten støtte, hjelp og bruk av resultater fra alle medarbeidere som har vært involvert i prosjektet.

1 Innledning

1.1 Bakgrunn

”Beskyttelse av samfunnet 5 (BAS5) – Sårbarhet i kritiske IKT[1]-systemer” har vært et forskningsprosjekt med fokus på metoder for analyse av kritisk informasjonsinfrastruktur. Prosjektet har vært et samarbeid mellom flere forskningsinstitusjoner, universiteter, høgskoler, departementer og direktorater, og er også støttet av Norges Forskningsråd gjennom IKT-SOS-programmet.[2] BAS5-prosjektet ble startet opp høsten 2004, og hoveddelen av arbeidet ble avsluttet første kvartal 2007. Imidlertid vil et PhD-arbeid i tilknytning til prosjektet vare til januar 2009.

Denne rapporten gir en *overordnet* oppsummering av hovedresultatene fra BAS5-prosjektet. Rapporten består av *korte* presentasjoner av mer detaljerte publikasjoner som er skrevet i forbindelse med prosjektarbeidet. Hovedhensikten med rapporten er å synliggjøre bredden av problemstillinger som BAS5 har berørt, og å vise hvor mer detaljinformasjon om ulike tema kan finnes. Med andre ord fungerer rapporten i stor grad som et veikart inn til de ulike delene av BAS5-prosjektet. En liste over publikasjoner skrevet ifm. prosjektet er vedlagt i appendiks D. Her er også de ulike publikasjonene sortert etter type målsetting i prosjektet.

I tillegg presenteres en del anbefalinger knyttet til det nasjonale arbeidet med informasjonssikkerhet. Anbefalingene er dels basert på BAS5-resultatene, dels basert på tidligere arbeider innen området. Disse anbefalingene står for FFIs regning.

Målgruppen for rapporten er primært prosjektets oppdragsgivere og øvrige aktører knyttet til det nasjonale arbeidet med IKT-sikkerhet.

1.2 Målsetting

Prosjektserien ”Beskyttelse av samfunnet” ble startet opp i 1994. Utgangspunktet for arbeidet var å vurdere hovedproblemstillinger for sivilt beredskap etter den kalde krigens slutt. Prosjektene fikk raskt et fokus på sårbarheten i kritisk infrastruktur, og ulike infrastrukturer (telekommunikasjon, kraftforsyning og transport) ble analysert i rekkefølge [1-4]. Formålet med arbeidene var å analysere sårbarheter i infrastrukturene, vurdere konsekvenser dersom de skulle svikte og anbefale tiltak for å redusere sårbarheter.

I alle BAS-prosjektene så man hvordan IKT-systemer var viktige for å opprettholde tjenester i kritisk infrastruktur. Samtidig ble det vurdert slik at IKT-sårbarheter kunne utnyttes for å ramme samfunnskritisk virksomhet. Det ble derfor foreslått et eget BAS5-prosjekt som skulle se spesielt på samfunnskritisk IKT.

[1] IKT = Informasjons- og kommunikasjonsteknologi
[2] IKT-SOS står for ”IKT – Sikkerhet og sårbarhet”

Prosjektet har hatt en klar metodisk innretning. Tre hovedmålsettinger ble satt ved starten av prosjektarbeidet:[3]

1. Utvikle og anvende metodikk for identifisering og rangering av kritiske samfunnsfunksjoner og IKT-systemer.
2. Utvikle og anvende metodikk for risikoanalyse av samfunnskritiske IKT-systemer.
3. Utvikle og anvende metodikk for effektivitetsvurderinger av tiltak som kan redusere sårbarheter i IKT-systemer.

Bakgrunnen for disse målene var en ambisjon om å understøtte ulike myndigheters og virksomheters mulighet til å forbedre informasjonssikkerheten i samfunnskritiske IKT-systemer. Prosjektmålsettingene følger en logisk sammenheng:

- Hva er de mest samfunnskritiske virksomhetene og IKT-systemene? (mål nr. 1)
- Hvordan kan risiko og sårbarhet i de kritiske IKT-systemene analyseres? (mål nr. 2)
- Hvordan kan man velge blant ulike tiltak for å øke sikkerheten i IKT-systemene? (mål nr. 3)

1.3 Oppdragsgivere og deltakere

BAS5 har vært et økonomisk spleiselag mellom en rekke aktører: Norges Forskningsråd, Fornyings- og administrasjonsdepartementet (FAD), Justis- og politidepartementet (JD), Olje- og energidepartementet (OED), Samferdselsdepartementet (SD), Norges vassdrags- og energidirektorat (NVE), Oljedirektoratet (OD), Post- og teletilsynet (PT), Kredittilsynet, Sosial- og helsedirektoratet (SHdir), Statnett, Direktoratet for samfunnssikkerhet og beredskap (DSB), Nasjonal Sikkerhetsmyndighet (NSM) og Forsvarets forskningsinstitutt (FFI). Totalt budsjett var drøyt 12 millioner kroner.

En delmålsetting i prosjektet var å stimulere til tettere kontakt mellom forskningsinstitusjoner og akademia innenfor informasjonssikkerhetsområdet. Dette gjenspeiler seg i listen over deltakere og bidragsytere i prosjektet. FFI har hatt administrativ ledelse for BAS5, men i tillegg har personell fra Universitetet i Stavanger (UiS), Norge teknisk-naturvitenskapelige universitet (NTNU), Høgskolen i Gjøvik (HIG), Statnett, NSM og DSB deltatt i prosjektet. Prosjektleder fra starten av var Janne Hagen, FFI. Håvard Fridheim, FFI, overtok prosjektlederjobben da Hagen i andre utlysningsrunde søkte og fikk PhD-stipendiatet ved Høgskolen i Gjøvik under BAS5-prosjektet.

En nærmere presentasjon av deltakere i og administrative erfaringer etter BAS5-prosjektet er vedlagt i appendiks C.

1.4 Rapportens oppbygging

Kapittel 1-3 gir generell bakgrunnsinformasjon og informasjon om BAS5-prosjektets

[3] I prosjektbeskrivelsen til BAS5 er disse prosjektmålene listet opp i en annen rekkefølge. Den nye rekkefølgen er satt opp av hensyn til denne rapportens struktur, og for å gi en ”top-down” tilnærming til problemstillingene i prosjektet.

gjennomføring og innretning.

Kapittel 4 og 5 rapporterer på de to første hovedmålene i prosjektet, knyttet til identifisering/prioritering og risikoanalyser.

Kapittel 6 inneholder vurderinger rundt aktuelle tiltak for det nasjonale arbeidet med informasjonssikkerhet. Det er flere årsaker til at dette kapittelet har blitt en del av sluttrapporten:

- BAS5-prosjektet er på mange måter et barn av Nasjonal strategi for informasjonssikkerhet [5]. Siden strategien i skrivende stund er under revisjon, ønsker prosjektet å gi innspill til det videre arbeidet med den, basert på erfaringene fra BAS5.
- Flere av oppdragsgiverne har ønsket mest mulig anbefalinger fra BAS5 om tiltak på nasjonalt nivå, ikke bare rapporter om metodeutvikling.
- Basert på flere års erfaring fra studier av så vel sivil som militær elektronisk kommunikasjon, kan FFI gi betraktninger rundt dette temaet. BAS5 er en naturlig ramme for å gjøre dette.

I kapittel 7 oppsummeres rapporten, og det pekes på mulige arbeidsområder i forlengelsen av prosjektet

I tillegg inneholder rapporten flere appendiks:

- Appendiks A gir en innføring i flere bakgrunnsstudier som er gjennomført i BAS5-prosjektet. De er gjennomført for å skaffe tilstrekkelig grunnkunnskap om et tema, slik at man i neste omgang var i bedre stand til å levere i forhold til hovedmålene i prosjektet. Tema i disse studiene har vært vurderinger av fremtidig teknologisk utvikling, en sårbarhetsvurdering av Internett samt tilhørende metodiske utfordringer, i tillegg til flere arbeider relatert til myndighetenes arbeider innen IKT-sikkerhetsområdet.
- Appendiks B gir en oversikt over prosjektets foreløpige arbeid med effektivitetsvurdering av tiltak, med andre ord prosjektets hovedmålsetting 3. Årsaken til at denne teksten er lagt i appendiks er at arbeidet ennå ikke er avsluttet.
- Appendiks C gir en nærmere presentasjon av administrative erfaringer i forbindelse med oppstart og gjennomføring av prosjektet.
- Appendiks D og E gir oversikter over hhv. publikasjoner fra BAS5 og foredrag holdt i regi av prosjektet.

2 Definisjoner og begreper

Det finnes en rekke begreper knyttet til samfunnssikkerhet og IKT-sikkerhet. Felles for mange av disse er at de tillegges forskjellig betydning avhengig av hvilket faglig miljø eller tradisjon man representerer. Det ville derfor ha vært en krevende oppgave å presentere alle tolkninger og nyanser av ulike begreper som har vært benyttet i løpet av BAS5-prosjektet. Rapporten spesifiserer derfor kun hvordan begrepene er ment forstått i denne rapporten. Det understrekes også at enkelte av begrepene her kanskje ikke er fullstendig presise heller. Dette er imidlertid et bevisst valg, for å redusere mengden av semantisk drøfting.

Samfunnets grunnleggende verdier er knyttet til befolkningens grunnleggende behov, og er her praktisk definert som liv og helse, livsmiljøet, økonomien, styringsevnen, og politisk tillit.

Kritiske samfunnsfunksjoner er alle funksjoner som samfunnet er avhengig av for å dekke befolkningens grunnleggende behov.

Kritisk infrastruktur er de av de kritiske samfunnsfunksjonene som er mest sentrale for å holde samfunnet i gang, her i praksis elektrisk kraft, telekommunikasjoner, vann og avløp, olje- og gassforsyning, transport, og bank og finans. Infrastrukturutvalget definerer begrepet slik [6]:

> *"Kritisk infrastruktur er de anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner som igjen dekker samfunnets grunnleggende behov og befolkningens trygghetsfølelse."*

I forlengelsen av begrepet kritiske samfunnsfunksjoner dukker begrepet *samfunnskritiske IKT-systemer* opp. I BAS5 er dette begrepet i første rekke benyttet om IKT-systemer som er viktige for funksjonaliteten av ulike kritiske samfunnsfunksjoner. Det er imidlertid viktig å understreke at dette ikke bare dreier seg om teknologiske forhold, men også om menneskene som anvender teknologien, organisatoriske forhold rundt IKT-systemet osv.

Risiko uttrykker fare for tap av viktige verdier som følge av uønskede hendelser. En vanlig tilnærming er å se på risiko som en kombinasjon av sannsynlighet for og konsekvens av en uønsket hendelse. En annen tilnærming er at risiko er en kombinasjon av mulige konsekvenser og tilhørende usikkerhet. Prosjektet har benyttet begge tilnærminger, men den siste definisjonen er lagt til grunn for det metodiske arbeidet rundt risiko- og sårbarhetsanalyse.

Sårbarhet er et uttrykk for et systems manglende evne til å fungere og oppnå sine mål når det utsettes for påkjenninger. I det metodiske arbeidet med risiko- og sårbarhetsanalyser er det lagt til grunn at sårbarhet er kombinasjonen av mulige konsekvenser og tilhørende usikkerhet, gitt en spesifikk fare eller trussel.

Sikkerhet er et samlebegrep for beskyttelse mot ulike uønskede hendelser. Innenfor sikkerhetsbegrepet skjuler det seg mange dimensjoner, blant annet om de uønskede hendelsene er tilfeldigheter og ulykker eller om de skjer som resultat av overlegg. For å skille mellom de sistnevnte hendelsestypene benyttes begrepene *ikke-tilsiktede* og *tilsiktede* hendelser.

Trusselbegrepet knyttes ofte til tilsiktede hendelser, og omhandler da kapasitet og intensjon til å gjennomføre skadelige handlinger. Begrepet trussel kan også brukes til å beskrive faren ved konsekvensene av utilsiktede hendelser, med andre ord at en hendelse i seg selv vil kunne utgjøre en trussel mot noe eller noen [6].

Informasjonssikkerhet defineres tradisjonelt ved hjelp av begrepene *tilgjengelighet, integritet og*

konfidensialitet. Med dette menes at informasjonen skal være *tilgjengelig* for autoriserte brukere, at informasjonen bare skal kunne endres eller slettes av autoriserte brukere (*integritet*) og at informasjonen ikke skal kunne leses av andre enn autoriserte brukere (*konfidensialitet*).

3 Hvorfor har BAS5 fokusert på metodikk i stedet for konkrete forslag til tiltak?

BAS-prosjektene har tradisjonelt hatt som sluttmål å presentere kosteffektivitetsberegnede tiltak som kan redusere sårbarheter innenfor de systemene prosjektene har analysert. Dette var også et utgangspunkt for de første versjonene av prosjektforslaget til BAS5.

Imidlertid fikk BAS5 til slutt en langt mer metodisk tilnærming enn tidligere prosjekter i serien, med mindre fokus på konkrete forslag til tiltak. Et av de spørsmålene prosjektet oftest får er hvorfor det ble slik. Det er mange årsaker til dette, men noen av de viktigste presenteres i dette kapittelet. Teksten er delvis basert på en rapport om temaet IKT-sikkerhet og tiltak på nasjonalt nivå [7].

3.1 Bidrar tiltakslister til at sårbarheten reduseres?

De senere år har det vært gjennomført en rekke forsknings- og utredningsarbeider om sårbarheter i kritisk infrastruktur, både generelt og innen enkeltsektorer som for eksempel kraftforsyning, telekommunikasjon, transport og vannforsyning. Fra offentlig forvaltning, forskningsinstitusjoner og konsulentselskaper har det blitt utformet store mengder med publikasjoner om sårbarheten i det moderne samfunnet, ikke minst med bakgrunn i økende avhengighet av IKT-systemer. Flere av arbeidene har også inneholdt konkrete forslag til tiltak for å redusere sårbarheter.

Det kan imidlertid stilles spørsmål om hvilken effekt arbeidene i nyere tid har hatt for sikkerhet og robusthet i nasjonale infrastrukturer. Arbeidet har åpenbart bidratt til å definere problemet og sette problemstillingen på den politiske agendaen, men fra et teknologisk ståsted kan det lett hevdes at sikkerhetsgevinsten ikke har vært like stor som volumet av arbeid skulle tilsi. Dette skyldes blant annet at problemstillingen rundt sårbarhet i infrastrukturene er kompleks. Eksempelet i neste avsnitt vil vise dette, med utgangspunkt i analyser av elektronisk kommunikasjon før og nå.

3.2 Analyser av kritiske infrastrukturer før og nå

Allerede på 80-tallet gjennomførte FFI analyser innen kritisk infrastruktur, blant annet for offentlig leverte telekommunikasjonstjenester i en totalforsvarskontekst. Utgangspunktet for disse arbeidene var:

- En enkel og oversiktelig tjenesterealisering i infrastrukturen. Selv om teknologiene som ble anvendt kunne være avanserte nok, var disse satt inn i innbyrdes strukturer som var relativt enkle og oversiktelige.
- Få tverrsektorielle avhengigheter. Telesystemet hadde i stor grad egen reservekraft som kunne tåle selv lange avbrudd i strømforsyningen, mens kraftbransjen på sin side hadde

egne radiosystemer for å ivareta sambandsbehovet.
- Et enkelt ”marked”, i form av at tjenesteleveransene skjedde fra kun én offentlig forvaltningsbedrift – Televerket.
- Et stabilt og omforent trusselbilde, hvor den dimensjonerende utfordringen var et militært angrep fra Sovjetunionen.

Med andre ord – analysesystemene var enkle og oversiktelige, endringer inntraff sjelden, trusselen var velkjent og kompleksiteten i beslutningsproblemet var overkommelig. I denne situasjonen kunne FFI bruke lineære analysemodeller (f.eks. feiltreanalyser) for å få oversikt over svake elementer eller funksjoner i selv større systemer, og på den måten identifisere behov for forbedringer og tiltak.

I løpet av 90-tallet oppstod imidlertid flere samtidige utfordringer for arbeidet med samfunnssikkerhet, i form av raske endringer og økt kompleksitet. For å fremdeles benytte telekommunikasjon som eksempel:

- Teknologiutviklingen akselererte, og endringer i systemene og tjenestenes oppbygging skjedde stadig raskere. Ulike IKT-systemer ble stadig viktigere som grunnlag for selv enkle kommunikasjonstjenester som telefoni. Internett utgjør i dag en sentral infrastruktur i denne utviklingen. Å få tilstrekkelig oversikt over enkeltsystemers oppbygging er dermed en stor utfordring.
- I tillegg kan det hevdes at samfunnets avhengighet av offentlige tjenester fra kritiske infrastrukturer ble dramatisk mye større enn tidligere, ikke minst pga. en sterk gjensidig innbyrdes avhengighet av systemer og tjenester mellom ulike sektorer. Kompleksitet som følge av den tette koblingen mellom ulike systemer ble dermed en stadig viktigere faktor å håndtere for sikkerhets- og beredskapsarbeidet.
- Tjenester innenfor elektronisk kommunikasjon ble utsatt for økt konkurranseutsetting. Tidligere offentlige forvaltninger som Televerket ble i løpet av få år forvandlet til private leverandører, og nye aktører dukket opp i tillegg. Kompleksiteten økte ytterligere som følge av dette, ikke minst i forbindelse med hvordan tiltak skulle finansieres og hvilke roller ulike aktører skulle ha ifm. IKT-sikkerhetsarbeidet. Det faktum at mange IKT-baserte tjenester og infrastrukturer ikke lenger er under direkte statlig forvaltning, er svært viktig for arbeidet med sikkerhet og robusthet.
- Den sikkerhetspolitiske utviklingen gav nye utfordringer. Det tidligere dimensjonerende scenariet for sikkerhetsarbeidet ble gradvis redusert i betydning utover 90-tallet. I dag er det mange aktuelle utfordringer for sikkerhets- og beredskapsarbeidet, uten at det er noen omforent oppfatning av hvilken som er viktigst. Dette gjør det vanskelig å sette klare mål for sikkerhetsarbeidet.

Disse utviklingstrekkene var sentrale for at mange av analysene og utredningene innen samfunnssikkerhet ble startet opp fra midten av 90-tallet. På den andre siden er de også viktige forklaringer på hvorfor arbeidet med samfunnssikkerhet er vanskelig. Kompleksiteten i problemstillingene øker, og utviklingen går i noen tilfeller så raskt at analyser og utredninger knapt rekker å bli ferdige før deler av resultatene er foreldet. Det er derfor fremdeles uløste

problemstillinger når det gjelder hvordan analyser av sårbarhet i samfunnet best kan bidra til økt sikkerhet.

3.3 Tiltak kontra metodikk

Selv om det de siste årene har blitt presentert en rekke forslag til tiltak for å redusere samfunnets sårbarhet overfor ulike farer og trusler, har mange av disse ikke blitt gjennomført etter analysenes slutt. Et eksempel i så måte er resultatene etter BAS2-prosjektet, som forelå i 1999 og som inneholdt konkrete forslag til alternative strategier for å redusere sårbarheter i offentlige telekommunikasjonssystemer [2]. Arbeidet var utgangspunktet for en egen stortingsmelding om temaet [8].

I ettertid har kun et fåtall av tiltakene som ble foreslått i arbeidet blitt gjennomført. Dette har flere årsaker, men den viktigste årsaken er at statiske tiltakslister kun er gyldige en kort periode etter at de er utarbeidet. Innenfor IKT-området har endringstakten vært svært rask de siste årene, og i dag er det lett på peke på at flere av tiltakene etter BAS2 er teknologisk foreldet. Den teknologiske og markedsmessige utviklingen gikk for fort til at tiltakene kunne iverksettes med mening.

En mulig løsning vil da være å prøve å iverksette tiltakene raskere, noe også Riksrevisjonens gjennomgang av arbeidet med nasjonal IKT-sikkerhet peker på [9]. Imidlertid er dette vanskelig innenfor dagens forvaltningsregime, hvor det må settes av tilstrekkelig tid til behandling av tiltakene, de gjeldende budsjettbehandlingsprosessene osv.

Etter vårt syn er det derfor ikke mangelen på forslag til tiltak som er utfordringen for det nasjonale sikkerhetsarbeidet innenfor IKT. Et større problem er å sikre at de tiltak som foreslås er realistiske og gjennomførbare innenfor den rammen de skal fungere i. Innenfor IKT-området innebærer dette at tiltak bl.a. må ta hensyn til:

- Den raske endringstakten i IKT-infrastrukturer og samfunnet som anvender tjenester fra disse.
- Utviklingen av markedet, med andre ord at pålegg om tiltak ikke virker konkurransevridende.
- Endringer i trusselbildet.
- Krav til forsvarlig byråkratisk behandling.

Med dette som utgangspunkt vil modellen med flerårige analyser som munner ut i konkrete tiltakslister med lang forventet levetid ikke være noen god løsning. En annen tilnærming er å legge opp til at sikkerhetsarbeidet skjer kontinuerlig, og at ulike virkemidler og tiltak kan utvikles fortløpende og vedlikeholdes ved behov. Dette er i tråd med tesen til en av informasjonssikkerhetsområdets store intellektuelle kapasiteter, Bruce Schneier: ”Security is a process, not a product”.[4]

[4] Se bl.a. Schneier B (2000): Secrets and Lies – Digital Security in a Networked World, John Wiley and Sons, 2000.

For å få til dette må man sikre arbeidsprosesser på tvers av sektorer og nivå som har klarest mulig målsettinger. En del av løsningen er også å utvikle gode metodiske tilnærminger på ulike nivå i sikkerhetsarbeidet. Derfor har også BAS5 fokusert spesielt på metodeutvikling.

De følgende kapitlene i denne rapporten peker på de metodiske problemstillingene som BAS5 har arbeidet med. Alle disse er sentrale for de prosessene som etterspørres i avsnittet over.

4 Hvordan identifisere og rangere samfunnsfunksjoner og IKT-systemer?

Dette kapittelet gir en kort oversikt over arbeidet som er gjort knyttet til identifisering og rangering av samfunnsfunksjoner i BAS5-prosjektet. For mer detaljinformasjon henvises til følgende to rapporter som er utarbeidet i prosjektet:

- Bakgrunnsstudie til metode for identifisering og rangering av kritiske samfunnsfunksjoner [10].
- Metode for identifisering og rangering av kritiske samfunnsfunksjoner [11].

Hoveddeltakere i dette arbeidet har vært DSB, NSM og FFI. Øvrige prosjektdeltakere har støttet arbeidet gjennom problemdiskusjoner og kommentarer til det gjennomførte arbeidet.

4.1 Problemstillinger i arbeidet

Behovet for å prioritere ulike hensyn i samfunnet er ikke av ny dato. Spesielt gjelder dette innenfor arbeidet med nasjonal beredskap, hvor et sentralt problem alltid har vært å fordele begrensede ressurser dit de kan gi størst virkning. Eksempler på beredskapsproblemstillinger innenfor prioritering er utpeking av nøkkelobjekter i samfunnet som må beskyttes av militære styrker i en krisesituasjon, klassifisering av objekter innenfor kritiske infrastrukturer for å avklare hvilke som skal underlegges de hardeste sikkerhetskravene, og utpeking av personer som skal prioriteres med vaksiner i tilfelle en pandemi brer seg. Muligheten for prioritering er også et vesentlig aspekt av en nasjonal tverrsektoriell ROS-vurdering, hvor ulike sektorer, virksomheter eller til og med personer og stillinger kan ses mot hverandre.

Innenfor IKT-sikkerhetsområdet kan det også defineres behov for å prioritere mellom ulike forhold. Dette kan gjøres blant ulike IKT-systemer, for å identifisere og rangere samfunnskritiske IKT-systemer slik at ressurser kan styres dit de bidrar mest til økt sikkerhet. Et annet forhold er å prioritere brukerne av ulike IKT-systemer, for å se hvilke av disse som bør tas hensyn til i knapphetssituasjoner.

Opprinnelig målsetting for BAS5 var å utvikle og anvende metoder for *identifisering og rangering av kritiske systemer og sektorer som er avhengige av IKT for deres produksjon av varer og tjenester*. Dette lot seg vanskelig avgrense, siden IKT-systemer har blitt allestedsnærværende som hjelpesystemer for alle sektorer i samfunnet. Med andre ord kunne ikke dette bare være en metodikk som så alene på IKT-systemene – metoden måtte også kunne

anvendes på kritiske samfunnsfunksjoner og infrastrukturer.

I henhold til bokmålsordboka[5] betyr *rangere* å ordne i en bestemt rekkefølge. Denne rekkefølgen kan være prioritert. *Prioritere* vil si å sette opp i rangorden og gi noe eller noen i denne ordenen fortrinn fremfor andre. BAS5-målsettingen har blitt tolket slik at mulighet for prioritering er ønskelig. Beskrivelsen i avsnittene over tilsier også dette. Dette er imidlertid ikke en banal oppgave. Prioritering av samfunnskritiske funksjoner og virksomheter er til syvende og sist et politisk valg, selv om valget kan understøttes av ulike metodisk baserte vurderinger. Blind anvendelse av en metodikk er derfor lite hensiktsmessig – det må også være klart hva prioriteringen skal anvendes til og hvilke ulike hensyn som skal tas i ulike prioriteringssituasjoner.

BAS5 har derfor gjort følgende:

- Prosjektet har utviklet en metode for identifisering og rangering av *alle* kritiske samfunnsfunksjoner, herunder alle kritiske infrastrukturer, og ikke bare kritiske IKT-systemer.
- Prosjektet har *beskrevet et system for beslutningsstøtte, og ikke et system for automatisk prioritering*. Dette betyr at relevante beslutningsmiljøer må involveres i bruken av metoden. Arbeidet kan ikke settes bort til ekspertmiljøer, selv om disse med fordel kan delta i prosessen.

4.2 Bakgrunnsstudien

Som et ledd i arbeidet med å utvikle metoden har BAS5 gjennomført en større bakgrunnsstudie [10]. Denne studien har vist til aktuelle metoder, kriterier, teori og begreper som er i bruk både i Norge og i utlandet, og som er relevante i utarbeidelsen av en norsk metode.

Et hovedinntrykk er at det ikke er produsert noen helhetlig metodikk for prioritering eller rangering av samfunnsfunksjoner og kritisk infrastruktur, i alle fall ikke en som er tatt i bruk av de lands myndigheter som studien har tatt for seg. Det er i alle tilfeller ikke funnet noen metodikk som faller helt sammen med målsettingen i BAS5-prosjektet. Likevel eksisterer det mye metodikk som kan relateres til vår, for eksempel analyser av gjensidige avhengigheter og nasjonale ROS-vurderinger. I enkelte tilfeller er metoder nylig utgitt og ikke utprøvd, som for eksempel en svensk metodikk for identifisering av samfunnsfunksjoner og en dansk metodikk for nasjonal ROS-analyse. Ulike metodiske innretninger er omtalt i bakgrunnsstudien [10].

Bakgrunnsstudien har vært viktig for å klarlegge rammebetingelsene for en metodikk for prioritering. Et meget viktig poeng er *hvem* som skal bruke den. Er det den enkelte virksomhet, de enkelte sektormyndigheter, en myndighet med tverrsektorielle interesser (som DSB eller NSM) eller ulike forskningsinstitusjoner? Det kan tenkes at selv en enkel metode er for vanskelig å bruke for aktører som ikke er vant til å tenke tverrsektorielt. Dette reiser også spørsmål om metodikken skal vedlikeholdes og eventuelt av hvem. I utgangspunktet har metodikken blitt

[5] Bokmålsordboka, Universitetsforlaget

utviklet med tanke på at en bred gruppe miljøer skal kunne anvende den, men den er likevel vinklet spesielt i retning av myndighetsorganer med (tverr)sektorielle problemstillinger.

Det må også tas hensyn til *hva* man ønsker at metoden skal gi svar på:

- Skal den produsere en ”autoritativ” rangert liste over hvilke funksjoner som er mest kritiske for samfunnet?
- Skal den brukes av den enkelte virksomhet som en egenevaluering av hvor kritisk egen virksomhet er for samfunnet?

Metodikken er fleksibel nok til å kunne anvendes til alle formålene over. Dette krever imidlertid et solid informasjonsgrunnlag for området som skal analyseres. Det kan også tenkes at metoden ikke gir endelige svar, men at resultater må justeres i samråd med sektoreksperter. Man kan lett forestille seg store forskjeller mellom eksempelvis en oversikt over prioriterte brukere av mobilnettet, og prioriterte mottagere av vaksine ved en pandemi. Metoden har rom for å ta opp i seg slike forskjeller, for eksempel ved å inngå samtaler med sektoreksperter.

En metode må også legge opp til åpenhet om hvordan et resultat er produsert. Det vil gjøre det enklere å få et resultat som er tilpasset det spesifikke behovet. Åpenhet gjør det også enklere å få tilbakemeldinger på selve metoden, slik at den kan justeres etter hvert som man høster erfaring med den. Selve prosessbeskrivelsen i BAS5-metoden bidrar til slik åpenhet.

4.3 Forslag til metodikk for identifisering og prioritering

I BAS5-prosjektet er ulike samfunnsfunksjoners kritikalitet knyttet til sårbarheten overfor ulike hendelser som kan ramme dem, i tillegg til betraktninger om deres vesentlighet eller viktighet for samfunnet. *Det er derfor knapt mulig å prioritere kritiske samfunnsfunksjoner uten samtidig å gjøre seg opp en grunnleggende mening om hvilke risikoer de er utsatt for eller utsetter andre for.* Det vil si at det må forutsettes at det foretas risiko- og sårbarhetsvurderinger (ROS-vurdering) på sektor- og virksomhetsnivå.

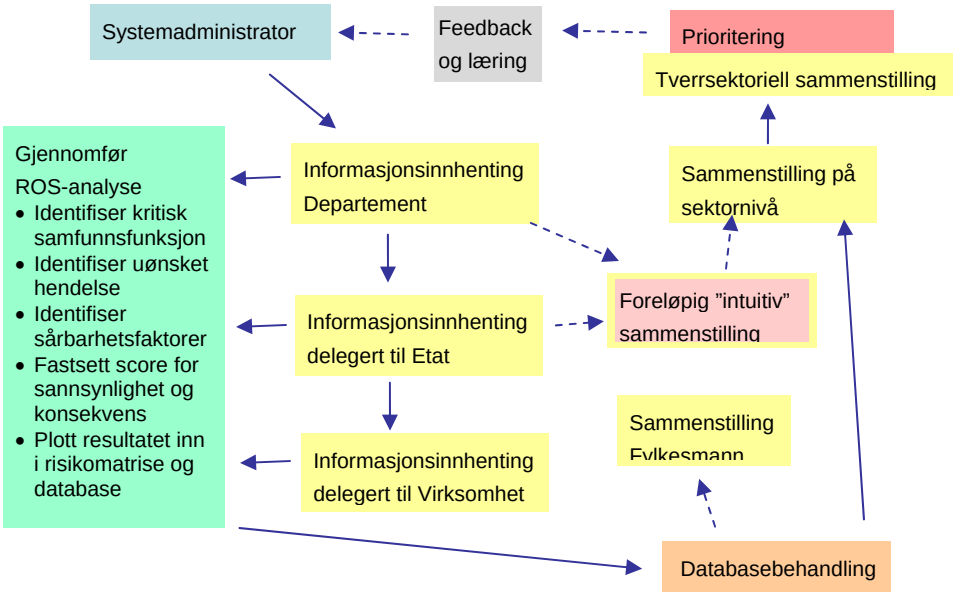
Metoden som er utviklet beskriver hovedtrekkene for beslutningstøtte i situasjoner hvor det kan være nødvendig å prioritere mellom forskjellige kritiske samfunnsfunksjoner. Den er risikobasert, og inneholder to hovedaspekter:

- Det utvikles og forankres en permanent løpende prosess som involverer ansvarlige departementer og alle andre som har ansvar og kunnskap innen egen sektorer
- Til støtte for denne prosessen brukes en teknikk som er ROS-basert, da antagelser om kritikalitet bør forutgås av nærmere analyse og vurdering

Prosessen krever følgende:

- At ”noen” pekes ut til å samordne den på nasjonalt nivå, på tvers av ansvarsgrenser
- At det ordinære ansvarsprinsippet utnyttes for å strukturere arbeidet
- At det etableres tverrsektorielle felles prosedyrer, inklusive permanente fora med tett møtefrekvens
- At det etableres tverrsektorielle standarder

Prosessen er illustrert i Figur 4.1:



Figur 4.1 Prosessoversikt. Heltrukne piler angir hovedløpet i prosessen, de stiplede angir mulige tilleggssteg.

Metoden skal understøtte prioritering på tvers av forskjellige samfunnssektorer. Dette krever et standardiserende grep på metodens teknikker. Konkret valg av ROS-metode er overlatt til den enkelte sektor eller virksomhet, tilpasset dennes forutsetninger. Innrapportering av resultater fra ROS-analyser skal derimot foretas i et rigid standardisert format. Denne standardiseringen omfatter:

- En hierarkisk organisert liste over kritiske samfunnsfunksjoner
- En hierarkisk organisert liste over uønskede hendelser

Den hierarkiske organiseringen tillater at listen enkelt suppleres ved behov. Dessuten fremstår denne typen organisering som et "trekkspill" i forhold til hvilket generalitetsnivå det er ønskelig å legge seg på for forskjellige formål, fra svært konkrete problemstillinger som krever identifikasjon av nøkkelpersoner, til mer generell prioritering mellom sektorer.

Dessuten standardiseres følgende:

- 11 sårbarhetsfaktorer i 5 konkretiserte trinn hver
  - Sted
  - Geografisk omfang
  - Befolkningstetthet
  - Utetemperatur (årstid)
  - Tid på døgnet
  - Varighet
  - Avhengigheter i forhold til andre kritiske samfunnsfunksjoner
  - Substitusjonsmuligheter, erstatning av komponenter, omgåelse av feil

    - Grad av kobling
    - Kultur
    - Mental forberedelse
- Sannsynlighet i 5 konkrete trinn
    - Mindre enn 1 gang pr 1000 år
    - 1 gang pr 100-1000 år
    - 1 gang pr 10-100 år
    - 1 gang pr 1-10 år
    - Mer enn 1 gang pr år
- Konsekvenskategorier i 5 konkrete trinn hver
    - Liv og helse
    - Livsmiljøet
    - Økonomi
    - Styringsevne
    - Politisk atferd/tillit
- Risikomatrise 5 x 5, 5 risikokategorier

Det forutsettes dessuten at det utvikles en enkel standard database for å håndtere disse informasjonene på tvers av virksomheter og samfunnssektorer.[6] Dette vil muliggjøre sortering av data etter ønsket variabel, tilpasset den konkrete problemstillingen. Arbeidet med å spesifisere hvordan en slik database kan bygges opp er startet i BAS5.

Metoden har foreløpig ikke vært anvendt (annet enn i mindre tester). Det kan selvfølgelig reises flere innvendinger mot dette, ikke minst fordi flere prosjektrådsmedlemmer har ønsket konkrete prioriteringslister innenfor utvalgte områder. Dels har dette vært et spørsmål om kapasitet. Arbeidet med å utvikle metodikken viste seg raskt å være vesentlig mer komplekst og arbeidskrevende enn opprinnelig antatt. Den viktigste årsaken er likevel at prosjektet på flere områder ser store problemer med å utvikle statiske lister, som er allmenngyldige på tvers av ulike scenarier. Et eksempel er ønsket om å innføre en prioriteringsordning innen mobiltelefoni, slik at viktige aktører i krisesituasjoner er sikret tilgang i perioder der kapasiteten ikke er tilstrekkelig. Hvilke aktører som er involvert vil imidlertid variere sterkt fra krise til krise. En liste som er satt opp basert på et typisk akutt redningsscenario (f.eks. en større trafikkulykke) er ikke nødvendigvis den riktige i en situasjon der en infrastruktur svikter (f.eks. at et område mister strømmen i lengre tid). Selv innenfor en hovedklasse av scenarier kan aktørtypen variere, avhengig av forhold som scenariets geografiske omfang, varighet, andre samtidige hendelser i samfunnet osv. På forhånd oppsatte prioriteringslister kan derfor virke mot sin hensikt.

4.4 Anbefalinger og videre arbeid

Anvendelsesområdene for en prioriteringsmetode kan være mange. Med utgangspunkt i prosjektets målsetting har BAS5 derfor utviklet en metode for identifisering og prioritering av

[6] En mulig innvending mot dette er at informasjonsmengden som utvikles i løpet av prosessen blir så stor at databasen ikke lenger kan kalles "enkel". Databasen vil også i seg selv inneholde mange vurderinger av sensitiv art, noe som gjør at den totale informasjonsmengden kan måtte bli gradert iht. Sikkerhetsloven.

alle kritiske samfunnsfunksjoner, herunder alle kritiske infrastrukturer og kritiske IKT-systemer. Dette innebærer i første rekke et system for beslutningsstøtte med formaliserte rapporteringskrav og nødvendig støttedokumentasjon.

Det anbefales *ikke* at metoden anvendes til å utvikle generelle, fastsatte prioriteringslister som forventes å ha allmenn gyldighet og lang varighet, selv om metodikken kan understøtte et slikt arbeid. Årsaken til dette er endringstakten i det moderne samfunnet. Eventuelle prioriteringslister som settes opp må revideres regelmessig.

Prioriteringer gir mest mening innenfor problemstillinger som er mest mulig konkrete, hvor mange rammebetingelser er lagt. Eksempler på potensielle anvendelsesområder er:

- Hvem bør ha prioritert tilgang til kommunikasjonstjenester i krisesituasjoner?
- Hvem bør få vaksine i en pandemisituasjon, og i hvilken rekkefølge?
- Hvilke virksomheter skal prioriteres ved kraftrasjonering?
- Hvor lønner det seg å sette inn investeringer for å forebygge kriser?
- Hvilke installasjoner bør prioriteres for fysisk beskyttelse?
- Hvilke virksomheter bør være underlagt Sikkerhetslovens bestemmelser?
- Hva bør bygges opp igjen først etter en naturkatastrofe?
- Hvilke samfunnsområder bør ha særlig oppmerksomhet omkring ROS-vurderinger?

Selv innenfor slike konkrete problemstillinger er det imidlertid en krevende oppgave å sette opp prioriteringslister som er gyldige på tvers av ulike scenarier. Klarhet i hensikten med prioriteringen, så vel som i hvilke situasjoner man forventer at den skal kunne brukes, er derfor avgjørende.

Metoden som er presentert er skalerbar, i den forstand at den kan anvendes på ulike nivå: nasjonalt/tverrsektorielt, innenfor en sektor eller også innenfor en virksomhet. Den er likevel ikke prøvd ut i løpet av BAS5. Det anbefales derfor at metodikken testes ut i forlengelsen av prosjektet. Dette kan være mulig i forhold til pågående og kommende ROS-prosesser innenfor ulike samfunnssektorer.

Metoden er utarbeidet uten at en spesifisert ”eier” står klar til å ta den i bruk. Imidlertid er det enkelte tverrsektorielle direktorater innenfor samfunnssikkerhetsarbeidet, spesielt DSB eller NSM, som kanskje er de mest åpenbare kandidatene til å ta arbeidet med metodikken videre. Det anbefales at Justisdepartementet tar stilling til og evt. beslutter at DSB og/eller NSM gis i oppdrag å forsøke å få til en tverrfaglig prosessforankring på dette området.

Det er flere metodiske problemstillinger som kan tas videre i etterkant av BAS5-prosjektet:

- Det foreslåtte hierarkiet over hendelser bør utvikles videre og underkastes nærmere analyse, med hensyn på å identifisere de viktigste scenariene og sile fra scenarier som er mindre plausible.
- Modellen inneholder foreløpig ikke prosesser eller teknikker som er spesielt rettet mot oppdagelse av hittil ukjent risiko, for eksempel scenarioteknikker, foresight-teknikker

eller horizon scanning-teknikker.

- Det er også behov for en nærmere kritisk gjennomgang av på hvilke områder en prioritering faktisk gir mening. En spesiell problemstilling er hvorvidt på forhånd fastsatte prioriteringer faktisk vil avhjelpe en krisesituasjon, eller om det kan være til hinder for krisehåndteringen der og da.
- Prioritering overfor en spesifikk situasjon kan sies å være relativt enkelt. Men hvordan kan man best prioritere hensyn på tvers av et bredt spekter av scenarier?

5 Hvordan gjennomføre risikoanalyser av IKT-systemer?

Dette kapittelet beskriver arbeidet med risiko- og sårbarhetsanalyser i BAS5-prosjektet. Det er skrevet en rekke dokumenter knyttet til ROS-arbeidet i prosjektet, og disse omtales fortløpende i teksten.

Hoveddeltakere i dette arbeidet har vært UiS og FFI. Øvrige prosjektdeltakere har støttet arbeidet gjennom problemdiskusjoner og kommentarer til det gjennomførte arbeidet.

5.1 Problemstillinger i arbeidet

En risiko- og sårbarhetsanalyse (ROS-analyse) er et virkemiddel for å håndtere risiko. I ROS-analysen blir uønskede hendelser identifisert og rangert ut i fra risiko, og dette gir et grunnlag for å komme frem til risikoreduserende tiltak i analysesystemet. Tiltak kan være fokusert mot ulike forhold ved systemet, for eksempel teknologi, organisasjon, arbeidsprosesser, prosedyrer og krav. Basert på en ledelsesgjennomgang kan identifiserte tiltak prioriteres.

Ledelsesgjennomgangen må sette analysene inn i en sammenheng, og ta hensyn til at de har sine begrensninger og bygger på en rekke forutsetninger. Med dette som utgangspunkt kan en ROS-analyse bidra til at man starter arbeidet med de viktigste systemene og de mest effektive tiltakene først. ROS-analyser kan brukes både for å redusere sårbarheten av eksisterende systemer og for å påvirke design og utbygging av nye systemer. ROS-analyser har vært brukt innen ulike industrier i mange år, blant annet innen kjernekraft, olje- og gassindustrien og prosessindustrien.

I ”Nasjonal strategi for informasjonssikkerhet” fra 2003 omtales ROS-analyser spesielt [5]:

> *”Risiko- og sårbarhetsanalyser skal ligge til grunn for alle tiltak myntet på informasjonssikkerhet. Strategier og tiltak skal utarbeides, gjennomgås og revideres på basis av regelmessig gjennomførte analyser. Det er i virksomhetenes egen interesse at det blir gjennomført analyser og utarbeidet strategier”.*

Med andre ord trekkes ROS-analyser frem som et viktig virkemiddel for å koble de ulike virksomhetenes løpende sikkerhetsarbeid med nasjonale sikkerhetsstrategier. På mange måter er dette også tankegangen bak metodikken for identifisering og prioritering av samfunnsfunksjoner som er skissert i kapittel 4.3. I et slikt perspektiv blir det viktig å sikre at ROS-analysene

gjennomføres på best mulig måte, metodisk og praktisk.

Flere særtrekk gjør at IKT-relaterte risikoanalyser skiller seg fra risikoanalyser som gjennomføres i andre sektorer [12]:

- Tilsiktede handlinger spiller en sentral rolle når IKT-sikkerhet skal vurderes. Dette er en utfordring å håndtere metodisk, som diskutert i kapittel 5.2
- Teknologien er kompleks. Det er vanskelig å få en god oversikt over ITK-systemer, og det mangler ofte en helhetlig beskrivelse av systemene som skal analyseres. Dette gir store ufordringer i forhold til å identifisere mulige hendelser, og ikke minst i forhold til det å få en god forståelse av sammenhenger og avhengigheter systemene imellom.
- Brukerne av IKT-systemene mangler ofte en detaljert systemforståelse. De har et forhold til informasjonen som IKT-systemet gir dem, men liten forståelse for teknologien som ligger bak.
- Det er få eller ingen som både har en god forståelse av både IKT-systemer og av fagområdet risikoanalyse.
- Teknologien endrer seg veldig raskt. Dette medfører at man ofte har en begrenset mengde erfaringsdata som kan brukes i analysene.

Til tross for disse utfordringene er det fremdeles mulig å gjennomføre risikoanalyser av IKT-systemer med godt resultat. Dette krever imidlertid gode arbeidsprosesser, bevissthet rundt hva analysene skal svare på og hvilke rammebetingelser som finnes for arbeidet. Dette har vært hovedproblemstillingen i BAS5-prosjektets delmål 2.

Siden det finnes svært mange ulike ROS-metoder allerede, har ikke BAS5-prosjektet sett det som hensiktsmessig eller fornuftig å prøve å utvikle en ny og universell metode. Utgangspunktet for BAS5 har vært å bygge på eksisterende arbeider og å fokusere forskningen på de områdene der prosjektet kan bidra til ny innsikt og kunnskap for å forbedre risikostyringsprosessen.

To metodiske hovedområder har vært i fokus for arbeidet [12]:

- Å etablere en helhetlig tilnærming til risikoanalyser som omfatter alle sikkerhetshendelser (ulykker og feil så vel som viljeshandlinger).
- Å etablere et rammeverk for valg av hensiktsmessig metode for gjennomføring av ROS-analyser.

I tillegg har prosjektet tatt for seg følgende problemstillinger:

- Hvilke uønskede hendelser og faresituasjoner kan IKT-systemer bli utsatt for?
- Hvilke utfordringer står man overfor når det skal gjøres en risikoanalyse av et IKT-system?

Erfaringer fra dette arbeidet beskrives i de følgende kapitlene.

5.2 Hvilke uønskede hendelser kan IKT-systemene bli utsatt for?

Utgangspunktet for enhver risikoanalyse er ønsket om å håndtere risiko overfor ulike farer og

trusler mot systemet som skal vurderes. Dette kapittelet diskuterer hvilke hendelser et IKT-system kan bli utsatt for. Dette er beskrevet nærmere i rapporten ”Risikoanalyser i BAS5 - Teknologiske erfaringer ” [13].

5.2.1 Tilsiktede kontra ikke-tilsiktede hendelser

Flere hendelser mot IKT-system skjer uten overlegg. Slike *ikke-tilsiktede hendelser* kan grovt deles i tre kategorier:

- *Menneskelige feil.* Feil som oppstår i forbindelse med systemdesign, arkitektur, implementasjon, bruk, drift, overvåking og vedlikehold. Mange av disse vil være menneskelige feil gjort utenfor systemeiers kontroll – for eksempel problem forbundet med ustabil programvare.
- *Fysisk svikt.* Dette inkluderer for eksempel fysisk slitasje (harddisker o.l.), kabelbrudd, kontaktfeil og komponentfeil som følge av varmeutvikling. Ofte vil de bakenforliggende årsakene igjen være menneskelige feil, som for eksempel feil dimensjonering, manglende utskifting av gammelt utstyr eller mangelfull overvåking.
- *Miljø/naturhendelser.* Oversvømmelse, vannskader, brann, lynnedslag og vind.

Disse feilkategoriene kan også inntreffe hos kritiske leverandører for IKT-systemet, og det er derfor naturlig å inkludere en kategori for indirekte hendelser, som for eksempel strømbrudd og eksterne kommunikasjonsbrudd.

Ikke-tilsiktede hendelser har potensial til å gi relativt store konsekvenser. Eksempler på slike hendelser er blant annet:

- I august 2001 opplevde EDB Fellesdata problemer i ca. en uke, som førte til at anslagsvis 2 millioner nordmenn mistet forbindelsen med sine banker. Feilen oppstod under en test av nye sikkerhetsløsninger, hvor innholdet på flere disker ble slettet på grunn av en operatørfeil.[7]
- Netcom opplevde i juni 2003 vannlekkasje i en sentral på Økern. Om lag 200.000 kunder ble rammet i sju timer.[8]

Med *tilsiktede hendelser* menes angrep mot eller manipulasjon av IKT-system og tilhørende infrastruktur. Dette kan inkludere alt fra fysiske angrep og ødeleggelser til logisk og sosial manipulasjon av system og organisasjon. Spesielt når det gjelder logiske angrep og sosial manipulasjon har man sett en urovekkende øking de seneste årene. Det er flere grunner til dette, men muligheter for repeterbarhet, enkel massespredning og selvspredning via Internett, lang avstand til målet (mål og angriper er gjerne i ulike juridiske domener) og muligheter for ulike grader av anonymitet nevnes ofte.

De siste årene har man også sett en utvikling der økonomisk gevinst stadig oftere er målet for

[7] Digi.no (2001): Et tastetrykk stoppet Fellesdata, 7. august 2001.
http://php.digi.no/digi98.nsf/pub/dd20010810002101_hb_36307164
[8] Itpro.no (2003): NetCom-skandalen: Uakseptabelt og kritikkverdig, 13. juni 2003.
http://itpro.no/art/3755.html

angrepene. Dette kan involvere alt fra utsendelse av uønsket e-post eller fremvising av reklame, til for eksempel direkte angrep på økonomisk infrastruktur[9].

Mesteparten av de tilsiktede hendelsene i et IKT-system oppstår på grunn av massedistribuert ondsinnet kode som ikke er rettet mot spesifikke organisasjoner. Disse kan på mange måter ses på som "miljøpåvirkning" fra Internett – de oppstår forholdsvis tilfeldig, og det finnes mange effektive beskyttelsesmekanismer.

Av nyere eksempel fra Norge kan en trekke fram to hendelser:

- I desember 2006 ble det for første gang rapportert i media om vellykkede angrep mot norske nettbankbrukere. Brukernes maskiner hadde blitt infisert av spesialtilpasset programvare som kunne ta over nettbanksesjonen og utføre transaksjoner etter at brukeren hadde logget seg inn på normal måte.[10]
- Virusangrep mot DnB NOR i mars 2007. Programvaren som ble spredt var laget for å stjele passord fra deltakere i nettverksspill og hadde dermed ingen "nytte" i det interne nettverket. Likevel førte utbruddet til utilgjengelige system og omfattende skader. Tapsoverslag etter 11 dager ble av uavhengige estimert til over 100 millioner kroner.[11]

5.2.2 Hvorfor er tilsiktede hendelser mot IKT-systemer vanskelig i risikoanalyser?

Tilsiktede ondsinnede handlinger mot IKT-systemer kan være et vanskelig tema i en risikoanalyse. Trusselvurderinger i forhold til tilsiktede hendelser tar ofte utgangspunkt i at det finnes aktører med ulike intensjoner og kapabiliteter. Dette kan være alt fra gutteromshackere via kriminelle organisasjoner til fremmede makters etterretningstjenester, alle med ulike formål og virkemidler. Å konvertere betraktninger rundt dette til vurderinger av sannsynlighet med samme skala som ikke-tilsiktede hendelser (f.eks. i form av relative frekvenser) er imidlertid vanskelig, og vurderingene vil i beste fall bli beheftet med stor usikkerhet.

I tillegg til usikkerhet knyttet til en eventuell angripers intensjon og kapabilitet, er det også vanskelig å få en god generell oversikt over hvilken trussel en faktisk står overfor. Trusselbildet er stadig i endring, og det er vanskelig å finne god og balansert informasjon om temaet. Konkrete hendelser blir ofte ikke oppdaget, og for de som faktisk blir oppdaget er rapporteringen meget varierende. Mye eksisterende kunnskap på området vil også være gradert av sikkerhetshensyn, og dermed ikke nødvendigvis tilgjengelig for operatører av ulike IKT-systemer i samfunnet.

På tross av denne usikkerheten er vår erfaring at det likevel er godt mulig å håndtere tilsiktede hendelser i en risikoanalyse. De aller fleste sårbarheter som blir utnyttet er allerede kjente, og de fleste hendelser inntreffer fortsatt rimelig tilfeldig og gjør dermed mindre skade enn det et rettet

[9] Symantec. Symantec Internet Security Threat Report, Trends for January 06 - June 06, Volume X, september 2006. http://www.symantec.com/specprog/threatreport/ ent-whitepaper symantec internet security threat report x 09 2006.en-us.pdf

[10] Se for eksempel Dagens Næringsliv (2006): "Tappet 14.000 fra nettbank-konto", 22. desember 2006. http://www.dn.no/forsiden/politikkSamfunn/article963881.ece

[11] Dagens IT (2007): " Svinedyrt DnB Nor-mareritt", 12. mars 2007. http://www.dagensit.no/bedrifts-it/article1046261.ece

angrep vil gjøre. Virusutbruddet hos DnB NOR nevnt ovenfor er et typisk eksempel på dette. På tross av at bankens interne system ble infisert, så ble kunder og forretningslogikk tilsynelatende ikke skadelidende ettersom det ikke var et rettet angrep.

5.3 Hvordan velge metode for risikoanalysen?

Kapittelet beskriver det metodiske arbeidet BAS5 har gjennomført for å understøtte prosessen med å velge riktig metode for ulike typer analyser. Dette arbeidet er i hovedsak dokumentert i rapporten ”Utvikling av metodikk for risikoanalyse av samfunnskritisk IKT” [12].

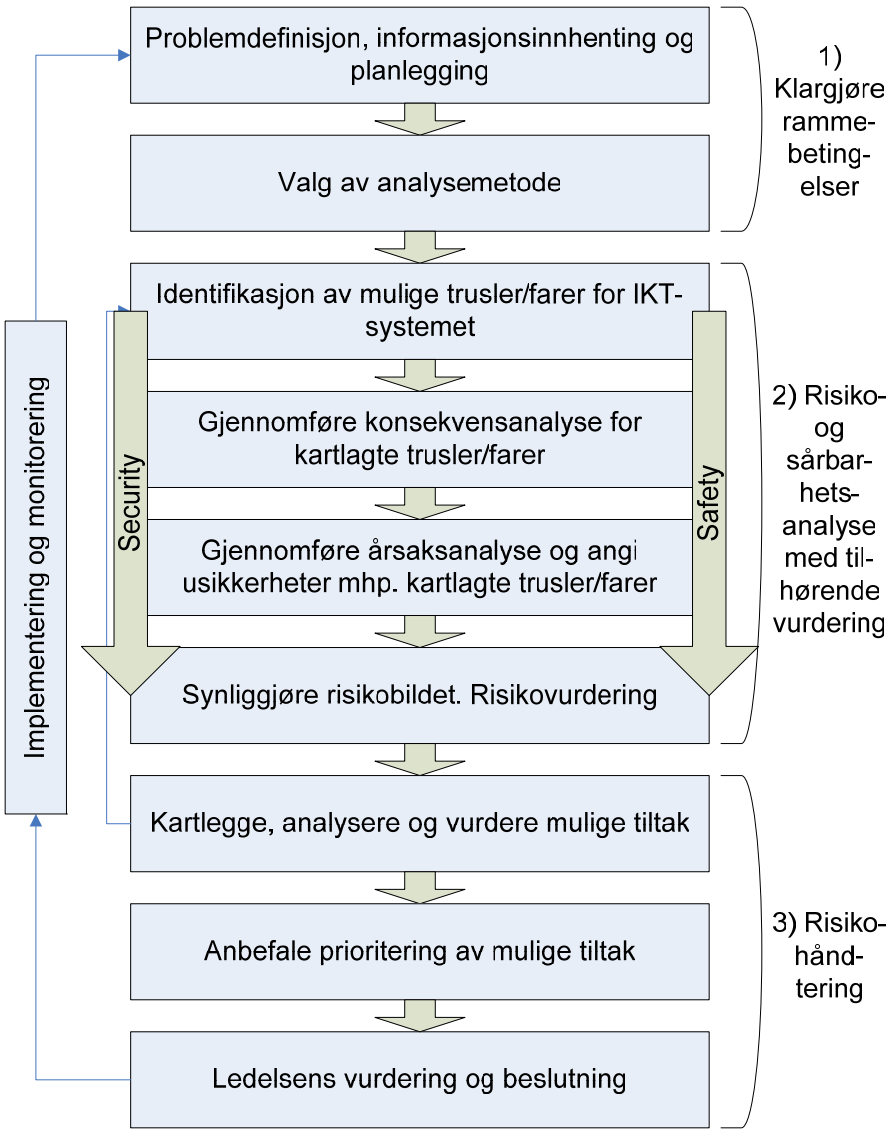
5.3.1 Risikostyringsprosess for både safety og security

Tradisjonelle ROS-tilnærminger springer ut av sikkerhetsarbeidet i industrien. Her blir risiko ofte uttrykt som en kombinasjon av sannsynligheten for at en uønsket hendelse oppstår og konsekvensene av den. Sannsynlighet uttrykkes ofte i form av frekvenser, for eksempel at en hendelse inntreffer 1 gang per 100. år. Frekvenser kan bl.a. utarbeides på bakgrunn av historiske data om feilrater i ulike komponenter.

De siste årene har det vært økende interesse for å inkludere tilsiktede handlinger i risikoanalyser. Det er imidlertid flere utfordringer ved å gjøre dette med den tradisjonelle tilnærmingen til risiko, som diskutert i kapittel 5.2.2. Dette gjelder spesielt vurderinger av sannsynlighet. Relative frekvenser kan fort bli meningsløse for viljeshandlinger, ikke minst fordi det er få gode oversikter over historiske data om ulike angrep.

En mulig tilnærming til dette innebærer å se på risiko i form av konsekvenser av uønskede hendelser og tilhørende usikkerhet. Dette innebærer et bredere perspektiv på risiko. Sannsynlighet kan fremdeles benyttes for å representere analytikerens usikkerhet om en hendelse og hva som vil bli konsekvensene, men fokus på usikkerhet innebærer at man også ser utover de beregnede sannsynligheter og forventningsverdier. For viljeshandlinger kan usikkerheten være meget stor, og da kan det være mer fruktbart å beskrive denne i stedet for å presse frem spesifikke sannsynlighetstall. Et eget paper beskriver denne tilnærmingen i mer detalj [14].

Med denne tilnærmingen som utgangspunkt er det mulig å sette opp en risikostyringsprosess som er grunnlag for ROS-analyser av alle sikkerhetshendelser, både tilsiktede og ikke-tilsiktede. Prosessen som er benyttet i BAS5 er presentert i Figur 5.1 [12].



Figur 5.1 Risikostyringsprosess

Prosessen er generell, og den skiller seg ikke vesentlig fra andre prosessbeskrivelser for risikostyring. Den inkluderer tre hovedaktiviteter:

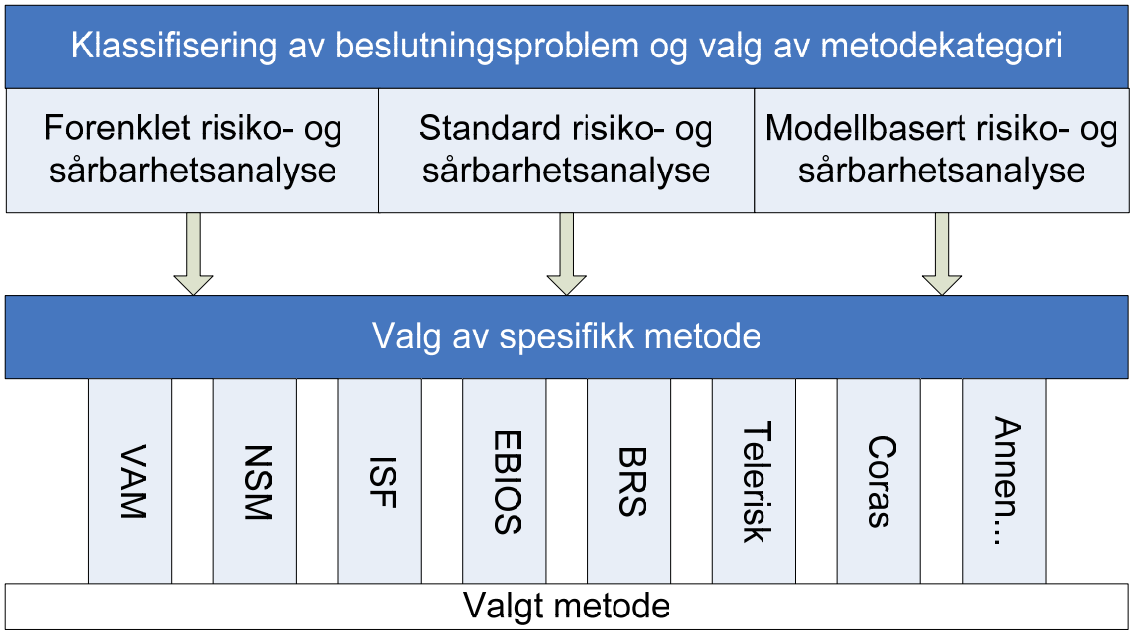
- Klargjøre rammebetingelsene for arbeidet
- Gjennomføre risiko- og sårbarhetsanalysen
- Håndtere risikoen

Figur 5.1 viser hvilke underaktiviteter som hører til hver hovedaktivitet.

5.3.2 Valg av metodikk

BAS5 har sett spesielt på den delen av risikostyringsprosessen som innebærer valg av metode for risiko- og sårbarhetsanalyser av IKT-systemer. Årsaken til dette er i første rekke at det finnes svært mange ulike ROS-metodikker, alle med ulike styrker og svakheter. Uten tilstrekkelig klarhet om hvilken problemstilling man ønsker å analysere, rammebetingelsene for analysen og egenskapene til ulike metoder, er det fullt mulig for en eier av samfunnskritiske IKT-systemer å velge en metode som i beste fall ikke er hensiktsmessig, og som i verste fall gir direkte gale

resultater.



Figur 5.2 Valg av metodikk

For å kunne velge metode behøves det en strukturert prosess. BAS5 har utarbeidet en slik prosess, som presentert i Figur 5.2. Prosessen er beskrevet i mer detalj i [12]; her gis en kort presentasjon.

Valg av metode er i Figur 5.2 presentert som en totrinnsprosess:

1. Klassifisering av beslutningsproblem og valg av metodekategori
2. Valg av spesifikk metode

Hensikten med den første aktiviteten er å klargjøre beslutningsproblemet og å bestemme hvilken hovedkategori av risikoanalysemetoder som er hensiktsmessig å bruke. I BAS5-prosjektet er det valgt å klassifisere ulike metoder i tre hovedgrupper:

- Forenklet risikovurdering (kvalitativ). Uformelle tilnærminger for å kartlegge risikobildet, ofte som idédugnader eller gruppediskusjoner.
- Standard risikovurdering (delvis kvantitativ). Mer formaliserte tilnærminger, blant annet med bruk av etablerte metoder som HAZID, HAZOP og grovanalyser. Risikomatriser benyttes ofte for å visualisere risikobildet.
- Modellbasert risikovurdering (kvantitativ). Bruk av kvantitative teknikker, for eksempel hendelses- og feiltrær for beregninger av konsekvenser og tilhørende usikkerhet/sannsynlighet.

Selve prosessen med å velge hovedkategori av metode gjøres ved hjelp av et sett med spørsmål knyttet til betydningen av IKT-systemet som skal analyseres. Spørsmålene er overordnede og knyttet til faktorer som:

- Forventet konsekvens for en uønsket hendelse, multiplisert med sannsynligheten for at den uønskede hendelsen skal inntreffe
- Usikkerheter knyttet til faktorer som kan skape overraskelser i forhold til

forventningsverdien.

- Rammefaktorer, dvs. begrensninger i forhold til budsjett, tid, tilgang til informasjon osv.

Spørsmålene leder brukeren gjennom en overordnet risikovurdering. Hensikten med denne er ikke å analysere systemet som sådan, men å benytte fastsatte skjema for å klassifisere problemstillingen slik at brukeren får hjelp til å velge hvilken hovedkategori metodikk han bør bruke.

Trinn to i prosessen å velge en spesifikk metode. En av aktivitetene i BAS5 har vært å evaluere ulike metoder og å karakterisere disse innenfor de tre hovedgruppene. Totalt har 7 metoder/verktøy blitt evaluert. Fire metoder (inklusive enkelte standardtilnærminger uten formelle verktøy) er prøvd ut i reelle caseanalyser, se kapittel 5.4. De øvrige har blitt vurdert etter en overordnet gjennomlesing og teoretisk vurdering. Dokumentasjon av vurderingene er gitt i en egen rapport [12].

For å sikre en systematisk evaluering av ulike metoder, har et sett med vurderingskriterier blitt definert. Kriteriene er i første rekke knyttet til:

- Metodiske forhold knyttet til risiko (teori, metodisk tilnærming osv)
- Erfarings- og kompetansebehov
- Nødvendige ressurser (spesielt tid og penger)

Metode kan da velges ved hjelp av de vurderingene som BAS5 har gjort. Hver metode er presentert med en overordnet kategorisering, som eksempelet i Tabell 5.1 viser. De blå områdene viser klassifiseringen av metoden som er lagt inn i tabellen. I tillegg er det utarbeidet mer detaljerte omtaler av hver metode.

	Faser som er dekket av metoden		
	Klargjøre rammebetingelser	Risiko- og sårbarhetsanalyse med tilhørende vurdering	Risikohåndtering
Egenskaper ved metoden	**Beskrivelse**		**Kommentar**
Fokus	Ulykker	Villede handlinger	Security
Attributter	Sikkerhet	Helhetlig (sikkerhet, miljø, økonomi, omdømme …	Fokuserer på konsekvenser
Oppløsning i analysen	Overordnet	Detaljert	Sjekkliste-basert
Bransje	Generell	Spesiell bransje (hvilken?)	IKT

Tabell 5.1 Oppsummering av egenskaper for en risikoanalysemetode, eksempel

Selv om prosessbeskrivelsen over kan virke omfattende, legger BAS5 opp til at en slik vurdering kan gjøres raskt, for eksempel i løpet av 1-2 timer ved bruk av standardiserte skjema. Dette skal som sagt ikke være full risikoanalyse i seg selv, men en klassifisering av problemstilling og valg av metode.

5.4 Casestudier i BAS5-prosjektet

5.4.1 Hvilke analyser har blitt gjennomført?

BAS5 har gjennomført fire risikoanalyser av eksisterende IKT-systemer innenfor det som kan kalles samfunnskritiske virksomheter. Analysene tok for seg følgende systemer:

- IKT-systemet ved et stort sykehus
    - Analysen vurderte IKT-systemene som var i bruk ved en av sykehusets avdelinger, spesielt elektroniske pasientjournaler.
- IKT-systemet for et stort finansforetak
    - Analysen omhandlet sikkerheten ved store finansielle transaksjoner overfor både ikke-villede og villede hendelser.
- IKT-systemet for en stor aktør innen kraftforsyningen
    - Analysen fokuserte på sikkerhet i IKT-systemene som understøttet kraftoverføring.
- IKT-systemet for en stor aktør innen petroleumsbransjen
    - Formålet med analysen var å vurdere sikkerhet i IKT-systemene mot offshoreinstallasjoner.

Et viktig grunnlag for casestudiene var en egen studie av sårbarheter i Internett, som omtalt i appendiks A.2. Arbeidet med ROS-casene og internettstudien er presentert i flere delrapporter [12;13;15-17].

Alle IKT-systemene som ble vurdert i analysene var i daglig bruk. Et generelt trekk for flere av systemene er at de opprinnelig har vært tenkt som støttesystemer for å understøtte den normale virksomheten. Med andre ord har systemene gitt bedriftens medarbeidere ekstra funksjonalitet (f.eks. støtte til beregninger, tilgang på bilder og rapporter osv.) som ikke har vært kritiske for å gjennomføre de normale oppgavene. Men i løpet av forholdsvis kort tid har disse systemene blitt kritiske, slik at feil i IKT-systemene umiddelbart vil påvirke virksomhetenes evne til å løse sine primæroppgaver.

Systemene er også fortsatt i meget rask utvikling, og flere tjenester blir utviklet og lagt til fortløpende. Generelt er kravet mer kapasitet (lagring, regning, nettverk) og bedre tilgjengelighet for brukerne. I helsesektoren ser man for eksempel en utvikling mot digitalisering av bilder, taleopptak til journaler, mobile enheter med journaler og prosedyrer, trådløse nettverk, sømløs tilgjengelighet osv. Tilsvarende krav finnes blant brukerne fra andre sektorer.

I forbindelse med casene har håndtering av sensitiv informasjon vært en utfordring. Resultatene fra ROS-analysene har ikke kunnet bli offentliggjort av sikkerhetshensyn. I stedet har prosjektet

utarbeidet noen nøytrale erfaringer fra dette arbeidet som kan publiseres offentlig. De viktigste erfaringene er knyttet til hvordan risikoanalyser av samfunnskritiske IKT-systemer best kan gjennomføres, og disse presenteres i det følgende (dette er i hovedsak basert på [12] og [13]).

5.4.2 Hvilket nivå og omfang skal man velge for analysen?

En klar avgrensing av hva som skal analyseres er viktig for å komme i mål på tilmålt tid. Et IKT-system har sjelden en naturlig geografisk eller organisatorisk avgrensing. I tillegg vil årsaker for hendelser gjerne ligge utenfor selve IKT-systemet. Spesiell oppmerksomhet må rettes til hvilket nivå konsekvensene skal måles mot. For IKT-systemer kan verdier for analysen finnes på mange nivåer:

- Sett mot IKT-systemet i seg selv – hvordan vil ulike hendelser i deler av systemet påvirke IKT-systemets tilgjengelighet, integritet, konfidensialitet osv?
- Sett mot virksomheten – hvordan vil en svikt i IKT-systemet påvirke virksomhetens mulighet til å gjennomføre sine arbeidsoppgaver?
- Sett mot samfunnet – hvordan vil en svikt i IKT-systemet kunne påvirke andre samfunnsfunksjoner, befolkningen osv. Dette er spesielt relevant for IKT-systemer innen kritisk infrastruktur.

Valg av nivå vil være viktig for hvilke svar analysen gir og hvilke tiltak risikoanalysen munner ut i. Klarhet i dette er viktig, men ikke alltid like lett å etterfølge under en analyse.

5.4.3 Hvordan sikrer man riktige deltakere i analysen?

Mye av arbeidet ved en risikoanalyse kan gjøres ved gruppeprosesser, f.eks. knyttet til identifikasjon av uønskede hendelser, diskusjon av konsekvenser av og frekvenser for ulike hendelser osv. Deltakersammensetning her vil avhenge av hvilken type analyse som skal gjennomføres, og gruppesammensetningen er avgjørende for resultatet. Det behøves andre deltakere dersom man vil gjennomføre en teknologisk analyse av et gitt et IKT-system, enn dersom man ønsker å analysere en virksomhets totale risiko overfor IKT-relaterte hendelser.

I tillegg til å sikre riktig kompetanse ved analysens oppstart, er det viktig å beholde denne kompetansen i løpet av arbeidet. Selv om det kan være ønskelig å stille med reserver eller dra inn ulik kompetanse underveis, viser BAS5-analysene at resultatet blir best dersom gruppen er den samme under hele analysen. Et arbeidsmøte i en risikoanalyse er også en psykologisk prosess, der en ofte er avhengig av fortrolighet og gjensidig tillit. Alvorlige sårbarheter og svakheter dukker for eksempel typisk opp sent i analysen, når deltakerne føler tillit til de andre deltakerne.

5.4.4 Hvordan får man tilstrekkelig forståelse av systemet som skal analyseres?

Risikoanalyser krever god oversikt over IKT-systemet som skal analyseres, gjerne i form av en modell av systemet. Her ligger en av hovedutfordringene i en IKT-risikoanalyse. I tillegg til å forstå de funksjonene som systemet skal utføre, må man ha kompetanse om og erfaring med IKT-systemets arkitektur, komponentene som inngår, programvare som brukes og sikkerhetsmekanismer som er i bruk. Man må også ha kunnskap om mulige sårbarheter som et slikt system kan ha og hvilke farer og trusler det kan utsettes for. Det er også viktig med generell

forståelse for IKT-sikkerhet og kjennskap til forskjellig teknologi: gammel, nåværende og fremtidig.

Et grundig arbeid med dokumentasjon og modellering viser seg ofte å ha nytte utover selve analysen. I tillegg til å være direkte til nytte i videre arbeid med risikoanalyser, er denne typen oversikt også nyttig som input til normal drift av systemet.

BAS5-prosjektet har ikke funnet noen universelle språk eller verktøy for å modellere komplekse IKT-systemer med tanke på trusler og sårbarheter. Dersom den valgte metodikken ikke har et eget modelleringsspråk, kan en enkel og forholdsvis intuitiv ”horisontal” inndeling oppnås ved å bruke nettverkslagene som utgangspunkt:

- *Fysisk.* Bygninger, rom, dører, låser, vinduer, innsyn, adgangskontroller, kabler, kabeltraseer, strømtilførsel, nødstrøm, miljøpåvirkninger (brann, oversvømmelse etc), annen fysisk sikring av maskinvare.
- *Nettverk.* Dette må ofte modelleres på flere lag. Svitsjer, rutere, brannmurer, servere for nettverksdrift og overvåking er aktuelle elementer. Til en viss grad kan programvare for drift og overvåking produsere systemtegninger på logiske nettverksnivå, og disse vil være nyttig input til modellering.
- *Mellomnivå.* Backup, felles autentiseringsmekanismer, katalogtjenester, filtjenester.
- *Applikasjonsnivå.* Operativsystem og applikasjoner for sluttbrukere med tilhørende serverprogramvare, databaser, servere for drift og overvåking.
- *Brukere.* Kompetanse, sikkerhetskultur, personellsikkerhet
- *Organisasjon.* Både verdiproduserende organisasjon og IT-organisasjon. Funksjoner og arbeidsoppgaver. Organisasjonsstruktur, ressurser, styring. Organisering av sikkerhetsarbeid. Hendelseshåndtering, vaktordninger, varsling, beredskapsplaner.

5.4.5 Hvordan vurdere risiko?

I risikovurderingen vil en vurdere sannsynlighet for og konsekvens av de spesifiserte uønskede hendelsene fra fareidentifikasjonen. Det er flere utfordringer ved å gjøre dette for IKT-systemer, og noen av de viktigste diskuteres her.

Tilgang til historiske data over uønskede hendelser er et stort problem. For risikoanalyser i andre domener har man gjerne detaljert statistikk for feilhendelser og ulykker. Men på grunn av den raske utviklingen av programvare, maskinvare og arkitekturløsinger, finnes det sjelden et pålitelig statistisk grunnlag for uønskede hendelser i IKT-systemer. Konkrete feil og sårbarheter blir som regel reparert etter en hendelse.

Hendelser med lav konsekvens og høy sannsynlighet viser deg seg ofte å være enkelt å behandle i en risikoanalyse. Hendelser med høy konsekvens og lav sannsynlighet er som regel vanskeligere å få til en god diskusjon om (”usannsynlig”, ”da er det uansett slutt”, ”det er det andre som tenker på”). Ofte blir slike hendelser utelukket fra analysene. En riktigere tilnærming ville ha vært å inkludere dem, men å gi dem lav sannsynlighet.

For å kunne vurdere risiko for ulike uønskede hendelser opp mot hverandre, må sannsynlighet og konsekvens kunne måles med en felles metrikk. Det å utvikle og anvende en slik felles metrikk er ofte en av hovedutfordringene i en risikoanalyse. For konsekvenser er det vanlig å kategorisere organisasjonens verdier i tre klasser:

- Økonomi: tapt eller forsinket produksjon, skade på utstyr og eiendom, erstatningsansvar, tapt arbeidstid.
- Tillit og anseelse: tillit hos kunder, marked, samfunn, ansatte og eventuelt regulerende organ (statlig tilsyn, konsesjonsutstedere osv). Dette kan også sees på som langsiktige økonomiske verdier.
- Helse, miljø og sikkerhet (HMS): Tap av liv, personskade, skade på miljø og omgivelser.

Det er vanlig å gradere tapene i de ulike konsekvensklassene basert på økonomisk tap. Denne inndelingen kan også brukes for IKT-systemer, men for at en slik konsekvensanalyse skal bli god, bør man sette av nok tid og ressurser til å analysere konsekvenser utenfor selve IKT-systemet. Dette er imidlertid vanskelig, og konsekvensanalysen må i alle fall stoppe der kompetansen i analysegruppen stopper. For rent tekniske analyser bør konsekvenser dermed måles i forholdsvis ”nære” konsekvenser for systemet. For eksempel kan konsekvensklassene beskrive nedetid for sentrale tjenester eller nettverk i systemet, konfidensialitetstap etc.

5.5 Veileder for risikoanalyse av IKT-systemer

Gjennom casestudiene som er beskrevet i kapittel 5.4 så prosjektet raskt at det er mange utfordringer med å gjennomføre gode risikoanalyser av IKT-systemer. Mange aktører gjennomfører risikoanalyser av IKT-systemer, men kvaliteten på analysene som gjennomføres er høyst varierende. I dette ligger det også en erkjennelse av at metodevalget på langt nær er det eneste suksesskriteriet for en god risikoanalyse – hvordan metodene anvendes er langt viktigere.[12]

En viktig del av prosjektarbeidet har vært å dokumentere disse erfaringene og systematisere disse i en overordnet ”veileder” for risikoanalyser av samfunnskritisk IKT. Denne er dokumentert som et vedlegg i rapporten ”Utvikling av metodikk for risikoanalyse av samfunnskritisk IKT” [12], og kan gi støtte til planlegging og utvikling av en risikoanalyse. Noe supplerende informasjon kan også finnes i rapporten ”Risikoanalyser i BAS5 – Teknologiske erfaringer ” [13].

Veilederen presenterer en stegvis gjennomgang av de ulike delene av risikoanalyseprosessen som er presentert i Figur 5.1. Prosessen er relevant for alle risikoanalyser, uansett hvilket nivå analysen gjennomføres på og hvilken metode som legges til grunn. For hvert av stegene gir veilederen råd om hva som bør gjøres og hva som ofte gjøres feil. Typiske fallgruver i arbeidet trekkes spesielt frem.

Veilederen kan bli et viktig hjelpemiddel for ulike myndighetsorganer innenfor IKT-sikkerhet, som kan tilby denne overfor virksomheter innenfor sin sektor for å øke bevissthet rundt hvordan

[12] Satt på spissen – erfaringene fra prosjektet tilsier at en god analyseledelse og -gjennomføring med en ”dårlig” metodikk gir bedre resultater enn den motsatte situasjonen.

analyser best kan gjennomføres.

5.6 Anbefalinger og videre arbeid

Risikoanalyser har de seneste årene inntatt nye områder i samfunnet. Mens denne tilnærmingen opprinnelig ble utviklet for analyse av teknologiske systemer i prosessbasert industri, benyttes den i dag på også på problemstillinger med betydelige innslag av menneskelige og organisatoriske faktorer. Årsaken til dette er sannsynligvis at metodikkens opprinnelige tankesett (risiko er en kombinasjon av sannsynlighet og konsekvens av ulike hendelser) er relativt intuitiv for de fleste. Det er imidlertid mange utfordringer ved å gjennomføre en god risikoanalyse med resultater som gir faglig mening. Dette har vært utgangspunktet for BAS5-prosjektets arbeid med risikoanalyser for samfunnskritisk IKT.

BAS5 har foreslått *en risikostyringsprosess for ROS-analyser av IKT og en formalisert prosess for valg av metodikk.* I tillegg har BAS5 utarbeidet *en overordnet veileder for ROS-analyse av IKT-systemer*. Resultatene vil bidra til økt bevissthet rundt og klarhet i selve risikoanalyseprosessen, og i tillegg gi bedre forutsetninger for at resultatene etter analysen blir gode.

Selv om prosessen for valg av metodikk har vært prøvd ut i prosjektet, vil nytten av den først kunne testes ut dersom ulike virksomheter får tilgang til resultatene og anvender disse i forbindelse med egne ROS-analyser. Det finnes også langt flere metoder for ROS-analyse enn de BAS5 har hatt mulighet til å evaluere i løpet av prosjektet. Rammeverket bør derfor oppdateres fortløpende med nye metoder. Dette krever imidlertid at prosessen blir anvendt og har klar nytte for ulike virksomheter.

Flere metodiske problemstillinger kan være gjenstand for analyser i forlengelsen av BAS5:

- Hvordan kan tilsiktede hendelser best inkluderes i risikoanalyser? En spesiell utfordring er hvordan sannsynlighets- og usikkerhetsvurderinger av slike hendelser bør behandles metodisk.
- Hvordan kan strategiske sikkerhetsinitiativer og lokale ROS-analyser best kobles? Resultatene fra BAS5-prosjektets delmål 1 og 2 bør derfor viderebehandles og integreres i større grad enn nå.
- Hvordan kan andre sikkerhetsteknikker inngå i og understøtte en risikoanalyse av samfunnskritisk IKT? Eksempler på slike teknikker er bruk av sjekklister, penetrasjonstester, tradisjonelle sårbarhetsanalyser av IKT-systemer osv.
- Hvordan kan følgekonsekvenser utenfor IKT-systemet best behandles i en risikoanalyse? Spesielt problematisk er konsekvensene for storsamfunnet som er avhengige av tjenester fra IKT-systemet. Den enkelte virksomhet vil sjelden ha tilstrekkelig kompetanse om slike forhold eller ressurser til å gjennomføre en detaljert analyse.

Til slutt er det viktig å presisere at risikoanalyser kun er ett av mange aktuelle virkemidler for å øke IKT-sikkerhet (alternativer kan være etterlevelse av standarder, bruk av penetrasjonstester osv). Generelle krav om å gjennomføre risikoanalyser som et ledd i det nasjonale

sikkerhetsarbeidet er derfor lite hensiktsmessige, dersom de ulike virksomhetene ikke samtidig klart ser *hvorfor* de bør gjøre det og *hvordan* det best kan gjøres. På dette området vil erfaringene fra BAS5 gi viktige innspill.

6 Tiltak for arbeidet med nasjonal informasjonssikkerhet

Det er flere typer tiltak som kan vurderes for å oppnå økt sikkerhet og robusthet i IKT-systemer. Som diskutert i kapittel 3 ligger problemet ofte i å sette tiltakene inn i en prosess som sørger for at de blir relevante i forhold til de rammebetingelsene de skal fungere under, og å følge dem opp i ettertid slik at de faktisk blir gjennomført. Her er det i praksis lite som skiller arbeidet med nasjonal informasjonssikkerhet fra de erfaringene BAS5-prosjektet har gjort for risikoanalyser av IKT-systemer generelt, som diskutert i kapittel 5.

BAS5 har bidratt til at flere tiltak har blitt foreslått, spesielt i forbindelse med risikoanalysene som prosjektet har gjennomført for ulike virksomheter (se kapittel 5.4).[13] Flere av oppdragsgiverne i prosjektet har i tillegg ønsket anbefalinger på nasjonalt nivå, f.eks. for å understøtte arbeider med nasjonale strategier for IKT-sikkerhet. Derfor diskuterer dette kapittelet nødvendige grep for det videre arbeidet med nasjonal informasjonssikkerhet. Det understrekes at dette er et komplekst tema, og flere relevante forhold er bare kort omtalt i den påfølgende diskusjonen. Arbeidet er i hovedsak basert på en egen rapport om temaet [7].

6.1 Kunde kontra leverandør – hva blir statens rolle?

I dagens IKT-marked er det to naturlige roller; *leverandøren og den kompetente kunden*. Med andre ord er det *kunden* av IKT-baserte tjenester som må etterspørre det han trenger av tilstrekkelig sikkerhet og beredskap. Kunden og leverandøren må så bli enige om egenskapene i leveransen dem i mellom, også med hensyn til sikkerhets- og beredskapsfunksjoner. Så lenge man er innenfor en tjenesteleverandørs ansvarsområde, vil avveiningen mellom ulike tiltak normalt være basert på virksomhetens egen kostnyttetilnærming, med utgangspunkt i hovedsaklig bedriftsøkonomiske hensyn. Kundene vil på sin side ofte tenke mer på pris enn på sikkerhet i tjenestene. Kunde-leverandørmodellen vil da gi et endelig sikkerhetsnivå som ikke nødvendigvis tas spesielle hensyn til ulike oppfatninger av hva som er ”samfunnets beste”.

Det kan imidlertid hevdes at spørsmålet om et tilstrekkelig nivå av sikkerhet og beredskap i samfunnsviktige IKT-systemer ikke bare bør baseres på en kommersiell diskusjon mellom leverandører og kunder, men også bør inkludere ekstra sikkerhetskrav fra samfunnet. Dette krever imidlertid klarhet i hvilke krav samfunnet kan og bør stille, hvilke virkemidler samfunnet kan ta i bruk og hvilke aktører som har en rolle for å bidra til økt sikkerhet i IKT-infrastrukturer.

I Norge har offentlige myndigheter lenge hatt sentrale roller i arbeidet med IKT-sikkerhet, gjennom blant annet lovmessig regulering og tilsynsvirksomhet. Et viktig spørsmål er hvordan denne rollen kan ivaretas i dag. Selv om statens rolle ikke er like naturlig i dag som den var

[13] Tiltakene har i hovedsak måttet unntas offentligheten pga. sensitivitetshensyn.

tidligere (spesielt fordi mye av den samfunnskritiske virksomheten ikke lenger er eid og drevet av offentlige selskaper), må sannsynligvis myndighetene på en eller annen måte på banen. Dette kan i utgangspunktet være å ivareta rollen som innkjøper på vegne av fellesskapet, tilrettelegger for sikkerhetsarbeid i virksomhetene eller kravstiller gjennom lover og forskrifter. I dagens sikkerhetsregime søker man å tilnærme seg dette på flere måter. Med bakgrunn i den teknologiske og strukturelle utviklingen som er skissert i kapittel 3, krever alle oppgavene svært høy kompetanse. Dette kompetansebehovet vil øke ytterligere med utviklingen i årene som kommer.

Det er et svært viktig poeng at myndighetene ikke lenger har tilgang til den kompetanse om IKT-baserte infrastrukturer som de hadde den tiden infrastrukturene i hovedsak var eid av det offentlige. De kan heller ikke uten videre forvente å tilegne seg denne kompetansen i en situasjon hvor teknologiutviklingen skjer svært raskt. Dette har svært mye å si for hvilke tiltak det er realistisk å iversette av myndighetene, og hvilke reguleringsmodeller som kan fungere.

6.2 Rammebetingelser for det nasjonale arbeidet med informasjonssikkerhet

Som diskutert i kapittel 3 mener FFI at en fruktbar fremgangsmåte til nasjonal IKT-sikkerhet er å understøtte et *kontinuerlig* sikkerhetsarbeid, som ikke avhenger av ”skippertaksbaserte” tiltakslister, men som fortløpende bidrar til vurderinger av sikkerhet og robusthet. For å få til dette, må flere rammebetingelser på plass. Det er FFIs oppfatning at slike rammebetingelser foreløpig ikke er klargjort på nasjonalt nivå. Da er det også vanskelig å foreslå konkrete tiltak for å redusere sårbarheten i samfunnskritisk IKT. I det videre presenteres noen forhold som må avklares i det videre arbeidet med nasjonal IKT-sikkerhet.

Et meget viktig tiltak for myndighetenes arbeid med informasjonssikkerhet er å etablere *en klar ambisjon for arbeidet.* Hvilket sikkerhetsnivå bør man kunne oppnå, og hvilken hensikt skal dette ha for samfunnet? Ambisjonen må ta utgangspunkt i:

- En omforent oppfatning av hvilket trusselbilde IKT-systemer står overfor. Utvikling av scenarier, eller i det minste en konkretisering av aktuelle trusselsituasjoner, er en viktig del av dette.
- En presisering av hvilke trusler man ønsker at samfunnet skal kunne motstå, og en tilsvarende vurdering av hvilke utfordringer som blir for store.

Ambisjonsnivået må ikke bare presiseres i forhold til trusler og sikkerhetspolitisk situasjon, men det må også være realistisk sett i forhold til utviklingen innen marked og teknologi for IKT-baserte infrastrukturer.

Deretter kan man iverksette tiltak for å oppnå den ønskede målsettingen. Dette krever imidlertid en *metodisk basert og ikke minst sporbar prosess, hvor nødvendige tiltaks effektivitet kan kobles mot og helst måles mot klare strategiske føringer og målsettinger.* Ikke bare er dette viktig for eventuelle forskningsinstitusjoner og konsulentselskaper som gjennomfører oppdrag innenfor IKT-området, men det er også tilsvarende viktig at myndighetene selv har slike prosesser i sitt arbeid.

Dette krever igjen betydelig kunnskap om IKT hos myndighetene. Til en hver tid oppdatert kunnskap om teknologi og marked vil være en avgjørende forutsetning, selv for et enkelt reguleringsregime. *Derfor er det svært viktig at det forankres god kontakt mellom myndigheter og operatører, slik at det skjer et tett integrert samarbeid om sikkerhetsspørsmål.* Det er naturlig at et myndighetsorgan har dette ansvaret. Samtidig er det viktig å merke seg de naturlige begrensninger som vil måtte ligge i en slik kontakt, gitt virksomhetenes klare kommersielle føringer.

Basert på det overnevnte, kan det fortløpende utvikles tiltak. Effekten av disse kan måles mot målsettingene som settes i forbindelse med prosessen.

BAS5-prosjektets metodeutvikling så langt understøtter arbeidet med å etablere prosessen som er skissert over. Arbeidet med identifisering og rangering av IKT-systemer skisserer i seg selv et eksempel på en nødvendig prosess, hvor ulike myndighetsnivåer kobles sammen på en hensiktsmessig måte. Vurderingen av hvordan risikoanalyser best kan gjennomføres, med strukturerte arbeidsprosesser med behov for klare målsettinger og rammebetingelser, gir bidrag til avklaringen av hvilke arbeidsprosesser som kan fungere. PhD-arbeidet forventes å gi større innsikt i effektivitet av sikkerhetstiltak og måleteknikker.

Det er også verdt å peke på at de tidligere BAS-prosjektenes metodiske tilnærming eksemplifiserer hvordan strukturerte arbeidsprosesser kan gjennomføres for hele nasjonale infrastrukturer. Mye kunnskap finnes derfor allerede på dette området. Utfordringen ligger i å benytte kunnskapen som allerede finnes i det praktiske sikkerhetsarbeidet.

6.3 Tiltak

Myndighetene vil normalt ha et spekter av virkemidler for å understøtte arbeidet med informasjonssikkerhet i samfunnet, bl.a. lovverk og forskrifter, ulike finansieringsmodeller for sikkerhetstiltak osv. Disse virkemidlene kan benyttes for å gjennomføre ulike typer sikkerhetstiltak. På nasjonalt nivå vil de prinsipielle tiltakene i hovedsak tilhøre tre kategorier.

1) Sårbarhetsreduserende tiltak i tjenestesystemene
2) Beredskapstiltak knyttet til produksjon eller anvendelse av tjenester
3) Tilrettelegging og rammebetingelser

Til den første kategorien tiltak inngår for eksempel krav til grunnleggende redundans i ulike deler av nettinfrastrukturen til ”viktige” tjenesteleverandører. Dette kan også dreie seg om ulike former for fysisk beskyttelse av viktige infrastrukturelementer. Stortingsmelding 47 inneholdt flere slike tiltak [8].

Imidlertid vil FFI hevde at det nasjonale handlingsrommet til å innføre denne typen tiltak er sterkt redusert i dag, i alle fall dersom de skal komme som krav fra offentlige myndigheter overfor virksomhetene. Utviklingen innen Internett har gitt betydelige bidrag til denne utviklingen [17]. Det anses derfor som lite hensiktsmessig at myndighetene går inn og krever at denne typen tiltak iverksettes, på bakgrunn av egne sårbarhetsanalyser. *I stedet bør offentlig aktører som kunder av*

IKT-baserte tjenester bli foregangsvirksomheter når det gjelder å stille kompetente krav til sikkerhet, og derigjennom motivere til at sårbarhetsreduserende tiltak iverksettes av leverandørene selv. Inntrykk samlet inn gjennom BAS-prosjektene over tid har vist at offentlige kunder ofte har vært svake i denne sammenhengen. I hovedsak bestiller man de tjenestene som er rimeligst, uten hensyn til sikkerhet.

Til den andre kategorien inngår tiltak for å bistå aktørene i markedet med å redusere konsekvensen av svikt i tjenesteproduksjon. Dette kan dreie seg om tilsyn med at beredskapsplaner utvikles og følges ut fra en standard. Dette kan også bestå av å arrangere faglig samarbeid mellom konkurrerende aktører på området, og arrangere ulike typer samøvelser for å øve på beredskapsutfordringer. En beredskapsplan har liten verdi hvis den ikke øves og er kjent av dem som skal bruke den.

Innenfor den tredje kategorien inngår å sikre at relevant informasjon om sikkerhet flyter mellom tjenesteleverandørene innen IKT og deres kunder, og at det etableres hensiktsmessige kundeavtaler dem i mellom. Herunder kommer også å utvikle bred informasjon om sikkerhet til ulike typer kundegrupper, for eksempel i form av "best practices". Hensikten med dette er at en kunde i størst mulig grad skal vite om hvilken grad av sikkerhet en IKT-basert tjeneste innehar. Dette for å kunne forstå den risikoøkning egen virksomhet påføres som følge av IKT-anvendelsen. I tillegg kan arbeidet rettes direkte mot leverandørene, gjennom utvikling av veiledninger for sikkerhetsarbeidet osv.

Uansett hvilke tiltak man søker å iverksette, er det viktig at disse kobles tett mot en prosess som er beskrevet i kapittel 6.2, med klare ambisjonsnivå, målbare beslutningskriterier og en sporbar arbeidsprosess.

6.4 Anbefaling

Vår vurdering er at det fremdeles er viktig at myndighetene har et ansvar for utviklingen innen sikkerhet og robusthet i IKT-systemer. Dette ansvaret må imidlertid i stor grad baseres på et tett integrert samarbeid med operatørene og virksomhetene innen de ulike samfunnskritiske funksjonene, ikke minst på grunn av kompetansebehovet som enhver regulering av sikkerhet innenfor IKT-området medfører. Det bør også spesifiseres et ambisjonsnivå for sikkerhetsarbeidet som er realistisk, gitt dagens rammebetingelser. Deretter vil tiltak naturlig kunne identifiseres basert på et slikt ambisjonsnivå, så lenge man har en god og løpende prosess for sikkerhetsarbeidet.

7 Avslutning

7.1 Oppsummering

IKT-systemer og IKT-baserte infrastrukturer er av grunnleggende betydning for svært mange tjenester i samfunnet. Det kan antas at konsekvensene vil bli store dersom svikt i

samfunnskritiske IKT-systemer oppstår og blir av en viss varighet. Et hensiktsmessig sikkerhetsarbeid er derfor viktig, men å oppnå god IKT-sikkerhet er en krevende oppgave. IKT-systemer er i sin natur komplekse, og i tillegg er de preget av en rask teknologisk utvikling. Å finne metodiske tilnærminger som kan fungere under slike rammebetingelser og gi hensiktsmessige svar er derfor en utfordring.

Det er likevel BAS5-prosjektets oppfatning at arbeidet med IKT-sikkerhet blir best dersom det legges strukturerte arbeidsprosesser med klare rammebetingelser til grunn for arbeidet, uavhengig av om arbeidet skal gjøres av den enkelte virksomhet eller av en offentlig forvaltningsmyndighet.

Den viktigste anbefalingen FFI vil gi i forlengelsen av BAS5 er derfor at nødvendige rammebetingelser settes for at det kan gjennomføres kontinuerlige og metodisk baserte arbeidsprosesser innen arbeidet med nasjonal IKT-sikkerhet.

Dette gjelder både nasjonalt/tverrsektorielt og innenfor de ulike samfunnssektorene. Kontinuerlige prosesser er nødvendige for å holde tritt med den kontinuerlige endringstakten i samfunnet. Nødvendige rammebetingelser for arbeidet med nasjonal informasjonssikkerhet innebærer blant annet et konkret ambisjonsnivå for arbeidet, en avklaring av ulike aktørers roller og oppgaver, og gode metoder som kan understøtte sikkerhetsarbeidet. Det er naturlig å se på dette nå, siden Nasjonal strategi for informasjonssikkerhet i skrivende stund er under revisjon.

BAS5 har i første rekke arbeidet med metoder som har relevans for IKT-sikkerhetsarbeidet i Norge. Målgruppen for de utviklede metodene er dels myndigheter som arbeider med nasjonal IKT-sikkerhet, dels virksomheter som eier og drifter samfunnskritiske IKT-systemer.

Det metodiske arbeidet i BAS5 har vært gjennomført for å understøtte tre hovedmål i prosjektet:

1. Utvikle og anvende metodikk for identifisering og rangering av kritiske samfunnsfunksjoner og IKT-systemer.
2. Utvikle og anvende metodikk for risikoanalyse av samfunnskritiske IKT-systemer.
3. Utvikle og anvende metodikk for effektivitetsvurderinger av tiltak som kan redusere sårbarheter i IKT-systemer.

Knyttet til det første målet har prosjektet utviklet en metode og en prosess for identifisering og prioritering. Denne er foreløpig ikke testet ut, men det anbefales at dette gjøres i etterkant av prosjektet.

Knyttet til det andre målet har prosjektet utviklet en prosess for risikoanalyser av samfunnskritisk IKT som ivaretar både tilsiktede og ikke-tilsiktede hendelser, et rammeverk som understøtter valg av analysemetodikk og en veileder for støtte til personer som skal gjennomføre risikoanalyser.

Det tredje målet er i hovedsak koblet til prosjektets doktorgradsarbeid, som foreløpig ikke er avsluttet. De innledende arbeidene er likevel presentert som vedlegg til denne rapporten.

Prosjektet har vært et møtested for forskningsinstitusjoner, akademiske institusjoner, myndighetene og ulike offentlige og private virksomheter. Delmålsettingen om tettere koblinger mellom BAS-prosjektene og akademia er godt ivaretatt.

Prosjektet har ikke foreslått konkrete kostnads- og effektivitetsberegnede tiltak for det nasjonale sikkerhetsarbeidet, men har pekt på behovet for nytenkning rundt det offentliges rolle i IKT-sikkerhetsarbeidet. Historisk sett har det ikke vært mangel på forslag til tiltak innen IKT-sikkerhetsområdet, men heller manglende rammebetingelser for at tiltak kan utvikles og inngå i en helhetlig og kontinuerlig arbeidsprosess. Et forslag til nødvendige avklaringer og overordnede tiltak er derfor presentert som en del av denne rapporten.

7.2 Videre arbeid

BAS5-prosjektet har favnet vidt og bredt over mange tema knyttet til sikkerhet i samfunnskritiske IKT-systemer. Enkelte steder har prosjektet kun gjort overordnede vurderinger, og når BAS5 nå avsluttes er det flere tema som kan tas videre i mer detaljerte oppfølgingsarbeider. *Det anbefales derfor at det i forlengelsen av BAS5 arbeides videre med relaterte metodiske problemstillinger*. Dels vil dette være å teste ut metodikkene som er utviklet og foreslått i løpet av BAS5. I tillegg har prosjektet pekt på enkelte områder hvor det er viktig med ytterligere forskning og utredning. Disse presenteres i det følgende.

Prioritering og identifisering av ulike forhold

- Metodikken for identifisering og prioritering av samfunnskritisk IKT inneholder foreløpig ikke prosesser eller teknikker som er spesielt rettet mot oppdagelse av hittil ukjent risiko, for eksempel scenarioteknikker, foresight-teknikker eller horizon scanning-teknikker. Hvordan slike best kan inngå i prosessen er en viktig avklaring. I parallell med dette bør et foreslått hierarki over ulike scenarier som kan inngå i prioriteringsarbeidet utvikles videre og underkastes nærmere analyse, med hensyn på å identifisere de viktigste scenariene og sile fra scenarier som er mindre plausible.
- Det er også behov for en nærmere kritisk gjennomgang av på hvilke områder en prioritering faktisk gir mening. En spesiell problemstilling er hvorvidt på forhånd fastsatte prioriteringer faktisk vil avhjelpe en krisesituasjon, eller om det kan være til hinder for krisehåndteringen der og da.
- I tillegg kan prioritering overfor en spesifikk situasjon sies å være relativt enkelt. Men hvordan kan man best prioritere hensyn på tvers av et bredt spekter av scenarier?

Risikoanalyser

- Hvordan kan tilsiktede hendelser best inkluderes i risikoanalyser? En spesiell utfordring er hvordan sannsynlighets- og usikkerhetsvurderinger av slike hendelser bør behandles metodisk.
- Hvordan kan strategiske sikkerhetsinitiativer og lokale ROS-analyser best kobles? Resultatene fra BAS5-prosjektets delmål 1 og 2 bør derfor viderebehandles og integreres i større grad enn nå.
- Hvordan kan andre sikkerhetsteknikker inngå i og understøtte en risikoanalyse av

samfunnskritisk IKT? Eksempler på slike teknikker er bruk av sjekklister, penetrasjonstester, tradisjonelle sårbarhetsanalyser av IKT-systemer osv.

- Hvordan kan følgekonsekvenser utenfor IKT-systemet best behandles i en risikoanalyse? Spesielt problematisk er konsekvensene for storsamfunnet som er avhengige av tjenester understøttet av IKT-systemet. Den enkelte virksomhet vil sjelden ha tilstrekkelig kompetanse om slike forhold eller ressurser til å gjennomføre en detaljert analyse.

Arbeid med nasjonal IKT-sikkerhet

- Rapportens forslag til tiltak og prosess for det nasjonale IKT-sikkerhetsarbeidet er basert på erfaringer fra FFIs arbeid med IKT-sikkerhet i flere år, og presenteres som et innspill til debatt. Denne debatten er svært viktig for å bringe arbeidet med IKT-sikkerhet i Norge et nødvendig steg videre. I forlengelsen av dette kan det imidlertid være behov for ytterligere utredninger, for eksempel knyttet til hvilket trusselbilde man skal planlegge IKT-sikkerhetsarbeidet mot, hvilke roller og oppgaver ulike aktører bør ha og hvilke tiltak og virkemidler som er best egnet for det nasjonale sikkerhetsarbeidet i tiden fremover.

Appendix

Appendix A Bakgrunnsstudier

BAS5 har gjennomført flere bakgrunnsstudier, som har hatt som primært formål å understøtte arbeidet med hovedmålsettingene i prosjektet. Bakgrunnsstudiene presenteres overordnet i dette kapittelet.

A.1 Fremtidig teknologiutvikling med fokus på nanoteknologi

Som en del av BAS5-prosjektet ble det gjennomført en studie av nanoteknologi. Hovedårsaken til dette er at nanoteknologi vil stå sentralt i utviklingen av IKT-kapasitet i årene som kommer, og prosjektet ønsket å få nærmere oversikt over teknologiutviklingen verden vil oppleve fremover. Arbeidet er dokumentert i en egen FFI-rapport [18].

Nanoteknologidomenet defineres ofte å strekke seg fra 0,1 – 100 nanometer (nm), hvor en nanometer er det samme som en milliondels millimeter. Dette er også størrelser som man finner på atomnivå – for eksempel er en typisk atomavstand i krystaller 0,3 nm.

Den enorme utviklingen som vi har sett i halvlederindustrien de siste 30 årene, med en fordobling av regnekapasiteten til mikroprosessorene hver 18. til 24. måned, ser ut til å nå en grense rundt år 2015 – 2018. For å opprettholde utviklingen må størrelsen på den enkle transistoren i prosessoren reduseres, og det må pakkes flere transistorer på hver prosessor.

En tilsvarende utvikling observerer man i datalagringssystemer. Forventningen er at den eventyrlige veksten i kapasitet man har sett til nå vil avta. Dataratene som de magnetiske medier kan leses med, øker raskere enn halvlederteknologien klarer å håndtere, og det forventes at andre teknologier (ikke-magnetisk, holografi, atomnivå) må overta. Den sistnevnte er innenfor nanoteknologidomenet.

Foreløpig står nanoteknologien ved begynnelsen, og antallet kommersielle suksesser er beskjedent. Men utviklingen går fort, oppmerksomheten som teknologien får er nå stor, og myndighetene i de fleste land har store forventninger til nanoteknologi og legger til rette for at teknologien overføres raskt til produktutviklere. Det økonomiske potensialet anses å være stort.

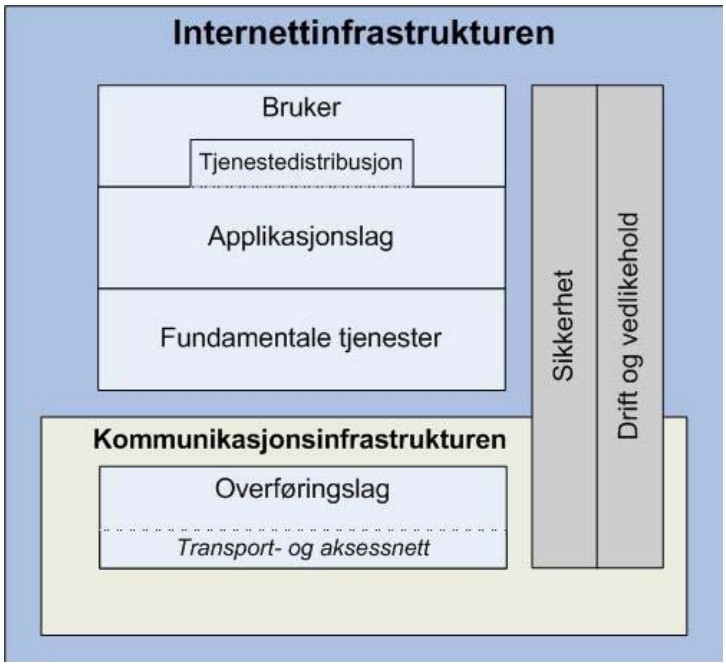
A.2 Sårbarhet i Internett

Som grunnlag for metodearbeidet og tilhørende casestudier i BAS5-prosjektet, ble det satt i gang et arbeid med sårbarhetsvurdering av internettinfrastrukturen [17]. Formålet var å gjøre en sårbarhetsvurdering med basis i anvendelsen av internettbaserte tjenester til produksjon av egne varer og tjenester som er viktige for det moderne samfunnet. Studien avgrenset seg til den norske delen av Internett.

Et viktig utgangspunkt for arbeidet var å gi økt kunnskapsoppbygging for bedrifter som skal gjøre

risikoanalyser av IKT-systemer som er koblet til Internett. Et annet utgangspunkt var å synliggjøre sårbarheter i Internett for beslutningstakere i offentlig forvaltning. Med andre ord har dette arbeidet hatt et klart ”voksenopplæringspreg”.

Fra et teknisk synspunkt utgjør Internett et nettverk av funksjoner. Disse kan modelleres i en lagdelt modell. BAS5 har utviklet en slik lagdelt modell over internettinfrastrukturen, som omfatter både brukere, organisatoriske aspekter og teknologi. Som en del av infrastrukturen inngår kommunikasjonsinfrastrukturen som dekker de nødvendige lagene for å frakte IP-pakker fra kilde til destinasjon, se Figur A.1. Sårbarheter i Internett drøftes sett i forhold til de ulike ”lagene” i denne modellen.



Figur A.1 Lagdelt modell av Internett

En viktig bakenforliggende årsak til sårbarhetene på Internett er ulike virksomheters naturlige fokus på egne hensyn fremfor fellesskapets beste. Dette fører til et fokus på økonomiske hensyn fremfor oppfyllelse av et ansvar som ikke er understøttet av positive eller negative insentiver. Global informasjonssikkerhet er på mange måter et felles gode som lider under dette prinsippet, når et eventuelt bidrag føles større enn det direkte utbyttet. Dette kan også føre til ansvarsfraskrivelse som en del av en virksomhetsforretningsmodell, noe som er svært tydelig innenfor programvareindustrien, gjennom blant annet lisenshåndtering. Regulering på dette området, både i global og nasjonal kontekst, er svært problematisk.

Vår sårbarhetsvurdering er svært sammensatt, og det fremkommer ingen entydig konklusjon. På den ene siden viser våre funn at Internett er sårbar for mange ulike angrep på de forskjellige lagene i referansemodellen, i form av utnyttelse av avhengigheter og fysiske, logiske og sosiale sårbarheter. Mange av disse sårbarhetene er velpubliserte, samtidig som det også kontinuerlig gjennomføres tiltak i infrastrukturen for å redusere disse. Eksempler på slike sårbarheter ligger i viktige funksjoner som ruting (Border Gateway Protocol) og navnetjeneste (Domain Name

Service). På den annen side er det, til tross for disse mer eller mindre kjente sårbarhetene, ikke dokumentert angrep mot Internett med omfattende konsekvenser i tid og omfang. Spørsmålet man da må stille seg er hvorfor, siden infrastrukturen tilsynelatende har mange sårbarheter. Et mulig svar er at de som har kapasitet til å utføre angrep selv er avhengige av Internett. Et annet svar er at Internett, tross sine mange enkeltsårbarheter, virkelig er en robust infrastruktur.

Vi har tro på begge svar, og antar at en viktig grunn til denne tilsynelatende robustheten er den høye kompleksiteten og dynamikken som ligger i Internett. For eksempel er det sterke innebygde funksjoner for å rute IP-pakker automatisk alternative veier ved feil/angrep. Viktige tjenestefunksjoner utstyres med redundans i eget nett, og i samtrafikk med andre internettilbydere. Denne kompleksiteten og dynamikken fører imidlertid til at drift av Internett sett fra hver operatørs ståsted er blitt et håndverk, der det kreves tilgang til svært høy kompetanse på døgnkontinuerlig basis.

Dette siste er antagelig den viktigste faktoren for at Internett i dag tross alt har utviklet seg til å bli en i hvert fall tilsynelatende robust og tilpasningsdyktig struktur. Imidlertid er det ikke sannsynlig at det i en så vidt kompleks struktur som Internett kan unngås svikt som følge av angrep eller feilfunksjoner. Det viktigste tiltaket for å redusere konsekvensene av slik svikt er rask tilgang på håndverkere som sørger for å redusere skade og skadeomfang, og deretter reetablerer tjenestetilbudet til sluttbrukerne.

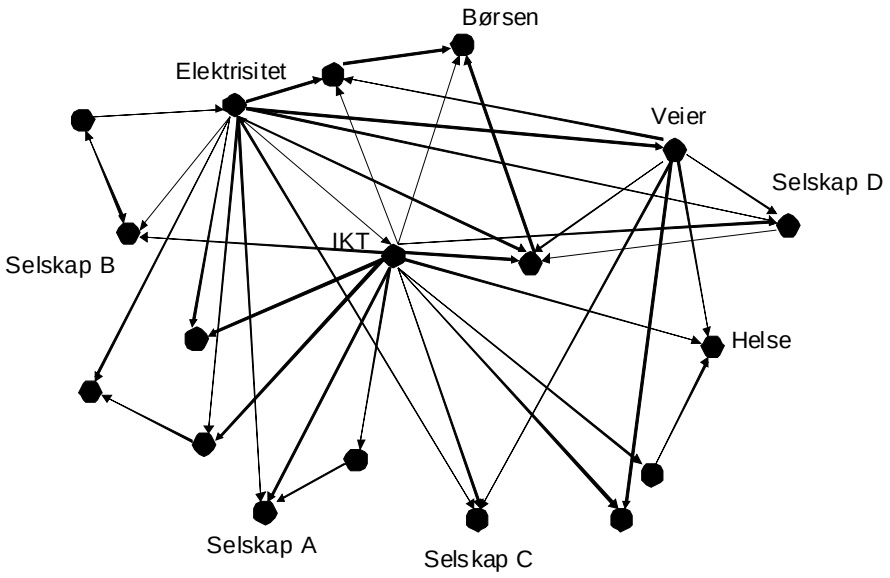
En sentral faktor i sårbarheten av Internett er den grunnleggende og i stor grad fysiske kommunikasjonsinfrastrukturen. Denne utgjør basis for alle internettjenester. Det er en klar trend at dagens nettverk og tjenester for elektronisk kommunikasjon (EKOM) migreres mot bruk av IP-teknologi. Dette innebærer at alle tidligere separat produserte EKOM-tjenester legges over på en felles IP-basert plattform, blant annet tradisjonell telefoni, kabel-TV, internettjenester og mobiltelefoni. IP-teknologien er dermed i ferd med å bli en felles plattform for alle EKOM-tjenester som produseres, noe som får direkte innflytelse på nettinfrastrukturens egenskaper og dens robusthet. Dette anses å få betydelig positiv betydning for robustheten til tjenestene, ved at i hvert fall de større operatørene baserer alle sine tjenester på en felles robust nettverksplattform. En slik felles plattform kan selvfølgelig også innebære sårbarheter, men det er vår vurdering at nettoeffekten er klart positiv.

A.3 Grafteori

Usedvanlig rask teknologisk utvikling, spesielt på IKT-området, har ført til at samfunnet har blitt mye mer komplekst og uoversiktlig de siste ti årene. Kompleksiteten er i seg selv en trussel, fordi det er vanskelig å forstå hvordan uheldige og til dels skadelige sammenhenger i et så komplekst system som samfunnet oppstår.

En farbar vei mot slik forståelse er å ta i bruk den nyeste kunnskap om nettverk eller grafer. Dette er innsikt som er fremkommet i løpet av de siste fem årene. Kunnskapen er fortsatt så ung at den kun i liten grad har trengt inn i undervisningen og forskningen rundt sårbarhet. Prosjektet fikk utarbeidet et notat om dette av Jan Audestad, professor ved Telenor/Høgskolen i Gjøvik [19].

Grafteori er et eget område innen matematikken, hvor systemer kan beskrives som grafer med noder (punkter) og en mengde kanter (hver kant forbinder to noder med hverandre). Eksempelet i Figur A.2 viser hvordan samfunnet kan representeres som en graf, der infrastruktur og produksjon i samfunnet er avhengig av hverandre. Ved å gjøre beregninger på grafen er det mulig å identifisere hvilke noder som er sentrale for systemets robusthet, og hvilke som ikke er så kritiske.



Figur A.2 Samfunnet som nettverk

Grafteori er en interessant tilnærming til analyser av komplekse systemer, og det er vel verdt å følge med på utviklingen innen dette feltet fremover. Metodikken ble vurdert, men ikke benyttet i BAS-prosjektet. BAS5 var imidlertid i kontakt med personell ved Høgskolen i Gjøvik om dette, blant annet med formål å anvende teknikken på en analyse av sårbarheten i Internett. Hovedårsaken til at dette ikke ble gjort i BAS5 er det samme problemet man står overfor i forbindelse med risikoanalyser av IKT-systemer: hvordan klarer man å fremskaffe nok informasjon av analysesystemet til at man klarer å lage en representativ modell?

A.4 Myndighetenes rolle innen informasjonssikkerhet - forebygger og kriseleder

BAS5-prosjektet har gjennomført flere studier som har berørt temaet IKT-krisehåndtering og det offentliges rolle innen informasjonssikkerhet. Disse oppsummeres i det følgende.

A.4.1 Nasjonal strategi for informasjonssikkerhet

I forprosjektet til BAS5 var et mål å skaffe oversikt over det internasjonale arbeidet innenfor informasjonssikkerhet, dog med vekt på å kartlegge de initiativer ulike stater har tatt i forhold til utfordringen som ligger i avhengigheten av åpne, verdensomspennende og sårbare informasjonsnettverk [20]. BAS5 valgte å fokusere på Norge, USA, Australia og EU.

USA ble valgt fordi USA er ledende i bruk av ny forsvarsteknologi og i å tenke på nasjonal sikkerhet. Australia ble valgt fordi Australia representer et annet kontinent, som på mange måter er likt med Norge i form av stor geografisk utbredelse og spredt bebyggelse. Det ble også naturlig å skjele til hva EU gjør på dette området, som en overbygning for flere europeiske stater og som en handelspolitisk premissgiver for Norge.

Studien belyser i hvilken grad arbeidet med informasjonssikkerhet på nasjonalt nivå har materialisert seg i strategier med avklart ansvarsområde og konkrete tiltak, og hvilket fokus strategiene har mht. trusler og innretning av sikkerhetsarbeidet.

Både USA, Norge og EU har strategidokumenter relatert direkte mot informasjonssikkerhet på nasjonalt nivå. USA har, slik vi tolker, et vesentlig større fokus på viljeshandlinger og planlagte ondsinnede anslag enn det Norge har. Imidlertid må det legges til at det norske regimet innen telesikkerhet og -beredskap har større fokus mot høynivåtrusler enn det som går frem av det nasjonale strategidokumentet for IKT-sikkerhet.

Australia har ikke noe strategidokument, så langt vi har sett, men har allikevel implementert en rekke tiltak og gjort mye innenfor området informasjonssikkerhet. Det australske fokuset synes også å være mer fredsrettet, blant annet er fysisk redundans i nettene et ”ikke-mål”. Når det gjelder tiltak for øvrig er det mye som er felles. Det er opprettet organisasjoner som har ansvar for å være meldingssentraler ved datainnbrudd og -angrep, ha rådgivende funksjoner med mer, og det satses på å bygge sikkerhetskultur, å heve kunnskapsnivået gjennom utdanning og forskning, på internasjonalt samarbeid, harmonisering av lovverk, Public Key Infrastructures (PKI) og sertifiseringsordninger for informasjonssikkerhet. De nasjonale variasjonene går på plassering av ansvar og vektleggingen av samarbeid mellom private og offentlige virksomheter. USA er spesielt i så måte, fordi landet har hatt et liberalisert markedsregime innenfor kritisk infrastruktur lengst. Dermed er privatiseringen kommet lengst her, og samarbeidet med privat sektor er dermed svært viktig.

Denne studien utgjør en bakgrunnskunnskap i forhold til senere studier i BAS5, av blant annet tilsynspraksis. Det kan nevnes at det for tiden arbeides med en revisjon av den norske nasjonale strategien for informasjonssikkerhet.

A.4.2 Infrastrukturbeskyttelse i USA

USA er i en særstilling internasjonalt når det gjelder satsing på kritisk infrastrukturbeskyttelse, og prosjektet ønsket nærmere kontakt med aktører i USA som har roller knyttet til dette arbeidet. BAS5 arrangerte derfor en studietur til USA høsten 2005 [21]. Følgende institusjoner ble besøkt:

- IT – Information Sharing and Analysis Center, Atlanta
- George Mason University, Washington
- Den norske ambassaden, Washington
- Department for Homeland Security, Washington
- Sandia National Laboratories, Albuquerque
- North American Electric Reliability Council, Princeton

Det er en overveldende oppgave å prøve å ta inn over seg amerikanernes samlede satsing innen området kritisk infrastrukturbeskyttelse, ikke minst på bakgrunn av en håndfull møter. Amerikanerne har økonomiske og personellmessige ressurser innen dette området som andre land bare kan drømme om, og totalt er det produsert en imponerende mengde strategier, rapporter og plandokumenter om temaet.

Noen metodikker for analyser av kritisk infrastruktur finnes også, men disse er vanskeligere å omsette til nytte på norske problemstillinger. Dels er dette et utslag av at metodene krever store ressurser (under turen ble det referert til et nylig oppstartet initiativ knyttet til bl.a. Sandia National Laboratories, der 300 personer har blitt øremerket for modellering av gjensidige avhengigheter i kritisk infrastruktur), men også at det pga. sikkerhetshensyn er vanskelig å hente ut direkte anvendbar informasjon. Det må også tillegges at heller ikke amerikanerne har klart å fremstille enkle og gode metodikker for prioritering av samfunnsfunksjoner.[14]

Til tross for at det ikke ble identifisert mye konkret metodikk som var anvendbar for prosjektet, var turen nyttig av flere hensyn:

- Det ble understreket at problemstillingene prosjektet arbeider med er relevante, også i andre land
- Prosjektet fikk flere innspill til hvordan det kan tenkes helhetlig innen sikkerhet og beredskap

A.4.3 Offentlig tilsyn og veiledning i forhold til informasjonssikkerhet

BAS5 har studert tilsynspraksis i norsk finans- og kraftsektor og sett den norske praksisen opp mot praksis i Sverige, Danmark, Finland og UK [22]. Prosjektet har også, men i mindre grad, studert tilsynspraksisen innenfor NSM og Datatilsynet, siden disse har grenseflater mot de sektorene vi har valgt som studieobjekt. Studien ble i første rekke gjennomført som støtte til arbeidet med effektivitetsvurderinger av tiltak, med utgangspunkt å se på om tilsynsprosesser kan fungere som grunnlag for å utvikle sikkerhetsmetrikker.

Det kreves lovhjemler for å føre offentlige tilsyn. Uten lovhjemler blir det heller ikke noe tilsynsprosess, og uten relevante lovhjemler blir det heller ikke et myndighetsfokus på relevante forhold. BAS5 har observert at ulikheter i lovverket også gjenspeiles i ulik tilsynspraksis mellom de ulike landene i studien. Studien viser at Norge bruker offentlig tilsyn med informasjonssikkerhet som virkemiddel i større grad enn de andre landene i studien. IKT-forskriften [23], som har sin anvendelse i finanssektoren, er i en særstilling ved at den alene fokuserer på informasjonssikkerhet. Vanlig praksis ellers er at informasjonssikkerhet er inkludert i andre forskrifter (for eksempel i den generelle beredskapsforskriften i kraftbransjen).

En suksessfaktor for at lovverket skal bli fulgt, er klare retningslinjer. De norske tilsynene i undersøkelsen, NVE og Kredittilsynet, utarbeider slike. I tillegg drives opplæring og rådgivning

[14] At et lite prosjekt fra Norge arbeidet med en såpass kompleks problemstillingen vakte en viss munterhet i epartment of Homeland Security. BAS5 ble oppfordret til å ringe og si ifra dersom vi fant løsningen.

overfor de virksomheter som er underlagt tilsynsmyndigheten. Tilsynsmyndighetene har også sanksjonsmuligheter overfor virksomheter som ikke følger loven. Selv om disse varierer i karakter mellom ulike tilsynsmyndigheter, så har alle de norske myndighetene som deltok i studien så sterke sanksjonsmuligheter at de virker avskrekkende. Klare retningslinjer, opplæring og sanksjonsmuligheter vil sammen bidra til at myndighetene oppnår effekt av loven.

BAS5 har observert at tilsynsprosessen stort sett følger samme mal på tvers av myndigheter og land: Varsling (som kan utelates), innhenting av skriftlig informasjon, tilsynsmøte, supplering med mer informasjon, rapport til virksomheten, tilsvar fra virksomheten, og endelig rapport med pålegg/tiltak. I etterkant følger gjerne opplæring.

Verktøyene som tilsynsmyndighetene bruker, er stort sett spørreskjema med ja/nei svar, der nei betyr avvik. Det er altså klare grenser for hva som er akseptert og hva som ikke er akseptert. Måleverktøyene varierer imidlertid. Kredittilsynet bruker egenutviklede COBIT[15]-skjemaer. Datatilsynet baserer sitt opplegg på standarden NS-ISO/IEC 17799. NVE har egenutviklede spørsmål med forankring i lovteksten, og NSM har en spørsmålsbank der tilsynsmyndigheten utøver stor grad av skjønn og bruker loven som baseline for sikkerhetsnivået.

Med referanse til teori om metrikker og indikatorer, synes det som om det kan være et potensial for å utvikle måleindikatorer innenfor tilsynsmyndighetenes virkeområde. NVE har på en måte tatt ett steg i denne retning med å beregne prosentandelen av nei-svar, sortert på virksomhet og tema. Selv om dette er enkle indikatorer, kan de (dersom de blir laget over samme spørsmål og over tid) gi informasjon om trender og utviklingstrekk når det gjelder hvor flinke virksomhetene er til å følge loven.

Kredittilsynets COBIT-skjema ville også kunne være et grunnlag for måleindikatorer eller metrikker etter modell av NVE; prosent nei-svar fordelt på prosess og tema, og prosent nei-svar fordelt på virksomheter over tid. Kreditttilsynet vurderer å utvikle slike indikatorer. Styrken med Kredittilsynets COBIT-metodikk er bredden og den standardiserte metoden som gjelder for alle virksomheter.

Avslutningsvis må det påpekes at BAS5 ikke har vurdert effekt av offentlig tilsyn opp mot effekt av andre mekanismer, for eksempel markedets makt som regulator, der sikkerhet er en premiss for tillit mellom kunde og virksomhet. Det som derimot synes klart er at lovverk og offentlig tilsyn tvinger toppledelsen til å følge opp informasjonssikkerheten, blant annet ved at representanter fra ledelsen er med på tilsynsmøtene og må svare på spørsmål. I tillegg sendes tilsynsrapportene innen finansnæringen til styret i foretakene. Sett i lys av toppledelsens distanserte forhold til informasjonssikkerhet (ansvar for informasjonssikkerhet er ofte plassert lavere i organisasjonshierarkiet) er dette positivt.

A.4.4 IKT-krisehåndtering

Begrepet “IKT-krise” er definert i [24] som en situasjon der informasjons- og

[15] Control Objectives for Information and related Technology

kommunikasjonssystemer blir satt ut i en grad som gjør at situasjonen ikke kan håndteres med ”vanlig” bemanning og normale rutiner. BAS5 utviklet tre IKT-krisescenarier for å studere evnen til nasjonal krisehåndtering: teknisk driftssvikt, naturlig årsak og sikkerhetspolitisk krise. Disse tre scenariene ble grunnlaget for en analyse av norsk krisehåndtering på IKT-området. Samtidig ble det gjort en sammenlignende studie av organisering og praksis i Italia og Frankrike.

Til grunn for organisering av samfunnssikkerhet i Norge, ligger sektorprinsippet og prinsippene om *ansvar, likhet og nærhet*. Ansvarsprinsippet innebærer at den som har et ansvar i en normalsituasjon, også har ansvar i kriser. Likhetsprinsippet betyr at kriseorganisasjonen skal være mest mulig lik den organisasjonen man opererer med til daglig. Prinsippet om nærhet går ut på at krisen skal håndteres på lavest mulig nivå. Disse prinsippene gjennomsyrer beredskapstankegangen i Norge, og innebærer at hver sektor blir ansvarlig for å etablere beredskapsplaner og ta høyde for krisesituasjoner.

BAS5-studien viser at det eksisterer klare linjer på hvem som skal håndtere *konsekvensene* av en IKT-krise, men problemet kommer når man skal definere hvem som eier selve IKT-krisen. Ettersom IKT-problemene uansett må løses på laveste nivå, kan man diskutere hvorvidt *eierskapet* til IKT-krisen er et reelt problem. Utfordringen i dag ligger i å tenke på IKT som sektorovergripende, isteden for å bruke ressurser på å ”lete” etter en eier til krisen. Dette krever at man løfter blikket opp fra sektorprinsippet og begynner å tenke mer helhetlig.

I en krisesituasjon vil det være helt nødvendig å ha på plass klare ansvarsavklaringer. En god løsning på dette er eksemplifisert gjennom italiensk praksis. For eksempel vil Innenriksdepartementet i Italia være ansvarlige for krisehåndteringen, inntil krisen eskalerer og det blir fare for liv og helse. På det tidspunktet overføres ansvaret til Statsministerens Kontor. På denne måten vil det være en helt klar rollefordeling uavhengig av hva slags krise det er, selv om ansvarsfordelingen aldri har vært utprøvd ved hjelp av øvelser.

For selve håndteringen av kriser, viser det seg at en enkel sektoravgrenset krise ikke er noe problem, ettersom dette knyttes opp til det ansvarlige sektordepartementet. Problemet oppstår når krisen eskalerer og dominoeffekten mot andre sektorer kommer til syne; hvem skal da koordinere? Myndighetene har få konkrete virkemidler å sette inn ved slike kriser. Det koker ned til at det operative ansvaret vil ligge på hver enkelt virksomhet. Myndighetenes viktigste rolle blir således å sikre at bedriften selv har gode rutiner på plass. Dette involverer både planverk og beredskapsøvelser.

En suksessfaktor for all krisehåndtering er forberedelse *lokalt*, og det blir viktig med et grundig og dekkende planverk, samt bruk av øvelser. Det ser ut til at det foretas en rekke nasjonale øvelser, som i stor grad er begrenset geografisk eller sektorvis. Det som mangler er gjennomføring av storskalaøvelser, som tar hensyn til større geografiske områder, flere sektorer, og med større fokus på sivilmilitært samarbeid. Det er enda ikke gjennomført rene IKT-øvelser, men IKT har vært del av andre beredskapsøvelser, som i forbindelse med forberedelse til år

2000.[16]

Erfaringene fra arbeidet i BAS5 viser at man i situasjoner ved ”fare for liv og helse” har et godt etablert beredskapssystem, noe som skyldes at denne faren har eksistert lenge, og at man har erfaring fra tidligere ulykker og katastrofer. Problemet med IKT-kriser er at dette inneholder et nytt element, ”IKT”. Det kan være en tendens til å tro at dette området er noe veldig nytt, som krever helt nye tenkemåter. Løsningen ligger muligens i å se på dette i forhold til erfaringene man har gjort seg på området ”liv og helse”, og at det dermed kan være tilstrekkelig med mindre tilpasninger.

Ved å studere krisehåndtering i andre land kan det identifiseres mange prosesser som ser bra ut på papiret, med for eksempel etablering av nye nasjonale CERTer[17] og planer for samarbeid mellom offentlig og privat sektor. Vi vet imidlertid lite om hvordan dette vil fungere i praksis, og landene selv har etterlyst øvelser og testing. Studien har ikke gitt noen ”bevis” på hvordan man vil være i stand til å håndtere IKT-kriser. Et fellestrekk for landene er at organiseringen følger nærhetsprinsippet, og at en IKT-krise i hovedsak kan sies å bli oppfattet som en hvilken som helst annen krise.

A.4.5 Behov for IKT i krisesituasjoner

Samfunnet er avhengig av IKT i ordinær drift. Behovet for IT-støtteverktøy vil øke i krisesituasjoner når mange geografisk spredte brukere skal samhandle for å håndtere de utfordringene krisene bringer med seg. I slike situasjoner kan imidlertid ikke alle brukere forvente å ha tilgang til elektroniske støttesystemer og kommunikasjonsmidler. Først og fremst er ikke kommunikasjonsnettene dimensjonert for å håndtere den økte trafikken som lett vil kunne oppstå i kriser. Men i tillegg vil kriser kunne medføre at kommunikasjonsnett blir degradert eller svikter helt.

FFI og DSB arrangerte et arbeidsseminar (workshop) 20. april 2005 som satte søkelyset på denne problemstillingen [25]. Arbeidsseminaret var et samarbeid mellom BAS5-prosjektet og DSBs prosjekt ”Kartlegging av samfunnskritiske funksjoner med behov for prioritet i mobilnettet”. Under seminaret ble det tatt utgangspunkt i et uværsscenario som medførte strømbrudd og dermed redusert tilgang til viktige IKT-systemer. Uværsscenariet ble brukt for å sette søkelyset på evnen til krisehåndtering.

Målsettingen i en krisesituasjon er effektiv krisehåndtering og raskest mulig gjenoppretting av kritiske systemer. De rammede kritiske infrastrukturene (her: tele, kraft, vannforsyning og transport) og nødetatene var de viktigste aktørene i en tidlig fase i scenariet som ble vurdert. Hensynet til liv og helse veide tungt, og både nødetatene og de kritiske infrastrukturene var viktige for å bidra til at hensynet til liv og helse ble ivaretatt. I en tidlig fase er rask varsling og riktig situasjonsbilde svært viktig for hvorvidt man lykkes godt senere.

[16] Ref. møte med Fylkesmannen i Oslo og Akershus, 3.08.05.
[17] CERT = Computer Emergency Response Team

Kriseorganisasjoner på ulike nivå (kommunalt, fylkeskommunalt og offentlig-privat samarbeid) vil bli etablert ettersom krisen vedvarer over flere dager. Etter hvert vil også antallet viktige aktører øke, både på lokalt, regionalt og nasjonalt nivå. Fremdeles er imidlertid gjenopprettingsarbeidet sentralt, slik at strømforsyning og kommunikasjon (helst mobilkommunikasjon) fås i drift igjen raskest mulig.

Appendix B Hvordan vurdere effektivitet av tiltak?

Dette kapittelet beskriver arbeidet med effektivitetsvurderinger i BAS5-prosjektet. I hovedsak er dette arbeidet knyttet til et PdH-stipend ved Høgskolen i Gjøvik, som ikke avsluttes før januar 2009. Kapittelet presenterer derfor de foreløpige resultatene fra arbeidet, og peker på hvilke arbeider som vil bli startet opp den nærmeste tiden.

B.1 Problemstillinger i arbeidet

Etter at en ROS-analyse er gjennomført, vil det være en mengde ulike typer tiltak som kan forbedre informasjonssikkerhet og redusere risiko. Slike tiltak kan være av preventiv art (f.eks. opplæring av ansatte i sikker bruk av epost) eller skadereduserende (for eksempel backup av viktige data). Tiltakene kan også klassifiseres som teknologiske tiltak (der alt fra fysiske låser og nødstrøm til ulike typer sikkerhetsprogramvare inngår) til sikkerhetsdokumentasjon, prosedyrer og rutiner i organisasjonen og opplæring av ansatte.

Sikkerhetsansvarlige har imidlertid budsjetter de skal overholde, og budsjettene gir begrensninger i forhold til hvor mye man kan investere i sikkerhet. Selv om man i etterkant av en ROS-analyse måtte komme fram til at flere tiltak må eller bør innføres, så er det ikke sikkert at de økonomiske midlene strekker til. I en slik situasjon er det viktig at man får mest mulig igjen for sin investering i sikkerhetstiltak. Det er da betimelig å stille spørsmålet: Hva er effekten av disse sikkerhetstiltakene? Virker de?

BAS5-prosjektet studerer effektivitet av sikkerhetstiltak gjennom en PdD-studie ved Høgskolen i Gjøvik, som også er forankret ved Universitetet i Oslo/UNIK[18]. Studien er koblet til BAS5-prosjektet som en ”forlenget arm” i forhold til ROS-analysene, for å kunne hjelpe beslutningstakere med å velge de beste tiltakene. PdD-studien har følgende forskningsspørsmål:

- Hvilke forskjellige betydninger kan legges til begrepet ”effektivitet av informasjonssikkerhetstiltak”?
- Hvilke metoder og metrikker gir gode målinger av effektivitet, og hvilke brukererfaringer finnes mht. å måle effektivitet av sikkerhetstiltak?
- Hvilke metrikker kan gi bedre målinger på effektiviteten av organisatoriske og tekniske informasjonssikkerhetstiltak, bli forstått av ledelsen og bidra til organisasjonens læring?
- I hvilken grad vil støy rundt beslutningsprosessen påvirke måling og rapportering av effektivitet av implementerte sikkerhetstiltak?

Arbeidet har som mål å produsere større innsikt i forhold til forskningsspørsmålene. En del av arbeidet baserer seg på analyse av data fra Mørketallsundersøkelsen i regi av Næringslivets sikkerhetsråd (NSR), NorSIS og Politiets datakrimsenter (PDS).

B.2 Arbeidet med mørketallsundersøkelsen 2006

PhD-prosjektet i BAS5 har fått tilgang til data fra Mørketallsundersøkelsen 2006 [26]. Dette gir

[18] Universitetsstudiene på Kjeller

muligheter for å studere sammenhenger mellom sikkerhetstiltak og datakriminalitetshendelser. I en slik setting må effektivitet av sikkerhetstiltak tolkes som graden av risikoreduksjon, og da med henblikk på frekvensen av rapportert datakriminalitet. I utredning om datakriminalitet foretatt av straffelovrådet i 1985 er det benyttet følgende definisjon [27]:

> *"Datakriminalitet skulle etter dette være straffbare handlinger hvor utnyttelsen av datateknologi har vært vesentlig for overtredelsen og som fører til at en eller flere straffebestemmelser overtredes"*

I undersøkelsen er det valgt å definere mørketall som antall hendelser som virksomhetene kjenner til, men ikke anmelder.

Datamaterialet gir mulighet for å analysere følgende spørsmål: Har virksomheter som har implementert sikkerhetstiltak signifikant mindre risiko for å bli utsatt for datakriminalitet enn virksomheter som ikke har implementert sikkerhetstiltak? Disse spørsmålene kan studeres ved hjelp av statistisk analyse av dataene.

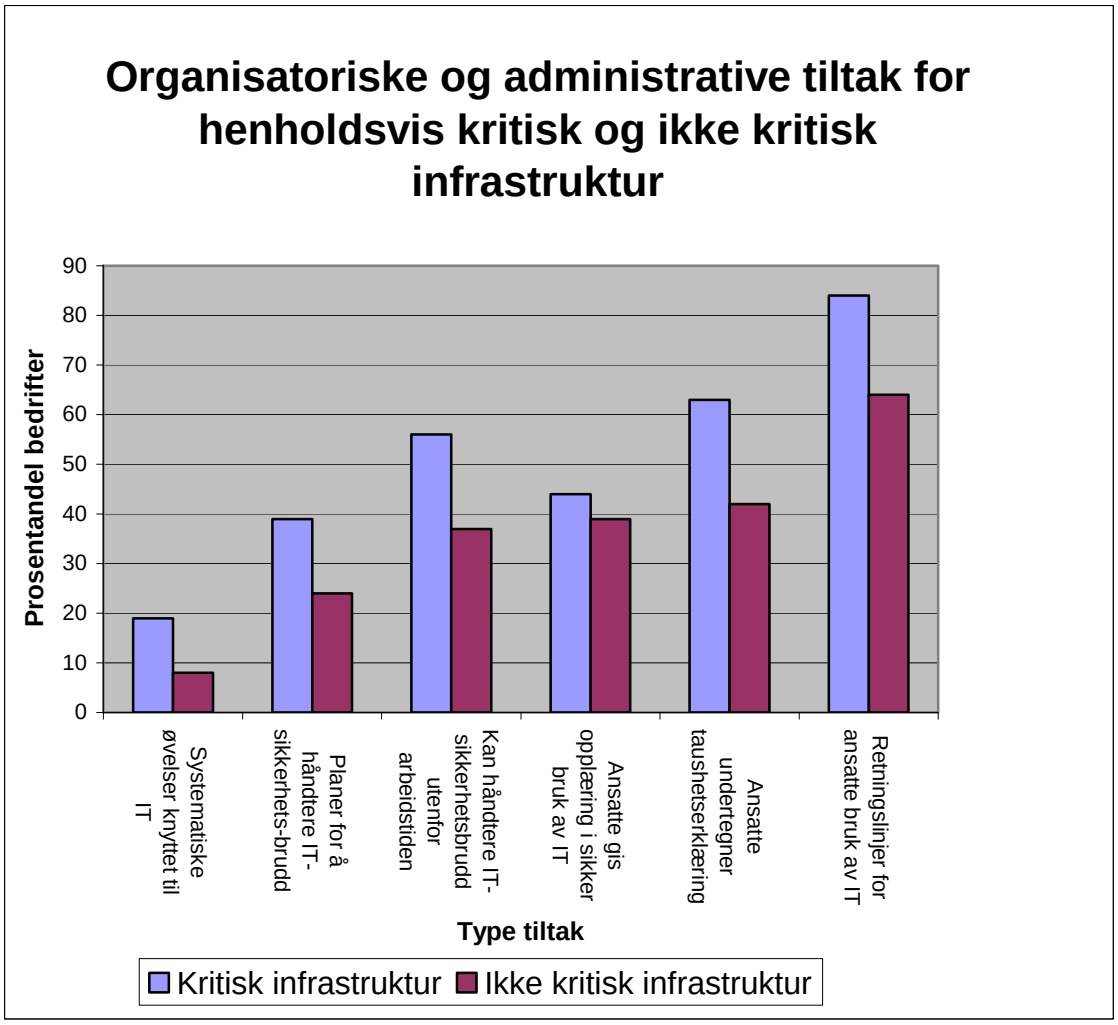
Mørketallsundersøkelsen 2006 er utført som et samarbeid mellom Næringslivets sikkerhetsråd, Politiets datakrimsenter og NorSIS. Spørreskjema ble sendt ut til et representativt utvalg av 2000 norske virksomheter innen offentlig og privat sektor i april 2006, og 749 svar ble mottatt.

I spørreskjemaet ble virksomhetene bedt om å oppgi hvilke tiltak de har satt i verk for å beskytte seg mot datakriminalitet. De ble spurt om hvor mange av forskjellige typer uønskede IT-hendelser de var blitt utsatt for, og hvilke følger disse hendelsene har fått.

B.3 Deskriptiv dataanalyse

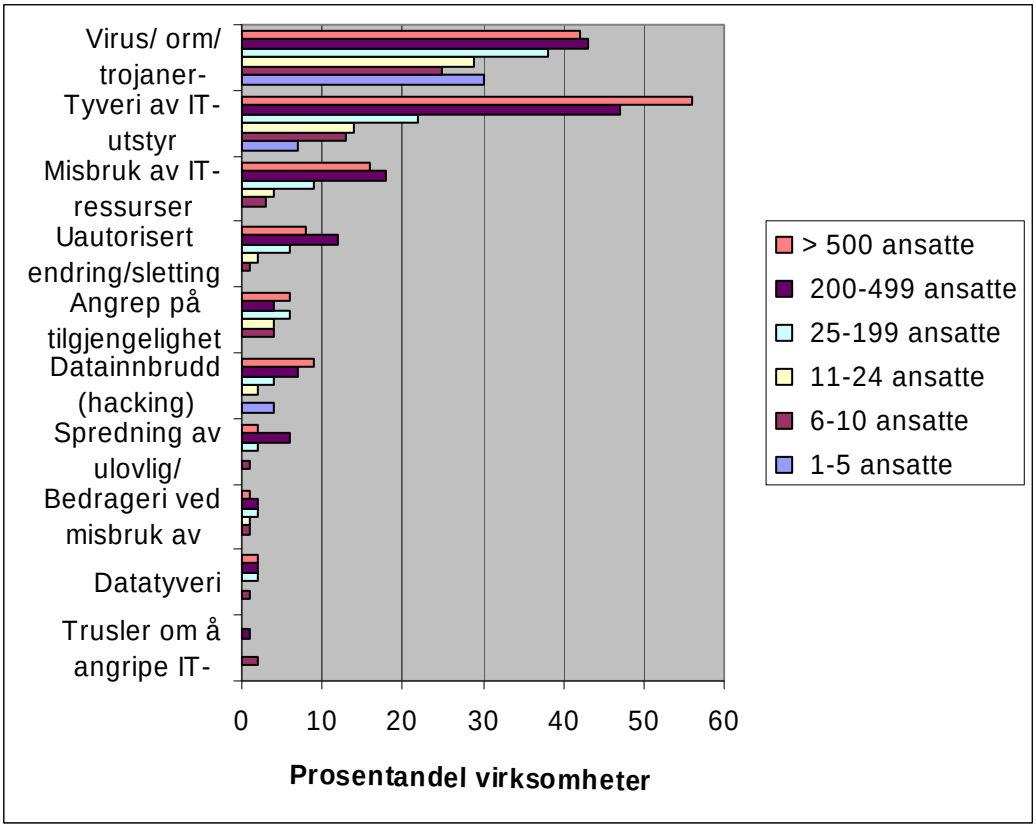
Hovedresultatet fra Mørketallsundersøkelsen er at norske virksomheter er svært avhengige av IT. Svikt i IT og Internett får i løpet av kort tid konsekvenser for inntjening og drift. Til tross for sterk avhengighet av IT, er det påvist store mangler når det gjelder bruk av ulike sikkerhetstiltak. Tradisjonelle tekniske tiltak, som brannmur og passordbeskyttelse, har stor utbredelse blant norske virksomheter. Flere organisatoriske og nyere tekniske tiltak, f.eks. biometri, er vesentlig mindre brukt, særlig blant mindre virksomheter.

I denne Mørketallsundersøkelsen er det satt et spesielt søkelys på virksomheter som anser seg som en del av nasjonal kritisk infrastruktur. Omtrent 10 prosent av virksomhetene som svarte på spørreskjemaet anser seg som en del av nasjonal kritisk infrastruktur. Det er en forholdsvis større andel store virksomheter i gruppen kritisk infrastruktur enn i gruppen andre virksomheter. Som ventet er virksomhetene som anser seg som en del av kritisk infrastruktur flinkere til å beskytte seg gjennom et bredt spekter av sikkerhetstiltak, men det er fortsatt store mangler i beskyttelsen også hos dem. Kartlegging av organisatoriske tiltak er nytt i 2006-undersøkelsen. En grafisk fremstilling av organisatoriske tiltak sortert på tiltak og virksomhet illustrerer forskjellene mellom kritisk infrastruktur virksomheter og andre, se Figur B.1.



Figur B.1 Organisatoriske tiltak [26]

Undersøkelsen har forsøkt å studere nærmere hvilke virksomheter som rapporterer om mest uønskede hendelser og om det finnes en sammenheng mellom sikkerhetstiltak og uønskede hendelser. En konklusjon fra undersøkelsen at store virksomheter rapporterer uønskede hendelser oftere enn de små virksomhetene. En klart større andel store virksomheter har rapportert minst en hendelse i forhold til små virksomheter, se Figur B.2. Det er flere forklaringer på dette, bl.a. at store virksomheter ofte står bedre rustet til faktisk å oppdage hendelser.



Figur B.2 Prosentandel virksomheter som har hatt ulike typer hendelser [26]

Visse bransjer peker seg også ut med høyere rapporteringsgrad. Media/presse, IT/telekommunikasjon og høyere utdanning/forskning er bransjer der 50 prosent eller flere av virksomhetene har hatt ormer, virus eller trojanerangrep. Høyere utdanning/forskning har sammen med kraft/vannforsyning en høyere rapportering av tyveri av IT-utstyr enn andre bransjer. Internasjonale organer og organisasjoner er særlig utsatt for misbruk av IT-ressurser. Undersøkelsen gir ikke grunnlag for å hevde at virksomheter som anser seg som kritisk infrastruktur er mer utsatt enn andre.

Et annet mål med undersøkelsen var å studere sammenhengen mellom sikkerhetstiltak og hendelser. Resultater fra undersøkelsen antyder at det å investere i sikkerhetstiltak på visse områder bedrer oppdagelsesevnen [26].

I [28] gjøres en nærmere vurdering av datagrunnlaget med fokus på aksesskontroll og beskyttelse av lagrede data. Dette paperet drøfter styrker og svakheter ved Mørketallsundersøkelsen, og avslutter med en anbefaling til forbedring av spørreskjema til Mørketallsundersøkelsen vedrørende analyse av aksesskontroll.

Et arbeid med å se på effektiviteten av organisatoriske tiltak er i gang som et samarbeid mellom Janne Hagen og Eirik Albrigtsen, stipendiat ved NTNU. En webbasert spørreundersøkelse danner grunnlaget for analysen som kartlegger tiltak og sikkerhetspraksis og analyserer hvordan respondentene vurderer effektiviteten av de implementerte tiltakene.

B.4 Videre arbeid

Det kan være slik at noen tiltak virker best sammen, eller at det oppnås effekt kun når flere tiltak er aktive. Derfor kan statistiske metoder som tar hensyn til dette være aktuelle for videre analyse av datamaterialet. Etter dette er det aktuelt å vurdere om man skal gjøre ytterlige datainnsamling i virksomheter, for å få en bedre forståelse for svakheter i implementasjon og drift av tiltak, og eventuelt kunne utføre målinger.

Det skal også gjøren en teoristudie på effektivitet av informasjonssikkerhetstiltak, der en søker etter både forståelse av begreper, bruk av ulike metoder, hvilke datakilder som er benyttet og ikke minst hvilket resultat andre forskere er kommet frem til.

Appendix C Administrative erfaringer etter BAS5

Dette appendikset beskriver praktiske forhold rundt BAS5-prosjektets oppstart og gjennomføring.

C.1 Opprinnelig målsetting

Prosjektserien ”Beskyttelse av samfunnet” ble startet opp i 1994. Utgangspunktet for dette arbeidet var å vurdere hovedproblemstillinger for sivilt beredskap etter den kalde krigens slutt. Prosjektene fikk raskt et fokus på sårbarheten i kritisk infrastruktur, og ulike infrastrukturer (telekommunikasjon, kraftforsyning og transport) ble analysert i rekkefølge. Formålet med arbeidene var å analysere sårbarheter i infrastrukturene, vurdere konsekvenser dersom de skulle svikte og anbefale tiltak for å redusere sårbarheter.

I alle BAS-prosjektene så man hvordan IKT-systemer var svært viktige for å opprettholde tjenester i kritisk infrastruktur. Samtidig ble det vurdert slik at IKT-sårbarheter kunne utnyttes for å ramme samfunnskritisk virksomhet. Det ble derfor foreslått et eget BAS5-prosjekt, som skulle se spesielt på utfordringer knyttet til IKT-sikkerhet.

BAS5 ble opprinnelig foreslått startet opp i 2003, med en prosjektskisse utformet etter samme lest som de tidligere BAS-prosjektene. Med andre ord hadde den første prosjektbeskrivelsen fokus på sårbarhetsanalyser og kosteffektivitetsanalyser av tiltak, men nå for samfunnskritiske IKT-systemer. BAS5 ble også omtalt spesielt i Nasjonal strategi for informasjonssikkerhet. Prosjektet ble imidlertid ikke startet opp, som følge av mangel på finansiering. Et mindre forprosjekt ble gjennomført og dokumentert i en egen rapport [20].

I april 2004 startet arbeidet med å få etablert BAS5 på nytt. Justis- og politidepartementet (JD) ga da Direktoratet for samfunnssikkerhet og beredskap (DSB) og Nasjonal sikkerhetsmyndighet (NSM) i oppgave å sikre oppstart av prosjektet. Etter hvert ble også FFI engasjert i arbeidet, i form av et nytt forprosjekt. Dette hadde som formål å utarbeide en prosjektskisse, undersøke finansieringsmuligheter og invitere til et arbeidsseminar om prosjektet. FFI, DSB og NSM gjennomførte deretter et idéseminar 13. mai 2004. Resultatet ble en omforent prosjektsøknad til IKT-SOS-programmet i Norges forskningsråd og en egen finansieringsplan for arbeidet. Søknaden ble sendt inn til Forskningsrådet 18. juni 2004. Egeninnsats fra DSB og NSM var også inkludert i finansieringsplanen.

Det nye prosjektet fikk en klar metodeprofil, med målsettinger som skissert i kapittel 1. Som en følge av endret innretning fikk BAS5 tilsvarende mindre fokus på å utforme konkrete sårbarhetsreduserende tiltak innenfor IKT-sikkerhet. Et av målene med BAS5-prosjektet var også å få til et tettere samarbeid mellom universiteter og høyskoler. Universitetet i Stavanger (UiS), Norges teknisk-naturvitenskapelige universitet (NTNU) og Høgskolen i Gjøvik (HiG) ble pga. sine faglige profiler og masterutdanninger innenfor risikostyring og samfunnssikkerhet, sikkerhetsledelse og informasjonssikkerhet invitert med i prosjektet av FFI.

C.2 Justerte målsettinger underveis

En kunnskapsstatus i oppstarten til BAS5 ble dokumentert i et eget notat [29]. Etter hvert som samarbeidet mellom de ulike prosjektdeltakerne kom i gang, ble målsettingene for prosjektarbeidet noe justert. De viktigste justeringene i løpet av prosjektet har vært:

- *Målsetting 1 "Utvikle og anvende metodikk for identifisering og rangering av kritiske samfunnsfunksjoner og IKT-systemer"*
  Dette viste seg raskt å bli en langt mer omfattende og krevende oppgave enn opprinnelig planlagt. Derfor ble målet underveis justert til å utvikle en metode, uten at det har vært mulig å anvende denne metodikken i løpet av BAS5 (annet enn i mindre tester). Metodeutviklingen ble blant annet basert på en omfattende kartlegging av andre lands tilnærming til denne problemstillingen.
- *Målsetting 2 "Utvikle og anvende metodikk for risikoanalyse av samfunnskritiske IKT-systemer"*
  Ved prosjektets start så man raskt at det var lite behov for å utvikle en egen ny ROS-metodikk, siden det finnes mange ulike metodikker allerede tilgjengelig. Arbeidet fikk derfor som formål å kartlegge og vurdere eksisterende metoder og verktøy, og utvikle et rammeverk for valg av den mest hensiktsmessige metode gitt en spesifikk problemstilling. Sentralt i arbeidet var gjennomføring av flere ROS-analyser (caser), for å prøve ut ulike metodikker i praksis.
- *Målsetting 3 "Utvikle og anvende metodikk for effektivitetsvurderinger av tiltak som kan redusere sårbarheter i IKT-systemer"*
  I hovedsak har denne aktiviteten vært knyttet til gjennomføringen av en PhD-studie ved Høgskolen i Gjøvik. Opprinnelig var også kostnadsperspektivet ved tiltak inkludert, men dette ble definert ut av oppgaven. Arbeidet fokuserer derfor primært på effektivitetsvurderinger.

C.3 Finansiering

BAS5-prosjektet har vært et økonomisk spleiselag mellom en rekke aktører: Forskningsrådet, Fornyings- og administrasjonsdepartementet (FAD), Justis- og politidepartementet (JD), Olje- og energidepartementet (OED), Samferdselsdepartementet (SD), Norges vassdrags- og energidirektorat (NVE), Oljedirektoratet (OD) Post- og teletilsynet (PT), Kredittilsynet, Sosial- og helsedirektoratet (SHdir), Statnett, DSB, NSM og FFI. Totalt budsjett var ca 12 mill kr.

En finansieringsplan forelå 18. juni 2004, da søknaden ble sendt inn til IKT-SOS programmet. Søknaden ble besvart i oktober. Svaret var positivt, men bevilgningen var redusert med litt over 1 million kroner i forhold til oppsatt budsjett. Forskningsrådet krevde også at deres bidrag i sin helhet skulle gå til de akademiske partnerne i prosjektet, og ikke til FFI. Samtidig skulle ambisjonsnivået opprettholdes. FFI fikk 2 uker på seg til å garantere restfinansiering, hvilket FFI også gjorde.

Imidlertid klarte FFI bare delvis å skaffe fram restbeløpet i form av økonomiske midler, og

resultatet ble at DSB og NSM i større grad enn planlagt skulle kompensere budsjettkuttet med egen arbeidsinnsats. Arbeidet med å skaffe restfinansiering pågikk hele høsten 2004 og frem til våren 2005.

Prosjektet ble etter en vurdering av FFIs jurist/revisor vurdert som ikke momspliktig. Dette utelukket samtidig hver enkelt deltakers rett til å kreve spesifiserte leveranser fra prosjektet i forhold til sin finansieringsandel. Slike krav ville være å betrakte som en hvilken som helst handelstransaksjon eller et tjenestekjøp, og ville dermed være underlagt momsplikt.

C.4 Personell

Prosjektleder fra starten av var Janne Hagen, FFI. Håvard Fridheim, FFI, overtok som prosjektleder da Hagen i andre utlysningsrunde søkte og fikk PhD-stipendiatet ved Høgskolen i Gjøvik under BAS5-prosjektet. Skifte av prosjektleder skjedde i august 2005, da stipendiatstillingen ble besatt.

Prosjektet har hatt mange medarbeidere og bidragsytere – de aller fleste på deltid: Terje Aven, Hermann Wiencke, Jan Erik Vinnem og Amund Junge fra UiS, Einar Snekkesnes fra HiG, Jan Audestad fra HiG/Telenor, Jørn Vatn, Jan Hovden og Marvin Rausand fra NTNU, Kjetil Sørli og Ann Kristin Henriksen etterfulgt av Stein Henriksen fra DSB, Bjørn Nilsen etterfulgt av Kjetil Sørli fra NSM og Tor Aalborg fra Statnett. Fra FFI har følgende medarbeidere jobbet i prosjektet: Tormod Kalberg Sivertsen, Aasmund Thuv, Ronny Windvik og Kjell Olav Nystuen. Flere andre personer fra FFIs miljø innen IKT-forskning har også blitt involvert i arbeidet med mindre innsats underveis.

I tillegg har flere studenter vært tilknyttet prosjektet. Mastergradsoppgaver gjennomført i tilknytning til prosjektet er:

1) Lene Bogen, NTNU, Organisering av IT-sikkerhet i Statlig sektor – styrker og svakheter ved dagens modell, 2005
2) Oddvar Aarseth, NTNU, Sikkerhetsutfordringer ved bruk og avhengighet av internett,
3) Helge Myrland, UiS, Edrift og sikkerhet, 2005
4) Steinar Liung, HiG, Rate vulnerability reducing measures based on a cost effectiveness analysis, 2005
5) Anja Elisabeth Føli, UiS, Utvikling av verktøy for evaluering av risiko- og sårbarhetsanalyser, 2006
6) Eric Patric Ford, UiS, Evaluering av metoder for risiko- og sårbarhetsvurdering, 2006
7) Nils Øyvind Audestad, UiO/UNIK, Analyse av datamaskiner og datanett med fokus på tid og tjenestetilgjengelighet, 2007

I tillegg har FFI engasjert 4 sommerstudenter for arbeid innenfor utvalgte områder i prosjektet:

- Sommeren 2005: Lene Bogen og Kristin Mørkestøl. De lagde FFI-rapporten ”Håndtering av IKT-kriser – aktører og roller” [24]. Bogen og Mørkestøl ble deretter tilknyttet prosjektet frem til februar 2006 i stipendiatstillinger.
- Sommeren 2006: Lisa Marie Nordøen og Elin Espeland Halvorsen. De bidro til FFI-

rapporten ”Tilsynsmetodikk og måling av informasjonssikkerhet i finans- og kraftsektoren” [22].

C.5 Administrasjon

FFI har hatt oppgaven som prosjektleder for BAS5. Prosjektledelsen har vært ufordrende, av mange årsaker:

- BAS5-prosjektet har vært preget av mange og tildels motstridende faglige interesser.
- Prosjektet har hatt mange deltidsansatte.
- I perioder har det vært knapphet på personellressurser og bytte av personell knyttet til sentrale oppgaver.
- Prosjektet har hatt ambisiøse målsettinger.

For å få gjennomført arbeidet har konkrete oppgaver blitt satt bort til samarbeidspartnere. Spesielt gjelder dette:

- UiS, som fikk et ansvar for metodeutvikling og -vurdering innenfor ROS-arbeidet
- DSB som fikk i oppgave å utvikle metodikk for å rangere samfunnsfunksjoner
- NSM som skulle produsere en trusselanalyse som input til ROS-analysene.
- Det kan også nevnes at SINTEF ble engasjert for gjennomføring av en egen ROS-analyse i prosjektet, ved at BAS5-prosjektet kjøpte seg inn i SECURIS-prosjektet (et av de andre IKT-SOS-prosjektene).

BAS5 startet opp med flere oppstartseminarer innenfor temaene ”trusler mot IKT-systemer”, ”rangering av samfunnsfunksjoner” og ”ROS-metodikk”. Etter hvert ble det gjennomført regelmessige arbeidsmøter, der bare aktuelle medarbeidere var til stede.

For å lette samarbeidet og informasjonsdelingen internt i prosjektteamet, ble webhotellet prosjektplassen.no forsøkt brukt til felles arbeidsområde. Denne ble i begrenset grad benyttet i starten, og da bruken ikke økte nevneverdig etter hvert, ble abonnementet på prosjektplassen.no sagt opp etter ca 1,5 års drift.

Prosjektrådet er rådgiver for prosjektledelsen og fungerer som en referansegruppe. I prosjektrådet til BAS5 satt alle oppdragsgiverne, prosjektdeltakerne og noen spesielt inviterte observatører fra bl.a. SINTEF, Næringslivets sikkerhetsråd, Universitetet i Oslo/UNIK og Telenor. I løpet av prosjektet ble det gjennomført totalt 10 prosjektrådsmøter.

C.6 Samarbeid

I starten av prosjektet ble alle medarbeidere invitert med på alle aktiviteter. Dette var oppstartingsaktiviteter som hadde som formål å samle mest mulig kunnskap til dem som skulle ta dette videre. Ettersom tiden gikk, ble det etablert arbeidsgrupper i forhold til prosjektets utlike målsetninger. Utkast til rapporter ble sendt på høring per e-post, og resultater ble fremlagt og diskutert på prosjektrådsmøter.

Samarbeidet mellom partene har gått bra, men det har vært flere utfordringer i arbeidet med å utvikle velfungerende prosjektteam. Noen av de viktigste forholdene har vært:

- Generelt har det vært et stort trykk mot prosjektets medarbeidere når det gjelder andre oppgaver. Samfunnssikkerhetsmiljøet i Norge er ikke stort, og flere analyser og oppdrag har kommet i tillegg til BAS5 og lagt beslag på tiden til prosjektmedarbeiderne. Særlig kan nevnes ”Utvalg for sikring av landets kritiske infrastruktur (Infrastrukturutvalget)”, som i slutten av 2005 og starten av 2006 tok mesteparten av tiden til NSMs og DSBs BAS5-medarbeidere. Konsekvensen var at leveranser til prosjektet har blitt forsinket eller uteblitt.
- Enkelte arbeidsoppgaver har også vært også langt mer arbeidskrevende, sammensatte og kompliserte enn opprinnelig antatt. Det har derfor vært vanskelig å plukke ut små og konkrete problemstillinger for de av deltakerne i prosjektet som har hatt minst innsats.
- Til sist er det også stor geografisk avstand mellom flere av prosjektdeltakerne. I perioder har det derfor vært stort behov for reiser, og særlig har medarbeiderne fra Stavanger blitt trukket til Oslo ofte i forbindelse med ROS-arbeidet.

Appendix D Publikasjoner fra BAS5

Oversikten sorterer de ulike BAS5-publikasjonene iht. til hvilken målsetting eller hvilket tema i prosjektet de er skrevet.

Sluttrapport

- Fridheim, H. Hagen, J. (2007): Beskyttelse av samfunnet 5 (BAS5): Sårbarhet i kritiske IKT-systemer – Sluttrapport, FFI/RAPPORT/2007-01204

Målsetting 1 - Utvikle og anvende metodikk for identifisering og rangering av kritiske samfunnsfunksjoner og IKT-systemer.

- Henriksen, S., Sørli, K, Bogen, L. (2007): Metode for identifisering og rangering av kritiske samfunnsfunksjoner, FFI/RAPPORT-2007/00784
- Sørli, K. et al..(2007): Bakgrunnsstudie til metode for identifisering og rangering av kritiske samfunnsfunksjoner, FFI/RAPPORT-2007/00785.

Målsetting 2 - Utvikle og anvende metodikk for risikoanalyse av samfunnskritiske IKT-systemer.

- Aven, T. (2006): A unified framework for risk and vulnerability analysis and management covering both safety and security security. Reliability Engineering and System Safety, to appear
- Aven, T. (2006): Expressing risk in a security context. ESREL 2006. pp. 2577-2582
  Aven, T., Wiencke H. (2006). Rammeverk for gjennomføring av risiko- og sårbarhetsanalyser av samfunnskritisk infrastruktur. I NoU 2006:6, vedlegg 9. s 262-267
- SEROS (2007): Utvikling av metodikk for risikoanalyse av samfunnskritisk IKT. SEROS-rapport nr 91892
- Sivertsen, T. et al. (2006): BAS5 CASESTUDIE - Risikoanalyse av et helseforetaks IKT-system, FFI/RAPPORT-2006/03133 (Unntatt offentlighet)
- Sivertsen, T. Wiencke, H. (2007): BAS5 CASESTUDIE - Risikoanalyse av et finansforetaks IKT-system, FFI/RAPPORT-2007/00486 (Unntatt offentlighet)
- Sivertsen, T. (2007): Risikoanalyser i BAS5 - Teknologiske erfaringer, FFI/RAPPORT-2007/00910
- Wiencke, HS. Aven, T. Hagen, J. (2006): A framework for selection of methodology for risk and vulnerability assessments of infrastructures depending on ICT. ESREL 2006, pp. 2297-2304

Målsetting 3 - Utvikle og anvende metodikk for effektivitetsvurderinger av tiltak som kan redusere sårbarheter i IKT-systemer.

- Hagen, J. (2005): Measuring the effectiveness of information security measures, Project Plan V.1, November 2005, Nislab, Gjøvik University College.
- Hagen, J. Sivertsen, T. Rong, C. (2007): Information security threats and access control practices in Norwegian businesses, paper under SSNDS 2007.

Bakgrunnsstudier:

1 Relevante arbeider og studier for BAS5

- Audestad, J. (2005): E-bomber og e-granater – Om IKT og sårbarhet, FFI/NOTAT-2005/0938
- Hagen, J. (2004): Beskyttelse av samfunnskritisk informasjonsinfrastruktur – Oppsummering av kjente studier i oppstarten til BAS5, FFI/NOTAT-2004/02712 (Unntatt offentlighet)

2 Norske myndigheter og andre lands innretning på IKT-sikkerhetsarbeidet

- Bogen, L., Mørkestøl, K.(2005): Håndtering av IKT-kriser – aktører og roller, FFI-RAPPORT 2005/03536
- Gulichsen, S. et al. (2003): Strategier for informasjonssikkerhet, En komparativ studie av strategiarbeidet i Norge, USA, EU og Australia, FFI/RAPPORT-2003/00271
- Fridheim, H. (2006): Kritisk infrastrukturbeskyttelse i USA - Erfaringer fra BAS5-prosjektets USA-reise 10-14. oktober 2005, FFI/REISERAPPORT-2006/01414 (Unntatt offentlighet)
- Hagen, J., Nordøen, L.M. Halvorsen, E.E. (2007): Tilsynsmetodikk og måling av informasjonssikkerhet i finans- og kraftsektoren. FFI/RAPPORT-2007/00880.
- Nystuen, K. Fridheim, H. (2007): Sikkerhet og sårbarhet i elektroniske samfunnsinfrastrukturer – Refleksjoner rundt regulering og tiltak. FFI/RAPPORT-2007/00941

3 System- og teknologistudier

- Thuv, A. et al (2007): Sårbarheter i Internett, FFI/RAPPORT-2007/00903
- Van Reenen, A.D. (2005): Nanoteknologi – en innføring. FFI/RAPPORT-2005/02017

4 Annet

- Hagen, J., Fridheim, H. (2005): Hva er kritisk infrastruktur? FFI-NOTAT 2005/00363
- Hagen, J. et al. (2006): Kraftbortfall i Rogland og bortfall av IKT-systemer, Erfaringer fra arbeidsseminar ved FFI 20.april 2005, FFI-NOTAT 2006/00139 (Begrenset)
- Hagen, J., Fridheim, H., Nystuen, K. (2005): New challenges for emergency preparedness in the information society, Telektronikk 1/2005

Masteroppgaver:

- Bogen, L. Organisering av IT-sikkerhet i Statlig sektor – styrker og svakheter ved dagens modell. NTNU, 2005
- Aarseth, O. Sikkerhetsutfordringer ved bruk og avhengighet av internett. NTNU, 2005
- Myrland, H. Edrift og sikkerhet. UiS, 2005
- Liung, S. Rate vulnerability reducing measures based on a cost effectiveness analysis. HIG, 2005
- Føli, A.E. Utvikling av verktøy for evaluering av risiko- og sårbarhetsanalyser. UiS, 2006
- Ford, E.P. Evaluering av metoder for risiko- og sårbarhetsvurdering. UiS, 2006
- Audestad, N.Ø. Analyse av datamaskiner og datanett med fokus på tid og tjenestetilgjengelighet. UiO/UNIK 2007

Appendix E Foredrag fra BAS5-prosjektet

Foredrag om BAS5-prosjektet har blitt gitt i følgende fora:

2004

September

- EAPC/PfP Workshop: Critical Infrastructure Protection and Civil Emergency Planning: Dependable Structures, Cyber Security and Common Standards, Zürich, Sveits

Oktober

- Norges vassdrags- og energidirektorat: Referanseforum for informasjonssikkerhet, Oslo
- Norges Forskningsråds møte om samfunnssikkerhet, Stavanger

November

- Møte med svenske beredskapsaktører: Krisberedskapsmyndigheten, Post- og telestyrelsen og Totalförsvarets forskningsinstitut, Stockholm, Sverige

Desember

- Norsk sikkerhetsforening, årsmøte, Oslo

2005

Januar

- Orientering for Infrastrukturutvalget, Oslo
- Orientering for Telenor, Oslo
- Orientering for Næringslivets sikkerhetsråd, Oslo

Februar

- Workshop ”The future of ICT for power systems”, Brüssel, Belgia

Mars

- Orientering på IKT-SOS-workshop, Gardermoen

Mai

- Nasjonalt utdanningssenter for samfunnssikkerhet og beredskap, Heggedal
- ”Sikkerhet og sårbarhet” – Den norske dataforening, Trondheim
- Møte med IFE Halden, Halden

Juni

- Presentasjon for Direktoratet for samfunnssikkerhet og beredskap, Tønsberg

August

- Presentasjoner på møte med SINTEF/Irma-prosjektet, Kjeller

September

- Presentasjon for representant for EBIOS-prosjektet, Kjeller

Oktober

- Presentasjoner for amerikanske beredskapsaktøter ifm. studietur til USA: IT-ISAC (Atlanta), George Mason University (Washington), Department for Homeland Security (Washington), Sandia National Laboratories (Albuquerque)
- Sikkerhetsdagene 2005, Trondheim

November

- Foredrag for ITAKT, Oslo
- Foredrag for Direktoratet for samfunnsikkerhet og beredskap, Tønsberg

- Nasjonalt utdanningssenter for samfunnssikkerhet og beredskap, Heggedal
- Foredrag for SINTEF, Trondheim

Desember

- Foredrag for VDI Forum, Oslo
- Foredrag for Stortingets utredningsseksjon, Kjeller

2006

Januar

- Nasjonalt utdanningssenter for samfunnssikkerhet og beredskap, Kjeller

Februar

- Arbeidsmøte Ags-IT (Nordisk kraftforsyning), Gardermoen

Mars

- Datateam – Vårkonferansen 2006

Mai

- Norges vassdrags- og energidirektorat – Informasjonssikkerhetskonferanse, Gardermoen

Juni

- Nasjonalt utdanningssenter for samfunnssikkerhet og beredskap, Heggedal
- Møte med Accenture, Oslo

September

- Samarbeidsseminar FFI/SIMULA, Kjeller
- ESREL 2006 Conference (Safety and Reliability for Managing Risk), Estoril, Portugal

Oktober

- Studiemøtet elektronikk og data, Oslo
- NTNU/Programvaresikkerhet, Trondheim
- Workshop KIS – Nasjonal strategi for IKT-sikkerhet, Oslo

November

- Norges vassdrags- og energidirektorat – Informasjonssikkerhetskonferanse, Oslo

Desember

- Nasjonalt utdanningssenter for samfunnssikkerhet og beredskap, Heggedal
- Sikkerhetsforum, Post- og teletilsynet, Oslo

2007

Januar

- Kurs for beredskapsledere i kraftforsyningen, Nasjonalt utdanningssenter for samfunnssikkerhet og beredskap, Heggedal

I tillegg er det avholdt en rekke presentasjoner ifm. gjennomføring av prosjektrådsmøtene, arbeidsmøter ifm. gjennomførte risikoanalyser osv.

Referanseliste

[1] O. M. Hæsken, T. G. Olsen, and H. Fridheim, "Beskyttelse av samfunnet (BAS) - Sluttrapport," FFI/RAPPORT 97/01459, 1997.

[2] J. Hagen and K. O. Nystuen, "Beskyttelse av samfunnet med vekt på offentlig telekommunikasjon," FFI/RAPPORT 99/00240, 1999.

[3] H. Fridheim, J. Hagen, and S. Henriksen, "En sårbar kraftforsyning - sluttrapport etter BAS3," FFI/RAPPORT 2001/02381, 2001.

[4] J. Hagen, G. H. Rodal, E. Hoff, B. Lia, J. E. Torp, and S. Gulichsen, "Beskyttelse av samfunnet med fokus på transportsektoren," FFI/RAPPORT 2003/00929, 2003.

[5] eNorge, "Nasjonal strategi for informasjonssikkerhet - Utfordringer, prioriteringer og tiltak.," Forsvarsdepartementet, Nærings- og handelsdepartementet, Justis- og politidepartementet,2003.

[6] Justis- og politidepartementet, "Når sikkerhet er viktigst,"NOU 2006:6, 2006.

[7] K. O. Nystuen and H. Fridheim, "Sikkerhet og sårbarhet i elektroniske samfunnsinfrastrukturer – Refleksjoner rundt regulering og tiltak," FFI/RAPPORT 2007/00941, 2007.

[8] Samferdselsdepartementet, "Stortingsmelding 47 (2000-2001): Telesikkerhet og -beredskap i et marked med fri konkurranse,"2001.

[9] Riksrevisjonen, "Riksrevisjonens undersøkelse av myndighetenes arbeid med å sikre IT-infrastruktur,"Dokument nr 3:4 (2005-2006), 2005.

[10] K. Sørli, S. Henriksen, L. Bogen, and K. Mørkestøl, "Bakgrunnsstudie til metode for identifisering og rangering av kritiske samfunnsfunksjoner," FFI/RAPPORT 2007/00785, 2007.

[11] S. Henriksen, K. Sørli, and L. Bogen, "Metode for identifisering og rangering av kritiske samfunnsfunksjoner," FFI/RAPPORT 2007/00784, 2007.

[12] SEROS, "Utvikling av metodikk for risikoanalyse av samfunnskritisk IKT," SEROS-rapport 91892, 2007.

[13] T. K. Sivertsen, "Risikoanalyser i BAS5 - Teknologiske erfaringer," FFI/RAPPORT 2007/00910, 2007.

[14] T. Aven, "A unified framework for risk and vulnerability analysis covering both safety and security," *Reliability Engineering and System Safety*, vol. 92, pp. 745-754, 2007.

[15] T. K. Sivertsen, A. Thuv, H. Wiencke, and H. Fridheim, "BAS5 Casestudie - Risikoanalyse av et helseforetaks IKT-system," FFI/RAPPORT 2006/03133 (Unntatt offentlighet), 2006.

[16] T. K. Sivertsen and H. Wiencke, "BAS5 CASESTUDIE - Risikoanalyse av et finansforetaks IKT-system," FFI/RAPPORT 2007/00486 (Unntatt offentlighet), 2007.

[17] A. Thuv, R. Windvik, K. O. Nystuen, and T. K. Sivertsen, "Sårbarheter i Internett," FFI/RAPPORT 2007/00903, 2007.

[18] A. D. Van Reenen, "Nanoteknologi - en innføring," FFI/RAPPORT 2005/02017, 2005.

[19] J. Audestad, "E-bomber og e-granater - Om IKT og sårbarhet," FFI/NOTAT 2005/00938, 2005.

[20] S. Gulichsen, E. Hoff, K. Sørli, J. Hagen, and K. O. Nystuen, "Strategier for informasjonssikkerhet, En komparativ studie av strategiarbeidet i Norge, USA, EU og Australia," FFI/RAPPORT 2003/00271, 2003.

[21] H. Fridheim, "Kritisk infrastrukturbeskyttelse i USA - Erfaringer fra BAS5-prosjektets USA-reise 10-14. oktober 2005," FFI/REISERAPPORT 2006/01414 (Unntatt offentlighet), 2006.

[22] J. Hagen, L. M. Nordøen, and E. E. Halvorsen, "Tilsynsmetodikk og måling av informasjonssikkerhet i finans- og kraftsektoren," FFI/RAPPORT 2007/00880, 2007.

[23] Kredittilsynet, "Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT)," 2003.

[24] L. Bogen and K. Mørkestøl, "Håndtering av IKT-kriser - Aktører og roller," FFI/RAPPORT 2005/03536, 2005.

[25] J. Hagen, H. Fridheim, A. K. Henriksen, and K. Sørli, "Kraftbortfall i Rogaland og bortfall av IKT-systemer - Erfaringer fra arbeidsseminar ved FFI 20.april 2005," FFI-NOTAT 2006/00139 (Begrenset), 2006.

[26] Næringslivets sikkerhetsråd, "Mørketallsundersøkelsen 2006,"2006.

[27] Justis- og politidepartementet, "Datakriminalitet," Justis- og politidepartementet,NOU nr 31 1985, 1985.

[28] J. Hagen, T. K. Sivertsen, and C. Rong, "Information security threats and access control practices in Norwegian businesses," SSND 2007.

[29] J. Hagen, "Beskyttelse av samfunnskritisk informasjonsinfrastruktur – Oppsummering av kjente studier i oppstarten til BAS5," FFI/NOTAT 2004/02712 (Unntatt offentlighet), 2004.