FFI RAPPORT

RISIKOANALYSE AV SAMFUNNSKRITISKE IKT-SYSTEMER - Teknologiske erfaringer

SIVERTSEN Tormod Kalberg

FFI/RAPPORT-2007/00910

RISIKOANALYSE AV SAMFUNNSKRITISKE IKT-SYSTEMER -
Teknologiske erfaringer

SIVERTSEN Tormod Kalberg

FFI/RAPPORT-2007/00910

FORSVARETS FORSKNINGSINSTITUTT
Norwegian Defence Research Establishment
Postboks 25, 2027 Kjeller, Norge

FORSVARETS FORSKNINGSINSTITUTT (FFI)
Norwegian Defence Research Establishment

P O BOX 25
NO-2027 KJELLER, NORWAY

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (when data entered)

REPORT DOCUMENTATION PAGE

1) PUBL/REPORT NUMBER	2) SECURITY CLASSIFICATION	3) NUMBER OF PAGES
FFI/RAPPORT-2007/00910	UNCLASSIFIED	46
1a) PROJECT REFERENCE	**2a) DECLASSIFICATION/DOWNGRADING SCHEDULE**	
FFI-I/1014	-	

4) TITLE

RISIKOANALYSE AV SAMFUNNSKRITISKE IKT-SYSTEMER -
Teknologiske erfaringer

RISK ANALYSIS OF CRITICAL INFORMATION SYSTEMS -
Technological Experiences

5) NAMES OF AUTHOR(S) IN FULL (surname first)

SIVERTSEN Tormod Kalberg

6) DISTRIBUTION STATEMENT

Approved for public release. Distribution unlimited. (Offentlig tilgjengelig)

7) INDEXING TERMS

IN ENGLISH:	IN NORWEGIAN:
a) Information security	a) Informasjonssikkerhet
b) Risk analysis	b) Risikoanalyse
c) Critical infrastructure	c) Kritisk infrastruktur
d)	d)
e)	e)

THESAURUS REFERENCE:

8) ABSTRACT

"Protection of the society 5" (BAS5) is a research project focusing on methodologies for critical information infrastructure protection. The project has included four case studies on risk analysis of IT systems in four different critical societal sectors.

The case studies have provided the project with experiences both from a methodological and a technological point of view. This report describes the latter by going through the steps normally included in a risk analysis, and for each step examining the challenges involved.

Two short appendices are included, one on logical intentional threats against IT-systems and one giving an overview of the architectures and technologies currently in use.

9) DATE	AUTHORIZED BY This page only	POSITION
2007-03-28	Jan Erik Torp	Director

ISBN 978-82-464-1186-6

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (when data entered)

INNHOLD

		Side
1	BAKGRUNN	7
1.1	Erfaringsgrunnlag	8
2	BEGREPER	9
2.1	Kritisk infrastruktur	9
2.2	Risiko	9
2.3	Informasjonssikkerhet	10
2.3.1	Hva menes med informasjonssikkerhet	10
2.3.2	Kobling mellom identiteter og informasjon.	10
3	RISIKOANALYSE AV IKT-SYSTEMER	11
3.1	Hvorfor gjennomføre risikoanalyser?	11
3.2	Metoder for risikoanalyser av IKT-system	11
3.3	Andre metodikker for analyse av informasjonssikkerhet	13
3.4	Uhell eller angrep, safety eller security?	15
4	UTFORDRINGER VED RISIKOANALYSE AV IKT-SYSTEM	16
4.1	Deltakere og praktisk arbeid	17
4.2	Systemforståelse og modellering	18
4.2.1	Dokumentasjon	19
4.2.2	Modellering	19
4.3	Fareidentifikasjon	21
4.3.1	Ikke-tilsiktede hendelser	22
4.3.2	Tilsiktede hendelser	23
4.3.3	Identifikasjon av hendelser	24
4.4	Risikovurdering	28
4.4.1	Årsak	28
4.4.2	Konsekvens	29
4.5	Risikohåndtering	30
5	OPPSUMMERING	31
APPENDIKS		33
A	LOGISKE TRUSLER MOT IKT-SYSTEMER	33
A.1	Angrep mot IKT-systemer	33
A.2	Hvem angriper? - Aktørtyper	33
A.3	Trender og sårbarheter.	37
A.4	Virkemiddel	38

A.5 Litteratur, undersøkelser og videre informasjon. 40

B HVORDAN SER SAMFUNNSKRITISKE IKT-SYSTEMER UT? 42

B.1 Oppbygging 42

B.2 Integrasjon av tjenester og nettverk 43

B.3 Hyllevare 44

B.4 WAN 45

B.5 Annen teknologi 45

B.6 Avhengighet av Internett og sektornettverk 46

**RISIKOANALYSE AV SAMFUNNSKRITISKE IKT-SYSTEMER -
Teknologiske erfaringer**

1 BAKGRUNN

”Beskyttelse av samfunnet 5” (BAS5) er et forskningsprosjekt med fokus på metodikk for analyse av kritisk informasjonsinfrastruktur. Prosjektet er et samarbeid mellom en rekke forskningsinstitusjoner, universiteter/høgskoler, departementer og direktorater, og er også støttet av Norges forskningsråd gjennom IKT-SOS-programmet[1].

Prosjektet hadde i utgangspunktet tre hovedmålsettinger:

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

I forbindelse med arbeidet under hovedmålsetting 1 er det gjennomført casestudier med risikoanalyse av IKT-systemer i fire ulike samfunnskritiske sektorer:

- Kraftsektoren
- Helsesektoren
- Olje- og gassektoren
- Finanssektoren

Denne rapporten beskriver FFIs erfaringer gjort i møtet mellom IKT-systemer og ulike tilnærminger til risikoanalyse. Rapporten er generell og oppsummerende, og den baserer seg tungt på empiriske erfaringer fra de gjennomførte analysene. Prosjektet har også hentet erfaringer om sikkerhet i kritisk informasjonsinfrastruktur gjennom møter og besøk hos andre aktører.

Rapporten har et hovedfokus mot to områder:

- Hvordan samfunnskritiske IKT-systemer ser ut og er bygget opp
- Hvilke mulige trusler som IKT-systemer kan utsettes for

I tillegg må rapporten ses i sammenheng med Universitetet i Stavangers oppsummerende rapport[2] etter risikoanalyseaktiviteten i BAS5. Deler av vår rapport er derfor å betrakte som supplerende innspill til Stavangers rapport.

[1] IKT – Sikkerhet og sårbarhet
[2] SEROS (2007): ”Utvikling av metodikk for risikoanalyse av samfunnskritisk IKT”. Universitetet i Stavanger. SEROS rapport nr. 91892.

1.1 Erfaringsgrunnlag

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 ble gjennomført av BAS5-prosjektet.
  - Analysen vurderte IKT-systemene som var i bruk ved en av sykehusets avdelinger, spesielt med tanke på system for elektroniske pasientjournaler.
- IKT-systemet i et stort finansforetak
  - Analyse ble gjennomført av BAS5-prosjektet.
  - Analysen omhandlet sikkerheten ved store finansielle transaksjoner overfor både ikke-villede og villede hendelser.
- IKT-systemet hos en stor aktør innen kraftforsyningen
  - Analysen ble gjennomført av SINTEF IKT, på oppdrag fra BAS5.
  - Analysen fokuserte på sikkerhet i IKT-systemene som understøttet kraftoverføring.
- IKT-systemet hos en stor aktør innen petroleumsbransjen
  - Analysen ble gjennomført av foretaket selv, med noe støtte fra BAS5-prosjektet.
  - Formålet med analysen var å vurdere sikkerhet i IKT-systemene som benyttes for kommunikasjon ut mot offshoreinstallasjoner.

Arbeidet med de to analysene som ikke ble utført av BAS5-prosjektet selv er fulgt med observatører gjennom hele prosessen.

Alle systemene var i daglig bruk. Med andre ord ble risikoanalysene gjennomført for å vurdere sikkerheten i eksisterende løsninger.

Et generelt trekk for flere av IKT-systemene som ble analysert er at de opprinnelig har vært tenkt som støttesystemer for å understøtte den normale virksomheten. Med andre ord har disse gitt bedriftens medarbeidere ekstra funksjonalitet (for eksempel støtte til beregninger, tilgang på bilder og rapporter osv.) som ikke har vært kritiske for å gjennomføre virksomhetens normale oppgaver. I løpet av forholdsvis kort tid har imidlertid 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, beregning, nettverk) og bedre tilgjengelighet for brukerne. I helsesektoren ser en 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.

Rapporten videre er bygget opp som følger:

- Kapittel 2 diskuterer begreper knyttet til risiko, kritisk infrastruktur og IKT-sikkerhet.
- Kapittel 3 gir en kort presentasjon av risikoanalyse og spesielt risikoanalyse av IKT-

systemer.

- Kapittel 4 diskuterer spesielle utfordringer ved risikoanalyser av IKT-systemer.
- Kapittel 5 gir en oppsummering av rapporten.
- Vedlegg A diskuterer hva trusselen kan være mot IKT-systemer, både knyttet til tilsiktede og ikke-tilsiktede hendelser.
- Vedlegg B trekker ut noen overordnede erfaringer om hvordan IKT-systemene har vært bygd opp, spesielt med tanke på sikkerhetsrelaterte aspekt.

2 BEGREPER

Kapittelet presenterer noen av de viktigste begrepene som er brukt i rapporten. Det understrekes at begrepene i andre sammenhenger eller miljøer kan ha andre tolkninger enn det som presenteres her.

2.1 Kritisk infrastruktur

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:[3]

- "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 dette er kritiske samfunnsfunksjoner alle funksjoner som samfunnet er avhengig av for å dekke befolkningens grunnleggende behov.

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

2.2 Risiko

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* og *konsekvens* for en gitt hendelse. En annen tilnærming er at *risiko er en kombinasjon av mulig konsekvens og tilhørende usikkerhet*. Denne tilnærmingen legger til rette for å vurdere risiko som ikke har noen historikk.

Sårbarhet er et uttrykk for et systems evne til å fungere og oppnå sine mål når det utsettes for påkjenninger. Sårbarhetsutvalget definerer på sin side sårbarhet på følgende måte: [4]

- Sårbarhet er et uttrykk for de problemer et system vil få med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet.

[3] Justis- og politidepartementet (2006): NOU 2006:6. *Når sikkerhet er viktigst*
[4] Justis- og politidepartementet (2000): NOU 2000:24. *Et sårbart samfunn.*

2.3 Informasjonssikkerhet

2.3.1 Hva menes med informasjonssikkerhet

Tradisjonelt bruker en de tre begrepene tilgjengelighet, integritet og konfidensialitet for å definere informasjonssikkerhet. 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*).

Disse tre begrepene dekker det som de fleste intuitivt vil mene med å sikre selve informasjonen. Imidlertid er det i et IKT-system mer enn bare informasjon som må vernes. Ressurser som for eksempel nettverkskapasitet, regnekapasitet og lagringskapasitet må også beskyttes. Denne type sikkerhetsbrudd sorteres ofte inn under brudd på ”tilgjengelighet”, men det kan godt tenkes at tilgjengelighet for eksisterende informasjon er opprettholdt ved denne typen sikkerhetsbrudd.[5]

Selv om informasjonssystemene sjelden har en verdi i seg selv, er det altså nyttig å legge til beskyttelse av systemene selv som en del av sikkerhetsbegrepet. Til dette kommer også flere og flere foretak der hele produksjonen kun består av informasjonsbehandling (de fleste finansforetak er typiske eksempler på dette). I slike tilfeller blir systemenes evne til å fungere riktig til enhver tid et meget sentralt sikkerhetsaspekt, det er ikke nok å bare sikre selve informasjonen. Dersom systemene ikke virker, mistes tilliten til at systemene kan behandle informasjonen på sikker måte.

2.3.2 Kobling mellom identiteter og informasjon.

Definisjonene knyttet til tilgjengelighet, integritet og konfidensialitet benytter begrepet autorisert bruker. Dette peker på en annen side av informasjonssikkerhet, som til en viss grad unnviker den tradisjonelle definisjonen. Den entiteten[6] som skal ha tilgang til informasjon eller ressurser i et system må *autoriseres* av systemet. Dette innebærer at entiteten må *identifiseres* (navngis) og *autentiseres* før en avgjørelse om tilgang kan tas. Enklest sett løses dette med en liste med autoriserte navn og en mekanisme for autentisering (for eksempel brukernavn og passord brukt for å logge seg inn på en maskin).

Den samme bindingen kan også benyttes for å oppnå *sporbarhet* og eventuelt *”ikke-benektelse”* i systemet. Med dette menes at handlinger utført i systemet kan spores tilbake til en gitt bruker, eventuelt på en slik måte at brukeren i ettertid vanskelig kan nekte for å ha utført handlingen. Også det motsatte, anonymitet, dukker ofte opp som et sikkerhetskrav. Et typisk eksempel finner en i medisinsk forskning – der vil en gjerne ha data ut av medisinske register uten at informasjonen i ettertid kan kobles til personer.

---

[5] Et eksempel på dette kan være en kompromittert datamaskin i et såkalt botnett. Dersom maskinen oppfører seg normalt vil det gå lenger tid før maskineieren oppdager at noe er galt, og noden får dermed lengre levetid i botnettet.

[6] Dette trenger ikke være et menneske, men kan for eksempel være en rolle, et kjørende program eller en komponent i systemet.

3 RISIKOANALYSE AV IKT-SYSTEMER

Kapittelet gir en kort presentasjon av risikoanalyser, spesielt risikoanalyser av IKT-systemer. Det gis ikke noen fullstendig drøfting av hva risikoanalyser er og hvilke metodikker som finnes. For dette henvises til Universitetet i Stavangers avsluttende rapport etter risikoanalyseaktiviteten i BAS5.[7]

3.1 Hvorfor gjennomføre risikoanalyser?

En risikoanalyse er en prosess for å kartlegge og dokumentere risiko forbundet med et gitt system. Målet med analysen er som regel å gjøre systemet mer robust mot ulike trusler, både villede handlinger og ulykker. Ved å kombinere kunnskap fra eksperter, ledelse og brukere i en strukturert prosess, identifiseres og rangeres uønskede hendelser ut i fra risiko, og det gis en beskrivelse av risikobildet knyttet til systemet som analyseres. Dette gir et grunnlag for å komme frem til risikoreduserende tiltak knyttet opp mot de identifiserte hendelsene. Tiltakene vil ofte være fokusert mot ulike forhold ved systemet, for eksempel teknologi, organisasjon, arbeidsprosesser og prosedyrer og krav. Basert på definerte prioriteringskriterier kan ulike tiltak prioriteres, for eksempel i kosteffektivitetsanalyser eller kostnytteanalyser. På denne måten vil en risikoanalyse bidra til at man kan starte med de viktigste systemene og de mest effektive tiltakene.

Risikoanalyser kan utføres både på eksisterende og på mulige fremtidige systemer, og de er ofte viktige i en overgang fra gammelt til nytt system eller i forbindelse med endringer i systemet.

Sikkerhetsarbeidet innenfor en virksomhet vil ofte møte motstand fra flere miljøer. Eksempler på dette kan være:

- Ledere, siden ekstra sikkerhet kan gi dyrere løsninger uten synlig resultat i hverdagen.
- Ansatte, siden sikkerhetstenkningen kan ødelegge for funksjonelle løsninger.
- Drifts- og sikkerhetsansvarlige, siden ekstra sikkerhetskrav fører til merarbeid og legger beslag på allerede knappe ressurser.

Ressursene til sikkerhetsarbeid vil normalt være begrenset, og det må argumenteres godt for at tiltak som innføres bidrar til økt sikkerhet. Da er det behov for metodikker som peker på de viktigste sikkerhetsutfordringene for virksomheten, og som gjør det mulig å prioritere mellom tiltak. En risikoanalyse kan bidra til dette.

3.2 Metoder for risikoanalyser av IKT-system

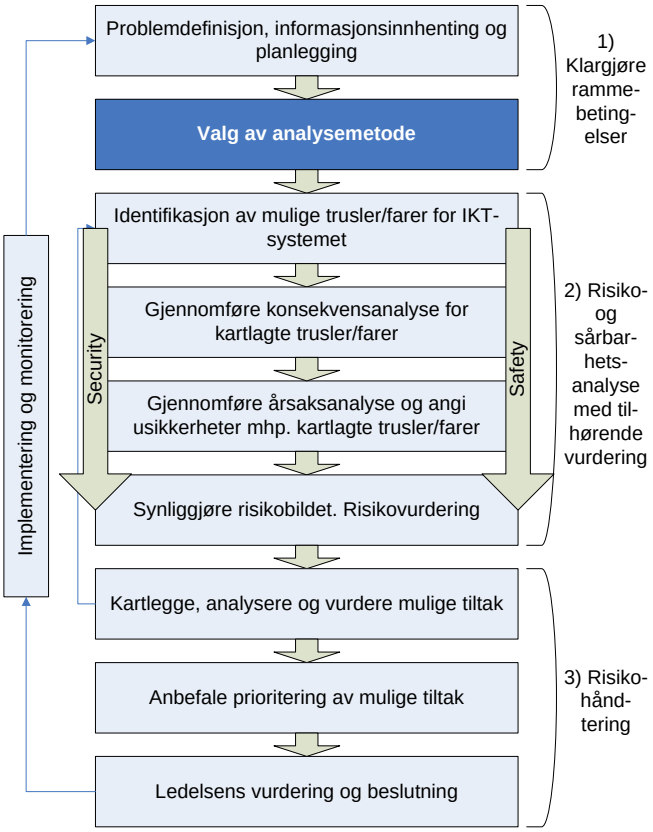
Risikoanalyser har sitt utspring fra industrier som kjernekraft, olje- og gassindustrien og

[7] SEROS (2007): ”Utvikling av metodikk for risikoanalyse av samfunnskritisk IKT”. Universitetet i Stavanger. SEROS rapport nr. 91892.

prosessindustrien. Tradisjonelt har analysene hatt som formål å analysere effektene av ulike feil som oppstår i teknologiske systemer, med vurderinger av konsekvensene av feilsituasjoner og tilhørende sannsynligheter.

Etter hvert har risikoanalyser bredt om seg til andre sektorer enn de som er nevnt over. De siste årene har dette også blitt et aktuelt virkemiddel innen informasjonssikkerhet. Mange virksomheter knyttet til kritisk infrastruktur og samfunnskritiske funksjoner har nå tatt i bruk risikoanalyser på sine IKT-systemer, enten som følge av myndighetskrav eller fordi metodikken anses som hensiktsmessig for sikkerhetsarbeidet.

De fleste risikoanalysemetodikker følger en fast prosess med ulike steg i arbeidet. Et typisk eksempel, som er anvendt i BAS5-prosjektet, er vist i figur 3.1.



Figur 3.1 En standard risikostyringsprosess.

Selv om prosessen bak ulike risikoanalyser har store likhetstrekk med hverandre, finnes det et bredt spekter av ulike metodikker. En av målsettingene med BAS5-prosjektet er å identifisere ulike metodikker for risikoanalyse av IKT-systemer og utvikle et rammeverk for valg av metodikk for ulike problemstillinger. Dette arbeidet er dokumentert i BAS5-prosjektets oppsummerende rapport om temaet[8], og vil ikke bli presentert i ytterligere detalj i denne rapporten.

[8] SEROS (2007): ”Utvikling av metodikk for risikoanalyse av samfunnskritisk IKT”. Universitetet i Stavanger. SEROS rapport nr. 91892.

Det kan imidlertid være verdt å peke på hvilke typer metodikker BAS5 har sett vært anvendt innen virksomheter med samfunnskritisk infrastruktur. Grovt sett kan disse metodikkene klassifiseres som følger:

- Egenutviklede virksomhetsinterne risikoanalysemetodikker. Her har bedriften selv laget metodikken som anvendes, typisk med maler, støttedokumentasjon og en fast måte å dokumentere resultater på. Eksempler er Telenors TeleRisk og British Telecoms Risk Analysis Method.
- Åpent tilgjengelige risikoanalysemetodikker. Det finnes en rekke eksempler på ”standard” risikoanalyser, hvor dokumentasjon er åpent tilgjengelig. To norske eksempel er Nasjonal sikkerhetsmyndighets ROS 2004 og DSBs risikoanalyseveileder for kommunene.
- Åpent tilgjengelige metodikker, spesielt utviklet for IKT. Her er risikoanalysen utviklet med hensyn til at den skal anvendes innenfor informasjonssikkerhet, og de er ofte koblet til standarder innenfor informasjonssikkerhet. Eksempler er bl.a. KITHs risikoanalysemetodikk for informasjonssystem[9], den franske stats EBIOS[10], RANDS VAMM[11] og CORAS-metodikken[12] utviklet av bl.a. SINTEF.
- Kommersielle metodikker, enten ved kjøp av software (f.eks. Buddy Systems Countermeasures) eller tilgang ved betalt medlemskap i en organisasjon (f.eks. Information Security Forum (ISF)). Også disse vil som regel etterleve internasjonale standarder innen informasjonssikkerhet.

Flere av de metodikkene leveres også med egne programvareverktøy for å støtte opp om arbeidet gjennom prosessen.

3.3 Andre metodikker for analyse av informasjonssikkerhet

Selv om BAS5-prosjektet har fokusert spesielt på risikoanalyser, finnes det også en rekke andre metodikker for å ivareta informasjonssikkerhet. Noen av disse presenteres i det følgende. Det er verdt å merke seg at selv for metodikker som ikke eksplittsitt benytter seg av risikobegrepet, så vil en ved praktisk bruk uansett måtte gjøre implisitte vurderinger av risiko. En vil for eksempel måtte avgjøre hvilke system som skal testes eller sertifiseres, eller hvilke punkt en kan utelate fra en sjekkliste for et gitt system. Dette innebærer vurdering av risiko.

Sjekklister er et godt hjelpemiddel for å sikre at relevante aspekter ved informasjonssikkerhet er ivaretatt. De kan benyttes for kvalitets- og sikkerhetskontroll, bl.a. for å undersøke om et IKT-system etterlever internasjonale standarder. Tema kan være alt fra teknisk detaljerte punktlister om konfigurasjon og oppsett av konkrete system til revisjonsverktøy for generell IT-styring

[9] Kompetansesenter for IT i helse- og sosialsektoren AS. Metodikken er tilgjengelig fra http://www.kith.no/
[10] http://www.ssi.gouv.fr/en/confidence/ebiospresentation.html
[11] Dokumentasjon og verktøy tilgjengelig fra http://www.rand.org/pubs/monograph_reports/MR1601/
[12] CORAS var et EU-finansisert forskningsprosjekt med SINTEF og Telenor i koordinerende roller. Programvare og metodikk blir nå vedlikeholdt og videreutviklet av SINTEF. Programvare og dokumentasjon tilgjengelig fra http://coras.sourceforge.net/

(som for eksempel COBIT[13]). Listene kan også spesifisere prosedyrer for krisehåndtering.

Sjekklister spesifiserer tiltak, men gir ikke nødvendigvis noen prioritering av hva som er viktigst å gjøre innenfor et spesifikt IKT-system. Alternativet vil da være å gjøre alt som står på listen, noe som fort kan vise seg å være for kostbart, eller å begynne å prioritere, med andre ord å gjøre vurderinger av risiko. I praksis vil det da vise seg at sjekklister er et godt utgangspunkt når man skal gjøre en risikoanalyse, men at de ikke kan erstatte risikoanalysen.

Internasjonal standarder og "best practices" gis ofte i form av forholdsvis omfattende sjekklister. Mest utbredt er trolig ISO 17799, som er et styringsrammeverk for IKT-sikkerhet. Det er mulig å sertifisere en organisasjon etter standarden, men dette gjøres i praksis i liten grad. Andre mye brukte "beste praksiser" er ISFs "Standard of Good Practice for Information Security"[14] og ISACAs COBIT-rammeverk.

"Common criteria" (ISO 15408) er en annen ISO-standard som gir et rammeverk for å sikre at selve prosessen med å spesifisere, implementere og evaluere sikkerhetskrav er gjort tilfredsstillende.

En siste "beste praksis" som bør nevnes er Information Technology Infrastructure Library (ITIL)[15]. Dette er et rammeverk som beskriver prosedyrer for å sikre kvalitet i generell IKT-drift. ITIL er ikke spesielt fokusert på informasjonssikkerhet, men er et meget godt utgangspunkt for en helhetlig sikkerhetstenking som inkluderer vern mot både tilsiktede og ikke-tilsiktede hendelser.

Med penetrasjonstesting menes aktiv kartlegging og forsøk på å utnytte sårbarheter i et gitt system. Målet er å kartlegge et systems sårbarheter overfor tilsiktede angrep. Som regel rettes testingen mot de rent tekniske delene av et system, men slik testing kan også brukes for å teste organisasjonen rundt systemet. Penetrasjonstesting kan gjennomføres både på system i drift eller på dedikerte testsystem i kontrollerte omgivelser. Målet er å simulere reelle angrep gjennom å bruke verktøy og metoder som en angriper vil benytte. Penetrasjonstesteren kan starte med tilgang fra et offentlig tilgjengelig netteverk eller fra en gitt plassering på innsiden av systemet.

Et prinsipielt problem med penetrasjonstesting er at det bare kan gi negative svar. Man beviser at en sårbarhet finnes, denne kan rettes opp, men etterpå vet en ingenting om hvor mange tilsvarende (eller ikke-tilsvarende) sårbarheter en har, eller hvordan en skal unngå slike sårbarheter i framtiden[16]. Penetrasjonstesting kan likevel være nyttig for å gi en effektiv illustrasjon på hvilke sikkerhetsproblem som kan oppstå.

Penetrasjonstestere benyttes stort sett mot hyllevaresystem, og en bruker vanligvis verktøy som

[13] Control Objectives for Information and related Technology. http://www.isaca.org/cobit.htm
[14] International security forum (ISF) er en internasjonal medlemsorganisasjon. Standarden de utgir er fritt tilgjengelig. http://www.securityforum.org/
[15] http://www.itil.co.uk/
[16] Denne logikken omtales ofte som "penetrate and patch".

er kommersielle eller fritt tilgjengelige for å utføre testingen.

Tekniske sårbarhetsanalyser. Med tekniske sårbarhetsanalyser menes her en grundigere analyse av enkeltkomponenter, programvare og protokoller, uten spesielt hensyn til trusler. Dette kan bli meget kostbart og vil i de fleste tilfellene kreve mye kompetanse. En slik analyse kan for eksempel involvere reversering av programvare dersom analysen skal gjøres grundig, og også her har en samme negative logikk som en har ved penetrasjonstesting.

Denne type analyser brukes som regel med tanke på villede handlinger der en typisk prøver å avdekke feil som kan utnyttes ved å gi ugyldige data til applikasjoner og protokoller. Det er også mulig å bruke denne type analyser for å undersøke stabilitet og pålitelighet for et gitt system.

3.4 Uhell eller angrep, safety eller security?

Det skilles ofte mellom de tilsiktede og de ikke-tilsiktede uønskede hendelsene som et IKT-system kan utsettes for. For ulike uønskede hendelser kan risiko vurderes, som diskutert i kapittel 2.2.

I Norge er det en tradisjon for å skille mellom begrepene safety og security, der safety brukes om vern mot ikke-villede hendelser og security om vern mot villede hendelser. Ingen etablerte norske begrep skiller mellom disse to. Dette viser seg i praksis også vanskelig å etablere, siden noen miljø utelukkende bruker sikkerhet om security, mens andre miljø utelukkende bruker sikkerhet om safety.[17] I forlengelsen av dette vil flere benytte begrepet trussel om hendelser som forutsetter en bevisst angriper med intensjon og kapasitet til å gjennomføre en uønsket handling. Uansett er terminologien på området fremdeles uklar.

Selv om den tradisjonelle definisjonen av informasjonssikkerhet (tilgjengelighet, integritet, konfidensialitet) strengt tatt dekker opp både tilsiktede og ikke-tilsiktede hendelser, har en også innen IKT-miljøene en tilsvarende deling. Enkelte miljøer, for eksempel innen system engineering, bruker ofte sikkerhet som tilgjengelighet, pålitelighet, stabilitet og tjenestekvalitet (på engelsk brukes her begrep som dependability og reliability – safety benyttes ikke). Et annet miljø, som ofte har utspring fra kryptografi og lignende, benytter sikkerhet om tema som integritet, konfidensialitet, autentisering og autorisasjon.

Det samme skillet kan en som regel finne igjen i begrepsbruken i ulike sikkerhetsmetodikker for IKT-systemer. Imidlertid omhandler veldig mye litteratur om datasikkerhet kun sikkerhet mot tilsiktede handlinger.

I denne rapporten vil begrepet sikkerhet inkludere begge disse perspektivene, og vi vil

[17] Det er gjort et forsøk på avklaring i et vedlegg til Infrastrukturutvalgets rapport, ”Når sikkerhet er viktigst” (NOU 2006:6). Sikkerhet omfatter der både security (kalt sikring) og safety (kalt trygghet).

argumentere for at et risikobasert IKT-sikkerhetsarbeid også må inkludere begge. En typisk fallgruve er å gjøre en ren ”security”-analyse, der en legger til noen få ikke-tilsiktede hendelser. Resultatet vil da feilaktig framstå som et helhetlig risikobilde.

4 UTFORDRINGER VED RISIKOANALYSE AV IKT-SYSTEM

Dette kapittelet går gjennom de stegene som vanligvis inngår i en risikoanalyse av et IKT-system, og diskuterer problemstillinger som man erfaringsmessig støter på. Utfordringene vil selvfølgelig variere, alt etter hvilken type analyse som skal gjennomføres og hvilken type system som skal analyseres – målet for en analyse kan være alt fra en enkeltapplikasjon eller en enkeltkomponent til et systems overordnede forretningslogikk med tilhørende organisasjon. I en bank kan for eksempel noen av de aktuelle temaene og systemene være:

- Finansielt kjernesystem og system for samhandling med andre finansinstitusjoner.
- Kundekommunikasjon (kundeservice, bestilling av banktjenester, web, epost osv.)
- Nettbank og andre automatiserte kundetjenester (sammen med outsourcingsavtaler, klientsystem for nettbank, sikkerhet hos sluttbrukere osv.)
- Behandling og bruk av sensitiv informasjon.
- Administrative verktøy for ansatte.

Mange problemstillinger vil likevel være de samme. Et typisk IKT-system vil være et distribuert system der flere brukere og ulike teknologier og arkitekturer inngår. I tillegg kommer eksterne avhengigheter, for eksempel til underleverandører, outsourcingspartnere, konsulenter, forretningspartnere og så videre. Organisasjonen rundt selve systemet kan som regel deles opp i en brukerorganisasjon og en driftsorganisasjon. Systemet diskutert i appendiks B kan stå som et konkret eksempel på den teknologiske delen: flere systemer knyttet sammen med et eller flere IP-nettverk, beskyttet fra offentlig tilgjengelig nett ved hjelp av brannmurer.

Kontinuerlig endring og utvikling bør også trekkes fram som et viktig fellestrekk for de fleste IKT-system.

En klar avgrensing av hva som skal analyseres er viktig for å komme i mål på tilmålt tid. I tillegg til å avgrense systemet eller objektet som skal analyseres, må en også spesifisere detaljeringsgraden til analysen. For et gitt IKT-system vil en aldri kunne analysere hele systemet ned i de minste detaljene. Detaljeringsgraden vil uansett avhenge av tilgjengelig relevant kompetanse.

Et IKT-system har sjelden en naturlig geografisk eller organisatorisk avgrensing. Det er derfor nyttig å bruke litt tid på å få klarhet i hvor en skal sette grensene for systemet i analysen. I tillegg vil årsaker for hendelser gjerne ligge utenfor selve IKT-systemet. Spesiell oppmerksomhet må rettes til hvilket nivå konsekvensene skal måles mot. En risikoanalyse er knyttet opp mot en ”eier” av systemet som skal vurderes og et sett med verdier. Risiko tolkes gjerne som potensielt tap, og man ønsker å kartlegge en eiers risiko for tap i forhold til en

mengde definerte verdier. Vanligvis knyttes verdiene direkte opp mot organisasjonens økonomi, anseelse/tillit og HMS.

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 tiltak risikoanalysen munner ut i. Hendelser kan gjerne ha umiddelbare konsekvenser som er alvorlige for samfunnet, men som ikke nødvendigvis medfører tap for virksomheten umiddelbart (selv om dette uansett vil gjenspeiles gjennom virksomhetens anseelse eller tillit, og på lengre sikt dens økonomi). Nivået for analysen bør derfor avklares ved analysens start.

4.1 Deltakere og praktisk arbeid

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. 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. Det første vil kreve deltakere med mye teknologisk spisskompetanse, mens det andre vil kreve deltakere med innsikt i virksomhetenes overordnede strategier. Likevel er det viktig å understreke at hovedmålet nettopp er å kombinere kunnskap og erfaringer fra eksperter, brukere og ledelse. Sammensetning av gruppen vil være avgjørende for resultatet av analysen.

Gruppene bør bestå av eksperter både på systemet som analyseres og på funksjonaliteten systemet skal yte. Et eksempel kan hentes fra ROS-analysen som BAS5 kjørte innenfor helsevesenet. Her ble både teknologisk driftspersonell for IKT-systemet samt brukere av systemet på avdelingene (sykepleiere, leger) involvert i samme gruppe, noe som ga en meget god sammensetning av kompetanse til analysen. For mer teknologiske analyser av er det i tillegg nødvendig med bred kompetanse og erfaring innen IKT-sikkerhet. Omfattende analyser kan også med fordel ledes av en fasilitator med erfaring innen risikoanalyse.

Deltagernes motivasjon for analysen og interesse for temaet har også vist seg å være meget sentralt for å få gjennomført en god analyse.

Selv om det kan være ønskelig å kunne 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. Gruppen bør dermed begrenses til relevante deltagere. Eksterne deltakere og observatører kan typisk legge demper på diskusjoner om sårbarheter i egne system. Alvorlige sårbarheter og svakheter dukker for eksempel typisk opp sent i analysen, når deltakerne føler tillit til de andre deltakerne.

Et viktig moment vil i enkelte tilfeller også være hvilket ledelsesnivå som skal være med i analysegruppen. Diskusjonen kan gå friere om sårbarheter i systemet eller mangler i organisasjonen dersom de høyeste ledelsesnivåene ikke er tilstede under selve analysen.

Spesielt for større grupper bør en ha med en egen referent med god oversikt over prosessen. Dette frigjør analyseleder til å drive diskusjonen og fange opp oppdukkende ideer.

Flere metodikker kommer med et egne rapporteringssystemer som kan forenkle arbeidet med dokumentasjonen underveis. Dersom en ikke bruker spesialisert programvare, står valget i praksis ofte mellom å bruke en tekstbehandler eller å bruke et regneark. En tekstbehandler fungerer bra dersom en ønsker å utføre grundigere kvalitative analyser på få hendelser (og bruke mer tid på hver), men dersom en har mange hendelser, vil et regneark eller en form for database være enklere å håndtere og også muliggjøre enklere eller automatisert rapporteringsfunksjonalitet.

Det finnes også analysemetodikker som inviterer til rent intervjubaserte analyser, i stedet for å bruke grupper. Denne typen analyser kan ofte være nødvendig av praktiske årsaker, når det ikke er mulig å samle riktig kompetanse til samme tid og sted. Imidlertid er erfaringen fra BAS5 at man med denne tilnærmingen mister en del sammenlignet med en gruppediskusjon. Meningsbrytninger forsvinner, metoden kan være tidkrevende og det er vanskeligere å få fram et helhetlig risikobilde etterpå.

4.2 Systemforståelse og modellering

Risikoanalysen krever at en har en oversikt over IKT-systemet som skal analyseres, gjerne i form av en modell av systemet til analyseformål. Her ligger en av hovedutfordringene i en IKT-risikoanalyse. I tillegg til å forstå de funksjonene som systemet skal utføre, må en 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 analysen som gjennomføres. 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.

4.2.1 Dokumentasjon

Oppdatert dokumentasjon og systemtegninger viser seg ofte å være vanskelige å få tak i. De fleste IKT-systemer er hele tiden i endring, med stadige oppgraderinger og utvidelser. Ofte er kunnskap om disse endringene fragmentert i organisasjonen – dette utgjør i tilfelle en risiko i seg selv. Som regel er det behov for dokumentasjon på flere nivå, fra fysisk infrastruktur til organisasjonssammensetting. Hvis arbeidsgruppen ikke har deltakere med denne type oversikt, må dette hentes inn på forhånd.

Selv i veldrevne IKT-systemer er det ofte mye ”lim” og udokumenterte løsninger som ”holder systemet sammen”. Slike forhold må også dokumenteres og tas med i analysen. Det samme gjelder spesielle arbeidsprosesser, for eksempel prosedyrer for å få systemet tilbake til normal drift ved feiltilstander.

4.2.2 Modellering

En form for modellering av systemet som skal analyseres er som regel nødvendig, selv om selve metoden som benyttes ikke er modellbasert. En god felles modell er viktig både for å kunne diskutere risiko i arbeidsgruppen og for å kunne kommunisere resultatene av analysen videre. Det er også nyttig å kunne ha *en* overordnet modell som utgangspunkt for diskusjoner under analysen, og ikke måtte hoppe mellom modeller av ulike systemdeler. Bruk av flere modeller kan bidra til å forvirre analysegruppen.

I IKT-verdenen finnes det mange ulike type modelleringsspråk, og mange verktøy og mye teori om for f.eks. pålitelighetsanalyse. BAS5-prosjektet har likevel ikke funnet noen universelle språk eller verktøy for å modellere komplekse IKT-systemer med tanke på trusler og sårbarheter. Enkelte unntak finnes likevel. CORAS er et eget rammeverk for modellbasert risikoanalyse av IKT-systemer, og spesifiserer et eget modellspråk basert på Unified Modelling Language (UML) for IKT-relaterte trusler og farer. Et slikt modelleringsspråk kan bidra som et presist språk for å dokumentere og arbeide med risikobildet, og gir altså noe mer enn en ”tegning” av systemet og risikobildet. For eksempel vil en kunne automatisere deler av arbeidet, arbeide mot samme modell med flere verktøy og eventuelt ta inn modeller fra andre domener.

”Misuse cases”[18] er annen ide basert på UML, der målet er å modellere negative scenarier for et system.[19] Mindre formalisert, men likevel mye brukt er ulike former for angrepstrær[20]. Med dette menes strengt tatt bare et hendelsestre der en lar ulike angrep være starthendelsene.

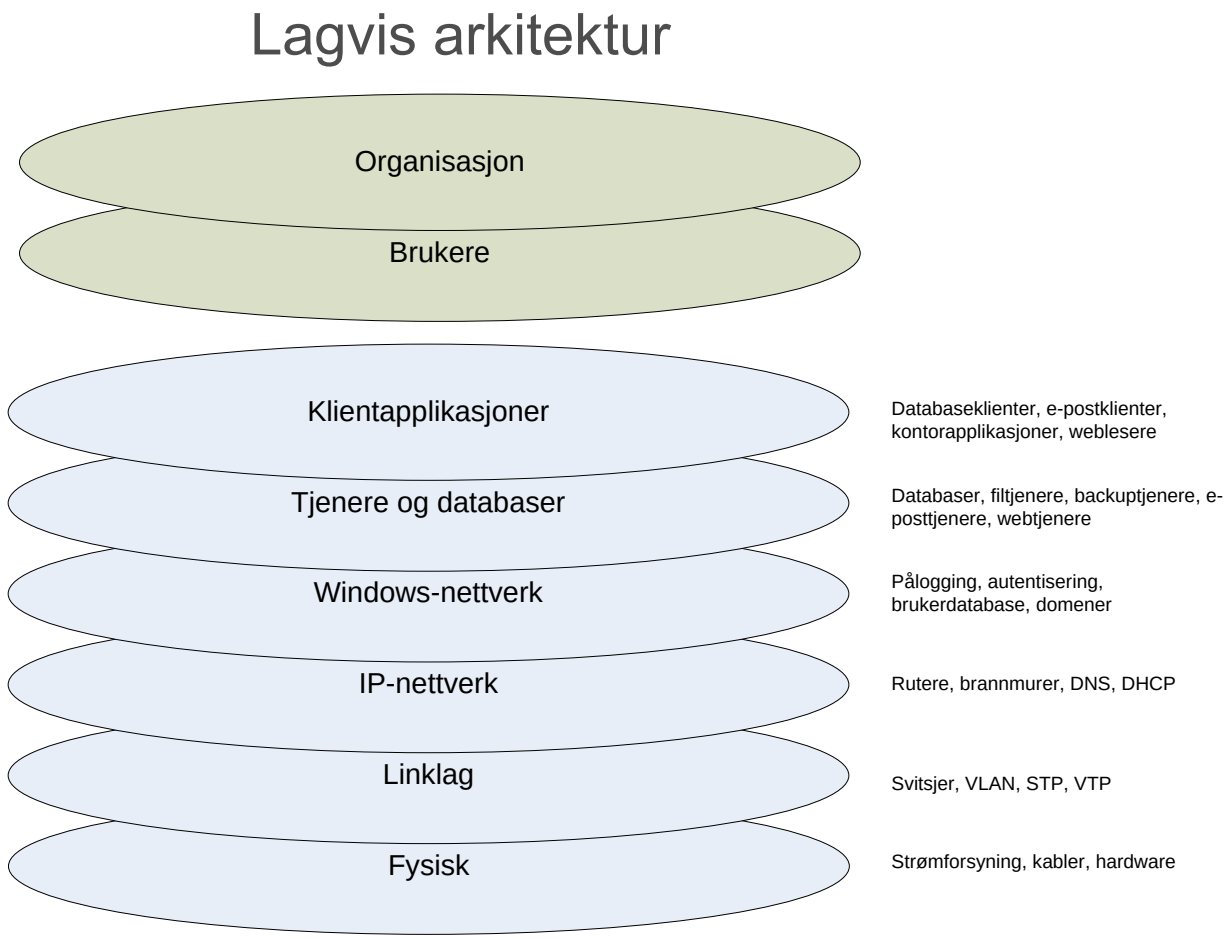
Hvilket nivå systemet modelleres på er avhengig av systemtypen og detaljeringsgraden som er bestemt i avgrensing, men modellering på flere nivå er som regel nødvendig. Dersom den valgte metodikken ikke har et eget modelleringsspråk, kan en enkel og forholdsvis intuitiv ”horisontal” inndeling oppnås ved å bruke nettverkslagene som utgangspunkt:

---

[18] Sindre G., Opdahl, A. L. (2005): ” Eliciting security requirements with misuse cases”, Requirements Engineering, Vol 10, No 1.
[19] Disse kan ses på som motstykke til UML ”use case” som brukes for å modellere *funksjonelle* krav i et system.
[20] http://www.schneier.com/paper-attacktrees-ddj-ft.html

- **Fysisk.** Bygninger, rom, dører, låser, vinduer, innsyn, adgangskontroller, kabler, kabeltraseer, strømtilførsel, nødstrøm, miljøpåvirkninger (brann, oversvømmelse osv.), annen fysisk sikring av maskinvare.
- **Nettverk.** Dette må ofte modelleres på flere nettverkslag. Svitsjer, rutere, brannmurer, servere for nettverksdrift og overvåking er aktuelle elementer. I større nettverk er det som regel mer enn bare ett linklag og ett netteverkslag: VLAN, VPN og andre tunneleringsmekanismer og virtualiseringsteknologier kan fort gjøre bildet uoversiktlig. 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.

Figur 4.1 ble brukt som illustrasjon i et av BAS5-casene, der en tilsvarende inndeling ble brukt i fareidentifikasjonsprosessen.



Figur 4.1 Lagvis arkitektur i et IKT-system

En slik ”horisontal” oppdeling, fra fysisk infrastruktur til organisasjon, kan være et godt utgangspunkt for å få med mange aspekter ved systemet. Spesielt for større system kan det også være nødvendig med en oppdeling per system eller per komponent. Videre er systemendringer alltid et moment i et IKT-system - det kan dermed være nyttig å modellere faser i utvikling og implementasjon av et system.

Avslutningsvis er det viktig å presisere at presentasjon gjennom en modell alltid innebærer en form for estimering av systemet. Deler av systemet utelates eller forenkles, og dette innebærer allerede en vurdering av risiko. Ideelt sett bør forenklingen kjenne igjen og identifisere standardløsninger med kjent risiko.

4.3 Fareidentifikasjon

Målet med fareidentifikasjonen er å identifisere de uønskede hendelsene som systemet kan bli utsatt for. Dette gjøres ved å identifisere trusler systemet er utsatt for og sårbarheter systemet innehar. Hovedutfordringen er hvordan en skal få med ”alt” som er relevant, uten å få med så mye at analysen ikke kan gjennomføres innen rimelig tid. For å unngå å bruke for mye tid på fareidentifikasjonen er sjekklister meget nyttige. Disse kan godt være generelle sjekklister som en kan finne i relevant litteratur, eller mer spesifikke sjekklister for det aktuelle systemet.

Mulighetene for gjenbruk av organisasjonens tidligere sjekklister benyttet i samme eller tilsvarende system er åpenbar.

Sjekklister, standarder og ulike ”beste praksis” finnes ofte som lister og kategorier av barrierer samt krav til disse. Dette er også mange eksperters innfallsvinkel til sikkerhetstenkningen, og det krever gjerne litt arbeid å få denne informasjonen og kompetansen integrert inn i fareidentifikasjonsprosessen. Enkelte barrierer, som for eksempel redundans, programvareoppdateringer, viruskontroll, nødstrøm og så videre kan enkelt konverteres til relevante uønskede hendelser, mens andre, som for eksempel overvåking, dokumentasjon, oversiktlighet, varslingsrutiner, generell sikkerhetskultur osv. kan kreve mer arbeid.

Selv om det ikke nødvendigvis er en god kategorisering i en analyse, finnes det et naturlig skille mellom tilsiktede og ikke-tilsiktede uønskede hendelser. I noen sammenhenger skiller en her mellom begrepene fare og trussel, der fare relateres til uhell og ulykker mens trusler relateres til tilsiktede handlinger. Denne distinksjonen blir ikke benyttet her.

4.3.1 Ikke-tilsiktede hendelser

Erfaringsmessig skjer de fleste uønskede hendelser i et IKT-system uten overlegg. Slike 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.[21]

[21] Digi.no (2001): ”Et tastetrykk stoppet Fellesdata”, 7. august 2001. http://php.digi.no/digi98.nsf/pub/dd20010810002101_hb_36307164

- Netcom opplevde i juni 2003 vannlekkasje i en sentral på Økern. Om lag 200.000 kunder ble rammet i sju timer.[22]

4.3.2 Tilsiktede hendelser

Med tilsiktede uønskede hendelser menes angrep eller manipulasjon på 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 en 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 en viss grad av anonymitet nevnes ofte. I tillegg til dette har IKT-markedet utviklet seg til å ha en forholdsvis høy smertegrense når det gjelder feil og sårbarheter i operativsystem og applikasjoner.

De siste par årene har en også sett en utvikling der økonomisk gevinst stadig oftere er målet for angrepene. Dette kan involvere alt fra utsendelse av uønsket epost eller fremvising av reklame, til for eksempel direkte angrep på økonomisk infrastruktur.

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 mot disse.

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.[23]
- DnB NOR virusangrep 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.[24]

Tilsiktede ondsinnede handlinger mot IKT-system kan være et vanskelig tema i en risikoanalyse. Både sannsynlighet for og konsekvens av denne type hendelser er forbundet med mye usikkerhet. Sannsynlighet er i prinsipp vanskelig å vurdere der villede handlinger er involvert, og spesielt er det vanskelig for nåværende IKT-system der en angripers muligheter for å utnytte et systemet i verste fall baserer seg på totalt ukjente sårbarheter (dette er sårbarheter som en risikoanalyse *ikke* vil avdekke).

---

[22] Itpro.no (2003): ”NetCom-skandalen: Uakseptabelt og kritikkverdig”, 13. juni 2003. http://itpro.no/art/3755.html
[23] Dagens Næringsliv (2006): ”Tappet 14.000 fra nettbank-konto”, 22. desember 2006. http://www.dn.no/forsiden/politikkSamfunn/article963881.ece
[24] Dagens IT (2007): ” Svinedyrt DnB Nor-mareritt”, 12. mars 2007. http://www.dagensit.no/bedrifts-it/article1046261.ece

I tillegg til usikkerhet knyttet til en eventuell angripers intensjon og muligheter overfor en konkret organisasjon, er det også vanskelig å få en god generell oversikt over trusselen en står overfor. Trusselbildet er stadig i endring, og det er til dels 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.

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 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 foretningslogikk tilsynelatende ikke skadelidende ettersom det ikke var et rettet virus angrep.

Vedlegg A omhandler disse truslene i noe mer detalj.

4.3.3 Identifikasjon av hendelser

Det er flere tilnærminger for å identifisere faresituasjoner og uønskede hendelser som skal vurderes i en risikoanalyse. En løsning er at en liste presenteres av fasilitator eller ”eksperter” på forhånd, for eksempel basert på en sjekkliste av typen som er presentert i Figur 4.2.

SJEKKLISTE
Ulykker/uaktsomhet
Tilgang via hjemmekontor: sikkerhet ved hjemmekontor **Tilgang via leverandør:** sikkerhet hos leverandør **Uaktsomhet**: slå av brannmur, bærbart utstyr med virus, pålogging, rutiner, prosedyrer **Feilhandlinger:** sette opp brannmur feil, feilkonfigurering, for mye access… **Gamle modemer:** faks, kopimaskin ….. **Ekstremt vær:** storm, vind, nedbør, flom **Brann:** brannsikring, design, slukkesystem **Vannlekkasje:** plassering av utstyr, design …….
Villede handlinger
Terror: spre frykt, skade, mulig mål, aktører, kompetanse **Kriminalitet:** bruk av data etc. for egen vinning, mulig mål, aktører, kompetanse **Hacker:** innbrudd for å komme inn **Virus:** ormer, trojanere….. **Utro ansatt:** oppsagt, i ubalanse… **Utro leverandør:** service personell, teknisk personell, …….
HARDE FAKTORER
Utstyr: feil/svikt, design, tilgjengelighet, pålitelighet, layout, levetid, utskifting, skade **Teknologi:** gammel, ny, kompleksitet… **Design:** filosofi, modifikasjoner, helhet, fragmentert, atskilte nett, VLAN **Utviklingstrekk:** fremtid, teknologiutvikling **Vedlikehold:** rutiner, prosedyrer, filosofi, oppdateringer **Grensesnitt/Avhengigheter:** mange, få, **Støttesystem:** strøm, HVAC, Telecom……. **Programvare:** kvalitet, sikkerhet, feil **Systemdokumentasjon:** prosedyrer, manualer, standarder, **Innkjøp:** rutiner, prosedyrer, filosofi **Kontrakter:** security, service … **Serviceavtaler:** tilgjengelighet, reservedeler, tid til rep…. **Dataadm:** tilgang, rutiner, **Ergonomi**: man-maskin interfrace, strekking, bøying, bevegelse **Adgangskontroll:** rutiner, prosedyrer **Tidspunkt:** tid på døgnet, årstid, ferie…..
MYKE FAKTORER
Mennesker: feil, kapasitet, følelser, sykdom, kultur, språk **Kompetanse:** erfaring, **Kommunikasjon**: normal, nød, muntlig, skriftlig, visuell, informasjon **Beslutning:** basis, ledelse, feil, forsinkelse **Trening:** krav, planlegging, behov, tilstrekkelig **Ressurser:** kvantitet, tilgjengelighet, kunnskap, kontraktør **Arbeidsmiljø:** stress, støtte, **Sikkerhetskultur:** holdninger, vaner, aksept, ledelse.. **Organisasjon:** antall brukere, kompetanse, kompleksitet …..
Barrierer/beredskap
Backupsystemer: prosedyrer, manualer, nødutstyr, aggregat, UPS **Sikkerhetssystemer:** …….. **Ledelse:** Beredskapsledelse, trening, scenarier…. **Trening:** Øvelser, **Analyser:** Risikoanalyser, bredskapsanalyser…..
..

Figur 4.2 Eksempel på sjekkliste for uønskede hendelser

Imidlertid kan det være et problem med ferdige lister som blir presentert til en arbeidsgruppe. Erfaringsmessig blir det da vanskelig å foreslå nye farer i plenum. Dersom en har nok tid, vil fareidentifikasjonen få mange nyttige innspill gjennom en idedugnad i arbeidsgruppen. Resultatet av denne kan deretter sorteres og eventuelt sikres med ekstern kompetanse før en

fortsetter analysen. En slik idedugnad med hele arbeidsgruppen er også nyttig for å bli kjent med kontekst, system og modell, samt for å sette i gang tankegangen om risiko i systemet. En bør søke å gjøre fareidentifikasjonen konkret for det systemet som skal analyseres, slik at prosessen ikke bare ender opp med en generell sjekkliste over faremomenter.

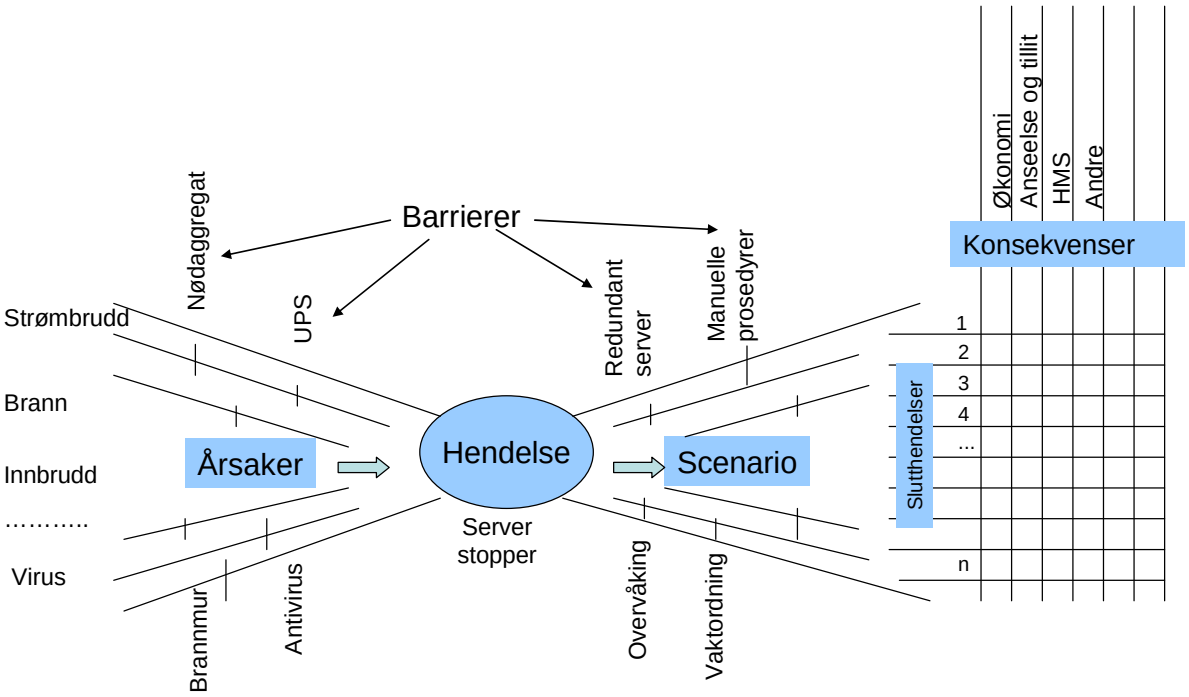
En mye brukt teknikk er å starte med hele eller deler av systemet som en svart boks, for så å gå gjennom alle veier inn i "boksen" som kan gi input til uønskede hendelser. Denne teknikken vil stort bare avdekke tilsiktede handlinger, og er ikke spesielt nyttig for å avdekke systemfeil eller andre interne hendelser. Det er erfaringsmessig heller ikke enkelt å få med alle aspekt av systemet i en slik analyse.

En annen start på en slik identifikasjon kan være å ta utgangspunkt i en modell som i avsnitt 4.2.2, og gå gjennom hvert av lagene tematisk: fysisk lag, nettverkslag, mellomlag, applikasjonslag, brukere og organisasjon. Dette kan hjelpe til med å få en strukturert gjennomgang av systemet, og hindre at en helt utelukker aspekt ved systemet. På alle disse lagene kan en ha ulike modeller, ulike trusler og sårbarheter og ulike sikkerhetsmekanismer, og de fleste vil påvirke hverandre gjensidig. For å kunne identifisere hele spekteret av farer er det nødvendig med bred kompetanse som dekker alle temaene. Figur 4.3 viser et eksempel på et skjema fra ett av BAS5-casene, som kan understøtte en slik tilnærming.

	Tilgjengelighet	Integritet, konfidensialitet, tilgangskontroll	Planlegging og dokumentasjon	Drift, vedlikehold, respons	Overvåking	Testing	Erfaringer
Fysisk							
Link							
Nettverk							
Windowsnett							
Applikasjon							

Figur 4.3 Sjekkliste fra en teknisk fareidentifikasjon gjort i et av BAS5-casene.

En tredje fremgangsmåte kan være å starte øverst med de funksjonene som systemet skal tilby, for deretter å gå "nedover" i systemet og identifisere kjeder av mulige feilhendelser. En slik fremgangsmåte vil lede fram til et feiltre, eventuelt et angrepstre. Metoden brukes typisk innen pålitelighetsanalyser der en angir sannsynligheter for de ulike initialhendelsene, slik at en kan komme fram til total sannsynlighet for de ulike hendelsene, og videre komme fram til kritikalitet for de ulike delsystemene. I de fleste IKT-risikoanalyser vil initialhendelsene være for komplekse eller avhenge av for mange eksterne faktorer til at en kan angi gyldige sannsynligheter, men metoden er likevel meget nyttig i en fareidentifikasjonsprosess.



Figur 4.4 Bowtie-modellen illustrerer årsaks- og konsekvensutvikling

Figur 4.4 viser en modell for årsaks- og konsekvensanalyse av en gitt hendelse (denne er ment for å illustrere ideen, ikke som mal for dokumentasjon). Hendelsen som skal analyseres står i en årsakskjede, og både før og etter hendelsen finnes barrierer som kan hindre eller redusere utviklingen. Barrierer til venstre vil redusere hendelsens sannsynlighet, mens barrierer til høyre vil redusere hendelsens konsekvenser.

En uønsket hendelse kan legges hvor som helst i denne tenkte årsakskjeden, men hvor en plasserer den vil være avgjørende for diskusjonen om hendelsen. Dersom en vil diskutere nødstrømsaggregat, legges hendelsen til venstre, og dersom en vil diskutere de manuelle rutinene organisasjonen har når en database går ned, legges hendelsen til høyre. For å få en god og konkret diskusjon er det ofte nødvendig å spesifisere nøyaktige hendelser. Sannsynligheter og konsekvenser vil endres på grunn av barrierer gjennom årsakskjeden, og en må være klar over hvilken hendelse en ønsker å analysere. Det er stor forskjell på ”fiber x blir fysisk kuttet” og ”fiber x blir fysisk kuttet og redundant kommunikasjonskanal virker ikke”. Der det er nødvendig kan en gjerne spesifisere flere hendelser i samme tenkte årsakskjede.

For å få en konkret diskusjon under risikovurderingen, bør også hendelsene spesifiseres med for eksempel varighet og omfang. For et strømbrudd er det for eksempel meget relevant å angi varighet og eventuelt hvilke kurser som forsvinner, og for et konfidensialitetsbrudd er det

tilsvarende viktig å vite hvilken type informasjon som er mistet, hvor store mengder som er mistet og hvem som eventuelt har fått tak i informasjonen. Der det er nødvendig, kan en spesifisere flere hendelser av samme type, men med varierende alvorlighetsgrad.

Driftsansvarlige, systemutviklere og andre teknikere med ansvar for et system har ofte egne interne og uformelle prioriteringslister og huskelister. Summen av disse vil som regel gi et meget relevant bilde av de tekniske tiltakene et system mangler. Denne informasjonen vil være meget nyttige innspill i en fareidentifikasjon. I tillegg vil en gjennomgang av eksisterende tiltak også være meget nyttig i forbindelse med fareidentifikasjonen. En kan her gå gjennom hvilke type hendelser de er tenkt å hjelpe mot, og om de er effektive i så måte.

4.4 Risikovurdering

Med utgangspunkt i resultatet fra fareidentifikasjonen, vil en under risikovurderingen vurdere sannsynlighet for og konsekvens av de spesifiserte uønskede hendelsene. Målet med vurderingen er å komme fram til sammenlignbar risiko for de ulike hendelsene.

Selv om de uønskede hendelsene er spesifisert på forhånd, er det viktig at denne prosessen gjøres dynamisk, slik at oppdukkende tema kan inkluderes eller eventuelt dokumenteres for framtidig arbeid. I tvilstilfeller er det spesielt viktig at hele vurderingene dokumenteres, ikke bare resultatet av vurderingen.

4.4.1 Årsak

I årsaksanalysen ønsker en å kartlegge de mulige hendelsesforløpene som kan forårsake en hendelse. Dette gjøres ved å se på mulige initialhendelser og på hvilke barrierer som kan stoppe eller begrense forløpet. Analysen munner som regel ut i en vurdert sannsynlighet for den gitte hendelsen, men det er også ofte nødvendig å dokumentere usikkerheten i årsaksanalysen. Sannsynlighet kan defineres enten som en antatt relativ frekvens eller som grad av tiltro til et gitt utsagn. En har her et skille mellom tradisjonell (”objektiv”) pålitelighetsanalyse og en mer ”subjektiv” risikovurdering. Erfaringene fra BAS5-casene tilsier at sistnevnte er nødvendig for å kunne favne om både ikke-tilsiktede og tilsiktede uønskede hendelser i et IKT-system.

For risikoanalyser i andre domener har en gjerne detaljert statistikk for feilhendelser og ulykker, men på grunn av den raske utviklingen av programvare, maskinvare og arkitekturløsinger har en for IKT-system sjelden et pålitelig statistisk grunnlag for uønskede hendelser. De historiske data som finnes vil dermed i liten grad være gjeldene for dagens system. Delvis på grunn av dette har også få organisasjoner et velfungerende system for å dokumentere alle typer uønskede IKT-relaterte hendelser.

For rent tekniske enkelthendelser, som harddiskhavari og strømbrudd, kan en ha gyldig statistikk. Som regel er likevel de hendelsene en ønsker å analysere mer komplekse, der en samtidig må vurdere flere barrierer og sårbarheter.

Mange feil og sårbarheter i et IKT-system er i tillegg av en ”binær” art, i den forstand at de enten finnes eller ikke finnes. Når en uønsket hendelse oppstår, vil feilen bli rettet, og hendelsen vil da normalt ikke oppstå igjen. I de logiske delene av systemet er heller ikke tema som slitasje og alder særlig relevante, og her er det også ofte mer kosteffektivt å reparere en sårbarhet enn å bruke tid på å vurdere graden av risiko.

Rettede og tilsiktede uønskede handlinger er det spesielt vanskelig å vurdere sannsynligheter for. En ”tilfeldig” angripers vilje og muligheter må her vurderes opp mot systemets (potensielt ukjente) sårbarheter. Vedlegg A omhandler dette i mer detaljer.

Hendelser med lav konsekvens og høy sannsynlighet viser seg ofte å være enkelt å diskutere i en risikoanalyse. Katastrofer, det vil si hendelser med høy konsekvens og lav sannsynlighet. er det vanskeligere å få til en god diskusjon om (”kommer aldri til å skje”, ”da er det uansett slutt”, ”det må det være andre som tenker på”). Riktig måte er ikke å droppe disse fra analysen, men heller å gi dem lav sannsynlighet.

4.4.2 Konsekvens

For å kunne vurdere risiko for ulike uønskede hendelser opp mot hverandre, må en kunne måle konsekvens med en felles metrikk. Det å lage og på en god måte anvende en slik felles metrikk, er ofte en av hovedutfordringene i en risikoanalyse.

Det er vanlig å kategorisere organisasjonens verdier i tre klasser og vurdere tap fra de uønskede hendelsene opp mot disse:

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

For hver uønsket hendelse analyserer en mulige konsekvensutviklinger og vurderer hvordan de ulike barrierene vil påvirke forløpet. Barrierene vil for eksempel være tekniske løsninger, redundant utstyr, vaktordninger, manuelle prosedyrer for fortsatt drift osv. Tids- og kostnadsperspektiv på gjenoppretting og ”friskmelding” av systemene må også tas hensyn til her. I et kompromittert system er det for eksempel ikke nok å rette opp sårbarhetene og deretter sette systemet i drift igjen. En må også forsikre seg om at integriteten til både applikasjoner og data er beholdt, og dette kan fort bli en lang og kostbar prosess.

Det vil ofte være mye usikkerhet forbundet med de ulike barrierenes virkningsgrad og kostnad ved bruk. Redundant utstyr kan for eksempel ha mindre kapasitet og dermed gjøre driften mindre effektiv, mens en overgang til manuelle reserveløsninger er avhengig av de ansattes

kjennskap til og erfaringer med aktuelle rutiner. Dersom usikkerheten knyttet til konsekvensutviklingen er for stor, kan en analysere disse i en egen konsekvensanalyse (for eksempel ved hjelp av en feiltreanalyse).

En spesifiserer konsekvens av de uønskede hendelsene i form av tap i en eller flere av de angitte kategoriene. En årsaks indirekte konsekvenser må også tas hensyn til her. Det at en server er nede en time kan for eksempel ha økonomisk konsekvens, uavhengig av om årsaken er et nettverksinnbrudd eller et strømbrudd. Konsekvensene med tanke på tillit til systemet vil derimot avhenge sterkt av opprinnelig årsak. I slike tilfeller kan også ukontrollert spredning av informasjon om hendelsen også påvirke hendelsens sluttkonsekvenser..

Det er vanlig å gradere tapene i de ulike konsekvensklassene basert på økonomisk tap. Denne inndelingen blir også brukt for IKT-systemer, men for at en slik konsekvensanalyse skal bli god, bør en sette av nok tid og ressurser til også å analysere konsekvenser utenfor selve IKT-systemet. Dersom en svitsj i et overvåkningsnettverk går ned, vil det være meget vanskelig å vurdere kostnadene av dette i en stor og kompleks organisasjon. For rent tekniske analyser bør konsekvenser heller måles i forholdsvis ”nære” konsekvenser, for eksempel kan konsekvensklassene beskrive nedetid for sentrale tjenester eller nettverk i systemet, konfidensialitetstap osv. En konsekvensanalyse som utvikles til domener utenfor analysegruppens kompetanse vil bare innføre mer usikkerhet i analysen. Likevel må en sammenligning mellom de ulike dimensjonene uansett gjøres før beslutninger om tiltaksprioritering skal tas, og dette kan gjerne gjøres i egne analyser.

Analyseleder må passe på at konsekvensklassene benyttes nøkternt og uniformt gjennom analysen.

4.5 Risikohåndtering

Etter at risikovurderingen er gjort, ender en opp med en rangert liste over uønskede hendelser eller en risikomatrise som illustrerer både sannsynlighet for og konsekvens av de ulike hendelsene. Dette gir likevel ikke umiddelbart en prioritering av relevante tiltak – enkelte tiltak kan for eksempel ha så lave kostnader at en uansett vil gjennomføre de selv om risikoen er lav, mens andre tiltak kan ha så store kostnader at de ikke lar seg gjennomføre. I tillegg er sjelden verken de analyserte hendelsene eller de relevante tiltakene uavhengige. Enkelte tiltak kan fjerne flere risikoer osv. Med andre ord må det foretas en kostnytteanalyse av de relevante tiltakene. Det vil også være aktuelt å analysere eksisterende tiltak i denne sammenhengen. De kan kanskje implementeres mer effektivt eller med mindre kostnader, eller kanskje tas helt bort (for eksempel ressurskrevende kontrollmekanismer som ikke er i bruk).

Dersom et tiltak tar bort hele risikoen forbundet ved en hendelse, vil nytte av tiltaket følge direkte fra risikovurderingen. Dette er imidlertid sjelden tilfelle, og en må dermed gjøre en vurdering av nytte eller effektivitet av tiltakene. På samme måte som vurdering av konsekvens og sannsynlighet er dette også en vanskelig oppgave. For tiltak som innføring redundant utstyr kan en få en forholdsvis presis vurdering, men spesielt for tiltak mot villede handlinger er det

meget vanskelig å vurdere nytte og effektivitet.

Det å vurdere reelle kostnader for tiltak kan også være vanskelig, siden de fleste tekniske investeringer vil ha driftsmessige kostnader i tillegg. For eksempel vil innkjøp av redundant utstyr kreve at det settes av mer tid til overvåking og testing. Videre er kostnadene til utstyr for overvåkning små i forhold til kostnadene ved å ha kompetent personell til å bruke og drifte dette utstyret. På samme måte er programvare for kryptering og signering av e-post meget billig i forhold til kostnadene ved å lage og opprettholde tjenester for tildeling og revokering av sertifikat og nøkler.

Dersom det er mulig, er det svært nyttig å sette opp tidsfrister for tiltak og ansvarlige for gjennomføring som en del av dokumentasjonen fra risikoanalysen. I praksis kan kostbare tiltak som regel ikke besluttes under selve analysen, men må vurderes opp mot andre system og forretningsområder. Det er dermed viktig at beslutningsprosessene i organisasjonen er tilrettelagt for å fange opp og behandle resultater fra risikoanalyser.

Som et siste steg i tiltaksprosessen må også restrisiko dokumenteres. I noen organisasjoner utformer en sluttdokumentasjonen etter en risikoanalyse som en kontrakt om tjenestenivå. Systemansvarlig kan da signere på at tiltakene vil bli gjennomført, mens avhengige brukere signerer for aksept av restrisiko.

5 OPPSUMMERING

Behovet for risikoanalyser innen kritiske informasjonssystemer flagges fra flere hold. Nasjonal strategi for informasjonssikkerhet[25] sier i klartekst at tiltak for å redusere sårbarheter i IKT-systemer skal baseres på risikoanalyser. I tillegg vil virksomhetene selv ha behov for å vurdere sikkerhet i sine IKT-baserte tjenester, og da anses risikoanalyser som et viktig hjelpemiddel for å velge blant ulike tiltak.

Det økte fokuset på risikoanalyser springer også ut av en oppfatning av at samfunnet har blitt kritisk avhengige av ulike IKT-systemer. BAS5-prosjektets arbeid understøtter en slik konklusjon, men peker også i retning av at vi vil bli langt mer avhengige i IKT i fremtiden. Da er det viktig at ulike risikoanalyser gjøres på riktig måte og med klare målsettinger. En risikoanalyse er på ingen måte et magisk verktøy som løser alle sikkerhetsproblemer i virksomhetene. Den gir ikke mer enn det virksomheten legger i prosessen rundt gjennomføringen av analysene, og i praksis innebærer analysene i første rekke en ”sorteringsprosess” av allerede tilgjengelig kunnskap på en systematisk måte. Validiteten til resultatene avhenger av valg og prioriteringer som blir gjort gjennom hele prosessen – målet er å få dette gjennomført på en strukturert måte, samt å dokumentere både resultatene og argumentene bak resultatene.

[25] Nasjonal strategi for informasjonssikkerhet - Utfordringer, prioriteringer og tiltak. Forsvarsdepartementet, Nærings- og handelsdepartementet, Justis- og politidepartementet, juni 2003.

Denne rapporten reflekterer rundt hvordan risikoanalyser for IKT-systemer ”best” kan gjøres i samfunnskritiske IKT-systemer. Den er skrevet fra et teknologifokus, og er blant annet ment som et innspill til Universitetet i Stavangers avsluttende rapport om risikoanalyseaktiviteten i BAS5.

Risikoanalyse av IKT-systemer vil på mange områder skille seg fra ”klassiske” risikoanalyser for industrien. Dette gjelder kanskje ikke så mye selve analyseprosessene som følges, men heller hva som bør gjøres i de ulike stegene av prosessen. Den viktigste bidragsyteren til dette er IKT-systemers egenskaper knyttet til:

- Systemer i nettverk, med komplekse gjensidige avhengigheter
- Hurtige endringer og dynamisk utvikling av system og teknologiske løsninger, sårbarheter, sikkerhetsløsninger, bruksområder og avhengigheter.

En stor del av arbeidet med risikoanalyser for IKT-systemer vil derfor gå med til å få oversikt over systemet. Modellering vil likevel være vanskelig, pga. momentene i punktlisten over. I tillegg er bred kompetanse og erfaring med relevant teknologi viktig, både for å kunne se helheten i systemet og for å kunne identifisere og vurdere sårbarhet.

I en IKT-risikoanalyse vil en normalt bruke mer tid på å finne sårbarheter enn å vurdere graden av risiko. Som en følge av dette vil også enkelte hevde at sikkerhetsarbeidet med et IKT-system ikke bør foregå ved hjelp av risikovurderinger, men ved et kontinuerlig arbeid med å lete etter sårbarheter. De sårbarheter som finnes må som oftest repareres, og kostnadene ved dette er som regel forholdsvis lave. Likevel kan man ikke lete etter sårbarheter og mangler i alle systemer samtidig, man må prioritere – altså vurdere risiko. Samtidig er det vanskelig å se for seg at *alle* sårbarheter som finnes kan repareres – da må det uansett gjøres en vurdering av nytte og kostnad av tiltak. Og nytte må i stor grad relateres til at tiltak reduserer risiko ved utnyttelse av ulike sårbarheter. Da slipper man ikke unna risikobegrepet.

I tillegg fokuserer rapporten spesielt på to forhold:

- Hvordan samfunnskritiske IKT-systemer ser ut og er bygd opp.
- Hvilke trusler IKT-systemer kan bli utsatt for.

Vår erfaring er at det ikke er en god ide å separere tilsiktede og ikke-tilsiktede hendelser i ulike analyser. Disse er nært knyttet sammen, og sikkerhet for begge innebærer de samme egenskapene. Årsakskjedene og konsekvensene blir ofte de samme uavhengig av opprinnelig årsak. Det samme gjelder hvilke tiltak som bør iverksettes for å redusere sårbarhetene overfor hendelsene.

APPENDIKS

LOGISKE TRUSLER MOT IKT-SYSTEMER

Dette avsnittet tar kort for seg aktører, metoder, trender og sårbarheter. Noen av momentene som tas opp er basert på et innledende arbeid av Bjørn Nilsen, NSM, i starten av BAS5.

Angrep mot IKT-systemer

Begrepet ”angrep mot IKT-systemer” tolkes meget forskjellig, og dette gjør tolking av tilgjengelig statistikk vanskelig. En intuitiv tolking av begrepet vil kanskje avgrense seg til rettede angrep. Imidlertid inkluderer nesten all statistikk om angrep også tilfeldige angrep fra selvspredende eller automatisk spredende programvare, og dette gir dermed ingen informasjon om angrep der en ondsinnet aktør med spesifikke mål angriper en gitt organisasjon. Det er heller ikke nødvendigvis gitt om statistikken bare kartlegger vellykkede angrep, eller om en også inkluderer mislykkede angrepsforsøk og kartlegging av systemer (disse to siste er det også vanskelig å skille fra hverandre).

Mye statistikk om IKT-angrep er ofte fokusert på opprinnelsesland for observerte angrep. Dette er også informasjon det er vanskelig å gjøre seg nytte av. Tilstandsløs trafikk kan trivielt forfalske avsenderadressen, noe som gjøres ved mange tjenestenektangrep. For trafikk fra selvspredende programvare er det programvarens egne algoritmer som vil avgjøre spredning, og dermed også opprinnelsesmønster. Dersom trafikken faktisk kommer fra et målrettet angrep, vil den som regel gå via kompromitterte maskiner, og målsystemet vil dermed ikke se faktisk opprinnelse. En angriper kan også benytte åpent tilgjengelige nettverk, eller i teorien gjennomføre angrep via et anonymiseringsnettverk.

Hvem angriper? - Aktørtyper

En grov kategorisering av aktørtyper med ulik motivasjon og kapabilitet kan være nyttig for å vurdere tilsiktede trusler i en risikoanalyse. På denne måten kan en vurdere ulike aktørers intensjoner og kapabiliteter opp mot et konkret system i en konkret organisasjon.

Amatører med automatiserte verktøy og trang til å utforske står bak en stor del av den ondsinnede trafikken på Internett. Det finnes mange offentlig tilgjengelige verktøy som kan brukes for å utforske og utnytte IKT-system via nettverk. Mange av disse har en lav brukerterskel, og de kan enkelt brukes uten noen inngående IKT-kompetanse. Med disse verktøyene kan en ved hjelp av få tastetrykk søke etter åpne tjenester eller kjente sårbarheter på tusenvis av maskiner, og ved hjelp av noen få ekstra tastetrykk få kontroll over de sårbare systemene en finner. Videre finnes det verktøy som gjør at fjernstyring og overvåking av en kompromittert maskin blir enkelt.

I en risikoanalyse vil en ofte se på denne typen aktører sammen med eksisterende selvspredende ondsinnet programvare som ”bakgrunnsstøy på Internett”. Utbredte sikkerhetsmekanismer som brannmurer, antivirus og ulike IDS-er vil stort sett gi en god beskyttelse mot dette. Det er likevel verdt å merke seg de potensielle konsekvensene denne typen hendelser kan ha på interne nettverk, som er antatt å være beskyttet fra omverdenen. Ondsinnet programvare kan for eksempel bli spredt via bærbart utstyr eller bærbare lagringsmedier, eller en ondsinnet ”amatør” kan få tilgang via tilgjengelige tilknytningspunkt til interne nettverk (for eksempel aktive fysiske nettverkspunkt eller VPN-forbindelser uten tilstrekkelig beskyttelse).

Mer kunnskapsrike **”hackere”,** med behov for anseelse, danner en annen aktørgruppe. Disse vil gjerne lete etter ukjente sårbarheter eller sette sammen flere teknikker og utføre mer avanserte angrep. Angrep vil gjerne rettes mot mål som gir høy status – dette vil ofte si organisasjoner med et antatt høyt sikkerhetsnivå (infrastrukturleverandører, finansforetak, enkelte offentlige organisasjoner osv).

Store deler av dette miljøet er endret til et mer akademisk miljø av ”sikkerhetseksperter”, der målet er å finne feil og sårbarheter i IKT-system, samt å utvikle og demonstrere angrep mot disse. I stedet for faktiske angrep oppnås anseelse gjennom publisering på konferanser[26] og i andre fora[27]. Publisering av sårbarheter gjøres gjerne etter at de aktuelle leverandørene er informert og feilen rettet, eller i samarbeid med leverandørene.

Ormer, virus og trojanere ble tidligere stort sett utviklet av disse to første aktørtypene, mens denne arenaen nå i stor grad er overtatt av personer eller grupper med økonomiske motiv.

Profesjonelle kriminelle har også inntatt IKT-domenet**.** I takt med samfunnets økende bruk og avhengighet av IKT, har en de siste årene sett en tilsvarende rask utvikling av IKT-kriminalitet. I motsetning til de overstående aktørkategoriene, er økonomisk vinning som regel motivet her. Tradisjonell kriminalitet som tyveri, utpressing og svindel har de siste årene blitt vanlig. Mest utbredt er trolig tyveri av kredittkortnummer og personlig informasjon som kan brukes videre til økonomisk vinning, men også annen sensitiv informasjon er ettertraktet. Interne dokumenter eller databaser over ansatte eller kunder kan brukes til utpressing eller selges videre til andre interesserte. En har også hatt flere tilfeller med utpressing, der organisasjoner har blitt truet med logiske angrep mot egne systemer. Svindel i form av ”phishing” har hatt et stort oppsving de siste årene. Enklest sett består dette av masseutsendt e-post som prøver å få intetanende brukere til å for eksempel oppgi passord eller andre opplysninger til websider som angriperen selv kontrollerer. Mer avanserte angrep kan utnytte tilgjengelig informasjon om en organisasjon, og sende spesialiserte meldinger som for eksempel utnytter etablerte tillitsforhold. Typisk utnytter en i tillegg svakheter i web- eller epostleser for å få angriperens side til å fremstå som gyldig.

[26] ”Black Hat”-konferansene er et eksempel på slike.
[27] Et eksempel er Uninformed, en journal for sikkerhetsteknologi, reverse engineering og lavnivåprogrammering (http://www.uninformed.org).

Vellykkede angrep mot norske nettbankkunder via kompromitterte kundemaskiner viser at disse angriperne har blitt forholdsvis sofistikerte, og at norskspråklige tjenester ikke er beskyttet mot angrep på tjenestenivå.[28]

Et viktig virkemiddel blant profesjonelle IKT-kriminelle er nettverk av kompromitterte maskiner under sentral kontroll (botnets). Nettverkene består av vanlige kontor- eller hjemmemaskiner med intetanende brukere, og kapasiteten brukes typisk til å sende ut store mengder spam, foreta tjenestenektangrep eller til å spre annen uønsket programvare til sårbare maskiner. Det å la nettverkene "klikke" på reklame på websider har også vist seg å være innbringende for eierne. Maskinene i slike nettverk kan også gjennomsøkes på jakt etter kredittkortnummer eller annen personlig informasjon, og tastaturloggere kan installeres for å fange opp pinkoder og passord. En meget stor del av den uønskede trafikken en ser på Internett kommer fra botnets. Sikkerhetsfirmaet Symantec identifiserte i første halvdel av 2006 rundt 60000 ulike nettverk som bestod av til sammen 4.5 millioner distinkte noder.[29]

Sammen med disse metodene har det også oppstått en egen økonomi der stjålet informasjon selges videre eller nettverk av kompromitterte maskiner leies ut eller selges. Foretak har også intetanende blitt involvert i dette, etter å ha leid inn tredjeparter for å få distribuert sin egen programvare.

Det finnes også en gråsone av aktører i denne klassen som distribuerer "uærlig programvare". Den økonomiske motivasjonen her er som regel spredning av reklame eller massiv innsamling av bruksmønster og lignende.

Utover vanlig kriminalitet har en også sett enkelte eksempler på såkalt "**hacktivisme**", der typisk webservere overtas og innholdet endres for å spre politiske budskap eller lignende. Våren 2006 traff en bølge av slike angrep flere danske og også enkelte norske webservere, trolig som reaksjon på Muhammed-karikaturene som ble trykket i danske og norske aviser.[30]

Mulighetene for **industrispionasje** øker også etter hvert som mer og mer informasjon blir tilgjengelig i digitale nettverk. En enkel trojaner installert på riktig maskin kan sende ut dokumenter og logge all aktivitet på maskinen, inkludert lyd fra mikrofon eller bilder fra tilknyttede kamera. Trojaneren kan installeres via nettverk på en sårbar maskin eller etter få minutters fysisk tilgang til en vilkårlig maskin. Dersom selve installasjonen ikke oppdages, kan det i ettertid være nærmest umulig å komme fram til hvem som står bak (utsendt informasjon kan for eksempel krypteres og postes til offentlig tilgjengelige fora).

Et eksempel her er et israelsk firma som brukte en spesiallagt trojaner for å få sensitiv informasjon fra flere bedrifters interne nettverk. Informasjonen ble via tredjepersoner senere

---

[28] Se for eksempel Dagens Næringsliv 22. desember 2006, "Tappet 14.000 fra nettbankkonto". http://www.dn.no/forsiden/politikkSamfunn/article963881.ece

[29] Symantec Internet Security Threat Report, Volume X.

[30] I følge http://comon.dk/index.php/news/print/id=25640 ble 2700 danske organisasjoner angrepet, men det er ellers lite innsamlet informasjon om hendelsene.

solgt til en rekke konkurrerende bedrifter.[31] Et annet illustrerende eksempel er et tilfelle der penetrasjonstestere la ut minnepinner utenfor inngangsdørene til bedriften som skulle testes – etter kort tid var programvare fra minnepinnene installert på flere av bedriftens interne maskiner.[32]

Trusselen fra **insidere** må også vurderes i en risikoanalyse. Egne ansatte, tilknyttede konsulenter osv. har som regel tilgang til mye informasjon om en organisasjons IKT-system, og kan også ha muligheter for å dekke over egne spor. Erfaringene viser at mange organisasjoner av bekvemmelighetsgrunner har vide interne tilgangsrettigheter i systemene. Det at en flere steder også benytter fellesbrukere på systemene gjør det i tillegg vanskelig å spore opp årsaker til eventuelle sikkerhetsbrudd. Mange mangler også ressurser og system for deteksjon av interne sikkerhetsbrudd. Motiv kan for eksempel være vinning, hevn eller ren nysgjerrighet.

Muligheter for misbruk av organisasjonens IKT-ressurser bør også vurderes i en slik sammenheng. Bruk av uautorisert programvare øker gjerne sårbarheten i systemet, og bruk av organisasjonens IP-adresser og domenenavn i feil sammenheng kan stille organisasjonen i et dårlig lys.

Det finnes mange rapporter om **terrorisme** finansiert ved IKT-kriminalitet, og det er også dokumentert at terrorister har brukt Internett til rekruttering og annen kommunikasjon.[33] Likevel har hittil ingen IKT-angrep allment blitt kategorisert som terrorisme. Terrorister søker å spre frykt og usikkerhet, og en generell tese er dermed at de heller vil bruke sprengstoff og andre fysiske virkemiddel enn ulike elektroniske virkemidler. Virus og ormer er i dag rutinemessige, og vil i liten grad skape frykt. Et logisk angrep mot kritisk infrastruktur vil trolig kreve meget store ressurser, og vil trolig også måtte bestå av koordinerte angrep mot flere ulike system for å gi samme effekt som de tradisjonelle fysiske virkemidlene.[34]

Fremmede staters bruk av logiske angrep forbindes gjerne med etterretning, og det finnes dermed lite tilgjengelig offentlig informasjon om temaet. På lengre sikt vil en trolig se logiske angrep utnyttet som en militær kapasitet – i tillegg til rent militære mål kan system som støtter eller driver kritisk infrastruktur antas å være potensielle mål for denne type operasjoner.

I et av BAS5-casene ble det foretatt en innledende trusselanalyse basert på en tilsvarende oppdeling av aktørtyper og mulig motivasjon. Figur A.1 viser utdrag fra skjemaet som ble brukt. Selv om en ikke gjennomfører prosessen som en grundig analyse, kan det være et nyttig verktøy for å sette i gang diskusjon og tanker i forbindelse med en fareidentifikasjon.

---

[31] The Guardian (2005): ”London couple remanded in Israel's biggest industrial espionage case”, 31. mai 2005. http://www.guardian.co.uk/israel/Story/0,2763,1495716,00.html

[32] http://www.darkreading.com/document.asp?doc_id=95556&WT.svl=column1_1

[33] Se for eksempel ”Cyberterrorism: The Sum of All Fears?”, Gabriel Weimann, Studies in Conflict and Terrorism, 2005

[34] Se overnevnte eller ”Terrorist Capabilities for Cyber-attack”, Clay Wilson, CIIP Handbook 2006 vol 2.

Trusselanalyse					
Motivasjon	**Virkemiddel**	**Aktører**	**Sannsynlighet**	**Konsekvens**	**Kommentarer**
			Svært sannsynlig Meget Sannsynlig Sannsynlig Lite Sannsynlig	Katastrofalt Kritisk Farlig Lite Farlig	
Utforskning, nysgjerrighet	logiske	hackere kunder			Automatiske verktøy, manipulering av webinterface og databaser
Prestisje	logiske sosiale	hackere			Ukjente sårbarheter i infrastruktur, mangelfulle sikkerhetsrutiner
Hevn	logiske fysiske sosiale	oppsagt ansatt forvirret ansatt andre tilknyttede			God kjennskap til interne rutiner og system, ikke tilbaketrukket autorisasjon, kjennskap til passord
Økonomisk (direkte eller via utpressing	logiske sosiale	organisert kriminalitet enkeltpersoner ansatte insidere			Manipulere databaser til egen fordel, uthenting av informasjon. Trusler om logiske angrep. Insidere med ekstra informasjon.
Publisitet (feks "hacktivisme")	logiske fysiske	politiske grupper terroristgrupper			Angrep som ikke trenger være "effektive" - feks defacing av
Spre kaos og usikkerhet	fysiske sosiale logiske	terroristgrupper fremmede stater			
Politiske/militære mål	logiske fysiske	terroristgrupper fremmede stater utilsiktet skade fra fremmede staters			Rettet angrep mot infrastruktur, angrep fra interne nettverk. Manipulering av applikasjonsdata.

Figur A.1 Utdrag fra matrise brukt i en trusselanalyse i forbindelse med et av BAS5-casene.

Trender og sårbarheter.

Potensialet for programvaresårbarheter finnes i alle typer systemer og på alle logiske nivå, men hvilken type nye sårbarheter som oppdages er i stor grad drevet av trender i sikkerhetsmiljøene. Tidligere lette en typisk etter sårbarheter i kjernefunksjoner i operativsystem og serverprogramvare. Disse sårbarhetene er ofte de mest effektive, siden de gjerne gir administratortilgang til de gjeldende systemene. Sårbarheter som oppdages i operativsystemer vil også finnes på flere maskiner og er dermed nyttigere for en angriper.

Etter mange år med angrep har operativsystem og serverprogramvare blitt mer robuste, samtidig som brannmurer og NAT-teknologier[35] generelt har gjort systemene mindre tilgjengelige fra utsiden. Dette har ført til et økt fokus på sårbarheter i klientapplikasjoner som weblesere og kontorapplikasjoner.

Weblesere har stadig blitt mer komplekse, med støtte for mer og mer funksjonalitet. I praksis betyr dette at de skal være i stand til å tolke flere forskjellige typer innhold, noe som igjen øker sannsynligheten for feiltolking og sårbarheter. For eksempel finnes det flere eksempel på at noe så enkelt som et feilkonstruert bilde kan få webleseren til å kjøre vilkårlig kode. Sårbare kontorapplikasjoner kan utnyttes tilsvarende ved å få en bruker til å åpne et dokument med

[35] NAT (Network Address Translation) er en teknikk som brukes for å la flere maskiner i et nettverk kommunisere ut på for eksempel Internett gjennom samme globale IP-adresse. Maskiner på utsiden av nettverket kan da normalt ikke initiere forbindelser til maskiner på innsiden, noe som gir en viss sikkerhetseffekt.

ondsinnet kode. Disse dokumentene kan spres gjennom mange kanaler, og de kan ha alvorlige konsekvenser hvis de tas med på innsiden av interne nett.

På serversiden har de oppdagede sårbarhetene og dermed også angrepene i stor grad flyttet seg oppover i de logiske lagene. I stedet for å angripe webserveren direkte, retter en angrepet mot det innholdet webserveren tilbyr og de bakenforliggende applikasjonene. Sårbarhetene her kommer som et resultat av mer interaktive websider som gjerne støttes av egenutviklede webapplikasjoner med lav kvalitet.[36] Angrepene vil ofte bare rette seg mot innhold i databaser som webserveren benytter, men de kan potensielt også føre til total systemovertagelse av webserveren. Faren for indirekte angrep mot andre klienter som bruker samme webapplikasjon er forsterket på grunn av flere og flere websider som viser fram brukerprodusert innhold.

Muligheter for sårbarheter i dedikerte nettverkskomponenter som rutere og brannmurer har fått mye omtale de siste årene, på grunn av de potensielt alvorlige konsekvensene et angrep mot disse vil kunne ha. En har likevel så langt ikke sett effektive angrep mot disse, utover tradisjonelle ormer som aktivt utfører tjenestenektangrep mot de nærmeste nettverkskomponentene.

Mobiltelefoner og andre håndholdte enheter gir også potensielt mange muligheter for en angriper. Etter hvert er det lite som skiller disse fra andre datamaskiner, og de har åpenbart gode muligheter for ekstern kommunikasjon. Dette satt sammen med innebygde digitale kamera og muligheter for taleopptak, gjør at konsekvensene av et angrep kan bli store. Likevel har en hittil sett forholdsvis få eksempel på ondsinnet kode for denne typen utstyr.

Et marked for kjøp og salg av informasjon om sårbarheter og fungerende angrep har vokst fram den siste tiden. Dette skjer trolig hovedskalig i kriminelle miljø, der sårbarhetene direkte kan benyttes til vinningskriminalitet. Enkelte sikkerhetsfirma lever også av å tilby beskyttelse i de tilfeller der sårbarheten ennå ikke er rettet opp av leverandøren, eller der firmaet har fått kjennskap til ellers ukjente sårbarheter. I følge Trend Micro ble det i desember 2006 tilbudt informasjon om sårbarheter som kunne gi uautorisert tilgang til nyeste versjoner av Windows for 20.000-50.000 USD.[37] Enkelte leverandører har innført belønningsordninger der rapportering av alvorlige feil premieres på ulike vis, i håp om motvirke salg på svartebørs.

Virkemiddel

Ondsinnet programvare eller ”malware” brukes gjerne som en fellesbetegnelse på programvare med forskjellige ondsinnede virkninger. Eksempler er ormer, virus, trojanere og bakdører. Applikasjoner for avlytting, overvåking og fjernstyring havner også ofte i samme kategori, selv om disse også kan benyttes som driftsverktøy. Litt på siden av disse finner en også en kategori som en kan kalle ”uærlige programmer”. Dette er programmer som helt eller delvis lyver om sin funksjonalitet. Programmene framstår gjerne som ”nyttige” gratisverktøy som for eksempel

[36] I første halvdel av 2006 stod sårbare webapplikasjoner for nærmere 70% av alle sårbarhetene dokumentert av Symantec. Symantec Internet Security Threat Report, Vol X.
[37] http://www.eweek.com/article2/0,1895,2073611,00.asp

skjermsparere, sikkerhetsverktøy eller søkeverktøy, men inneholder også ekstra funksjonalitet som normalt er uønsket. Dette kan for eksempel være reklamevisning (adware) eller informasjonsinnsamling (spyware).

Navngiving av ondsinnet programvare varierer en del, og det har etter hvert blitt forholdsvis vanskelig å kategorisere ulike instanser entydig. Per i dag er det ikke uvanlig at samme programvare spres på ulike måter, og underveis oppdateres med ny funksjonalitet. Vi vil her kort gå gjennom noen av de ulike egenskapene ondsinnet kode kan ha og noen av virkemidlene de bruker.

Spredning
Selv om programvaresårbarheter ofte får mye oppmerksomhet, spres veldig mye ondsinnet programvare via ren sosial manipulasjon. For eksempel spres mesteparten av de selvspredende variantene (ormer) typisk ved å sende eksekverbare filer som vedlegg til epost.[38] Brukeren lures til å kjøre filen og blir dermed infisert. På tilsvarende måte kan brukere lures til å laste ned ondsinnede filer fra websider, fildelingsnettverk osv.

Effekt
Idet den ondsinnede programvaren er installert på en maskin, vil den kunne gjøre det samme som brukeren som fikk den installert. Noen eksempel:

- All tilgjengelig informasjon kan gjennomsøkes. For eksempel kan en lete opp kredittkortnummer, personidentifiserende informasjon, passord osv. Selvspredende programvare vil også lete etter nye infeksjonsmuligheter (for eksempel epostadresser eller aktive fildelingsklienter).
- Informasjon kan forandres. For eksempel kan innhold på websider forandres.
- Ny programvare kan lastes ned og installeres. Programvaren kan oppdatere seg selv eller laste ned programvare til andre formål. Dette kan for eksempel være programvare for masseutsendelse av epost, tastaturloggere, programvare for distribuerte tjenestenektangrep osv.
- Nettverksforbindelser kan opprettes. Dette kan gjøres for å sende tilbake innhentet informasjon, for å muliggjøre fjernstyring eller for automatisk viderespredning.
- Tilkoblede enheter kan overvåkes og kontrolleres. Mikrofoner og webkamera kan benyttes og andre tilknyttede maskiner kan styres (for eksempel mobiltelefoner og PDA-er).

Skjuling
For å vanskeliggjøre analyse av ondsinnet programvare brukes gjerne ulike obfuskeringsteknikker og anti-debuggingteknikker. Det vil for eksempel innebære at programmet bruker utradisjonelle systemkall og gjerne udokumentert funksjonalitet for å forvirre. Selvspredende programvare kan i tillegg endre seg selv for å unngå signaturbasert deteksjon (polymorfi).

[38] For eksempel spres utbredte familier som Netsky, MyDoom og Stratio på denne måten. Ref http://www.sophos.com/pressoffice/news/articles/2007/01/toptenjan07.html

Rootkits er en betegnelse på teknikker som skjuler kjørende program, filer, nettverksforbindelser eller lignende for deler av operativsystemet og dermed også for legitime brukere av systemet. Mange av teknikkene som brukes har lenge vært kjente, men en har i de siste årene sett en massiv økning i faktisk bruk. Tidligere ble teknikkene stort sett brukt for enkelte trojanere, men de har i de siste årene blitt tatt i bruk for flere typer ondsinnet programvare. Det finnes flere offentlig tilgjengelige program og bibliotek som tilbyr slik funksjonalitet.

Utvikling
Allerede da utviklingen av MS-DOS-virus startet på 1980-tallet, var utviklingsmiljøene preget av kollaborativ utvikling og åpen utveksling av informasjon om teknikker og metoder. Denne trenden har fortsatt, og en finner i dag ondsinnet programvare som utvikles ved hjelp av profesjonelle utviklingsmetoder. Dette innebærer typisk at en har et prosjektbasert utviklingsmiljø med flere bidragsytere, versjonskontroll, bugfixer, modulbasert programvare, muligheter for oppgradering av aktive instanser av programvaren osv.[39]

For botnets finnes det også ferdige rammeverk for å effektivisere utviklingen. Disse er gjerne modulbaserte, slik at ulike sårbarheter kan benyttes for å få tilgang til nye maskiner.

For rettede angrep finnes både kommersielle og fritt tilgjengelige verktøy for utføre angrep, og også rammeverk for å støtte utviklingen av nye typer logiske angrep.

Litteratur, undersøkelser og videre informasjon.

NorCERT er et senter underlagt Nasjonal sikkerhetsmyndighet (NSM) som har som primæroppgave å koordinere respons ved alvorlige IKT-sikkerhetsangrep mot viktig infrastruktur i Norge. Senteret arbeider med innhenting av informasjon om alvorlige IKT-relaterte trusler, sårbarheter og hendelser, og skal også kunne bidra med råd og konkrete tiltak når slike hendelser inntreffer. NorCERT er Norges kontaktpunkt mot tilsvarende organisasjoner i utlandet. Under samme enhet hos NSM ligger også Varslingssystem for digital infrastruktur (VDI). VDI-sentralen samarbeider med utvalgte offentlige og private organisasjoner som driver eller støtter opp om kritisk infrastruktur i Norge og identifiserer angrep og kartleggingsaktivitet fra Internett mot disse. Hver måned gir VDI-sentralen ut en offentlig tilgjengelig statusrapport fra siste måneds aktivitet.

Norsk senter for informasjonssikring (NorSIS) er finansiert av Fornyings og administrasjonsdepartementet samt en del private og offentlige sponsorer. Senteret arbeider primært mot små og mellomstore virksomheter i privat og offentlig sektor og gir ut veiledninger om IT-sikkerhet og informasjon om relevante trusler og sårbarheter.

Mørketallsundersøkelsene er en serie med undersøkelser som utarbeides av Datakrimutvalget i

[39] McAfee (2006): ”Global Threat Report”, Vol 1, juli 2006.

Næringslivets sikkerhetsråd (NSR). Undersøkelsen gjøres via spørreskjema til et bredt spekter av norske virksomheter innen både privat og offentlig sektor. Generelt er målet med undersøkelsen å belyse omfanget av datakriminalitet og andre uønskede IKT-hendelser hos norske virksomheter. Spesielt ønsker en å belyse i hvor stor grad denne typen hendelser rapporteres eller anmeldes til politi og andre myndigheter. Den femte undersøkelsen ble foretatt i mai 2006[40]. Internasjonalt foretas det også jevnlige mørketallsundersøkelser. Eksempel finnes i Sverige[41], Storbritannia[42] og USA[43].

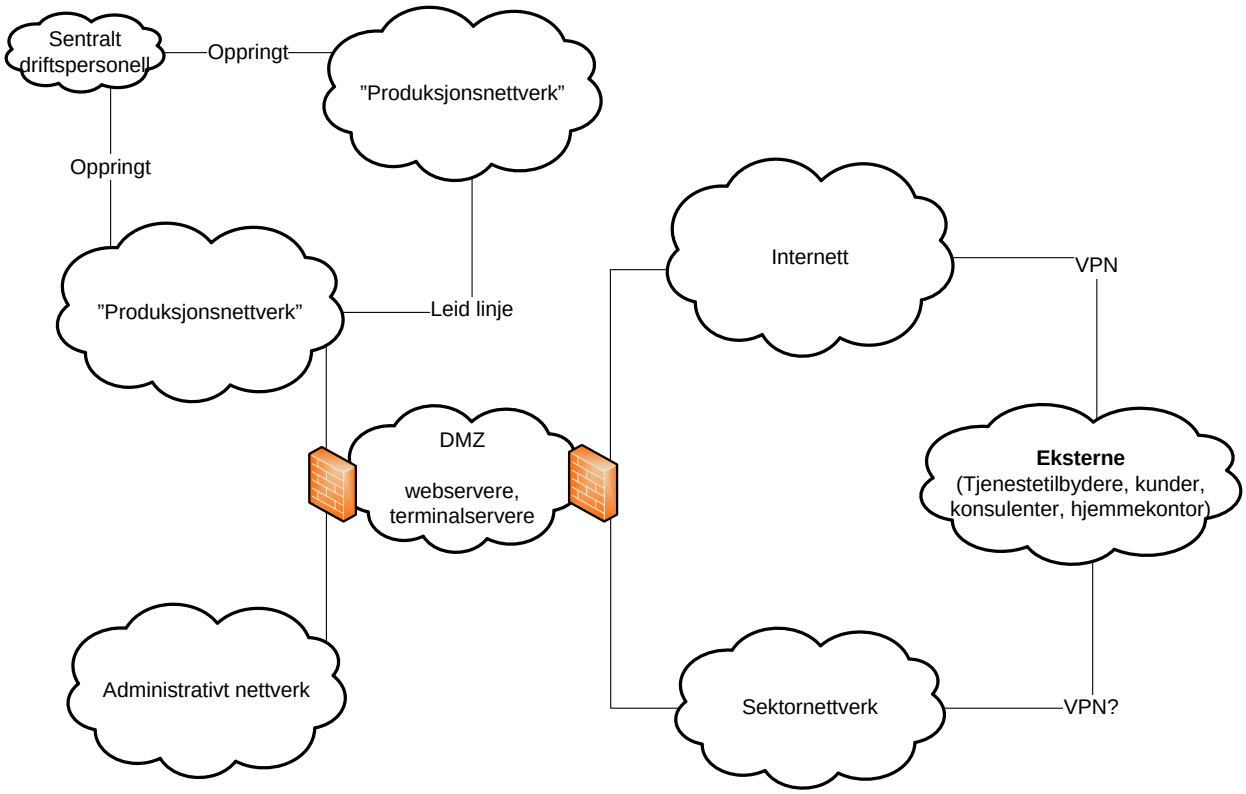
Oppdatert informasjon om trusler og trender kan også finnes i periodiske rapporter fra antivirusselskap som for eksempel McAfee og Symantec.

[40] Næringslivets sikkerhetsråd (2006): ”Mørketallsundersøkelsen om datakriminalitet 2006”.
[41] Post & Telestyrelsen: “Mörkertalsundersøkningen 2005 - Svenska organisationer om IT-säkerhetsincidenter”. Post & Telestyrelsen, 5. juli 2005
[42] PriceWaterhouse Coopers: “DTI Information security breaches survey 2006”. Technical report.
[43] Gordon, L A., Loeb, M P., Lucyshyn, W. and Richardson, R.: “2006 CSI/FBI Computer crime and security survey”.

HVORDAN SER SAMFUNNSKRITISKE IKT-SYSTEMER UT?

Oppbygging

Det er lite som skiller IKT-systemer som inngår i samfunnskritisk infrastruktur fra andre IKT-systemer. Teknologien, arkitekturen og bruksmønstrene er ikke ulike de som finnes andre steder.



Figur B.1 Generell nettverksskisse

Figur B.1 skisserer hvordan den grunnleggende IKT-infrastrukturen typisk ser ut. Normalt vil virksomheten ha et eget produksjonsnettverk, der kjernevirksomheten foregår eller styres/støttes fra. Systemene her består gjerne av proprietære, spesialtilpassede eller egenutviklede løsninger. Produksjonsnettverket og de tilknyttede systemene har som regel mindre dynamikk (færre endringer og oppgraderinger) enn det resterende nettverket. Ved større endringer i disse systemene, vil en normalt måtte teste endringene i et separat testmiljø på forhånd. Dette innebærer også si at sikkerhetsoppdateringer av programvare og komponenter skjer sjeldnere her.

I tillegg er det som regel et eget nettverk for administrative oppgaver. Systemene her består som regel av vanlige kontormaskiner med standard programvare. Oppgavene som løses her krever

som regel nettverkstilknytninger både til produksjonssystemene og til nettverk utenfor organisasjonens domene (for eksempel til Internett eller til ulike sektornettverk).

En ”demilitarisert sone” (DMZ) er en egen nettverkssone som skiller mellom nettverk med ulike sikkerhetsnivå. Denne er som regel implementert som en grense mellom produksjonsnettverket og administrasjonsnettverket, og samtidig som en grense ut mot offentlig tilgjengelige nett eller sektornettverk. Filtreringen gjøres ved hjelp av brannmurer, som ofte må omkonfigureres på grunn av systemendringer eller innføring av nye tjenester.

Integrasjon av tjenester og nettverk

En ser stadig en utvikling der flere og flere system kobles sammen og ulike tjenester integreres. I et sikkerhetsperspektiv byr dette på mange utfordringer. Systemene blir mer komplekse og får flere gjensidige avhengigheter – mulighetene for feilhendelser blir dermed vanskeligere å analysere og konsekvensene vanskeligere å forutsi. Sammenkoblingene fører også til at system med ulike sikkerhetsnivå kobles sammen, og dette øker faren både for lekkasje av sensitiv informasjon ut av interne nettverk og faren for å få uønsket programvare eller direkte angrep inn i interne nettverk. Systemene med høyere sikkerhetsnivå viser seg ofte å ikke være sikret med nødvendige oppdateringer, og en bruker typisk også svakere mekanismer for autentisering i slike ”atskilte” nettverk. Barrierene som skiller mellom disse sonene blir dermed meget viktige i en sikkerhetskontekst. På lavere lag vil barrierene være brannmurer og for eksempel VPN-konsentratorer, mens de på høyere lag gjerne vil bestå av terminalservere og applikasjonsservere. Det er også verdt å merke seg at disse barrierene selv kan skape sårbarheter i systemet - de utgjør naturlig nok eneste mulig vei mellom sikkerhetssonene, og feilhendelser her kan dermed stoppe viktige tjenester som krysser sonene.

Krav om økt tilgjengelighet og fleksibilitet har også gjort mobile kontor og hjemmekontor vanlige. De interne nettverkene vokser dermed i stor grad ut av de domenene organisasjonen selv har kontroll på (et hjemmekontor for å drive kritisk infrastruktur har naturligvis også mange sikkerhetsproblemstillinger utover de rent tekniske). Løsninger der eksterne konsulenter og leverandører har tilgang inn i interne nettverk er også utbredt.

Rent teknologisk er nettverkene som regel realisert i et felles IP-nettverk, og denne teknologien brukes flere og flere steder helt ut i produksjonssystemene. Tidligere bestod produksjonsnettverkene av spesialiserte og proprietære komponenter med egne kommunikasjonsløsninger, mens en nå heller har sensorer og styringsenheter direkte koblet til et IP-nettverk. Det samme underliggende nettverk brukes også i større grad til telefoni, alarmsystem, videokonferanser, videoovervåking osv. Det er dermed ikke gitt at en kan ta en telefon når nettverket går ned. En slik integrasjon av ulike tjenester gir også behov for kvalitetsdifferensiering i nettverket.

Virtualisering av nettverk er mye brukt for å gi økt fleksibilitet og potensielt forenklet drift og styring. Virtualiseringen kan gjøres på flere nettverkslag, men den underliggende ideen er at flere virtuelle forbindelser skal kunne dele en felles underliggende kanal uten at de i særlig grad påvirker hverandre. For mange kritiske IKT-system er disse teknikkene sentrale i utbyggingen av nødvendig redundans. Nettverkstrafikk med ulike sikkerhetsnivå legges da på samme fysiske

infrastruktur, mens den fysiske infrastrukturen bygges ut med redundans. Naturligvis innfører dette også ny sikkerhetsproblematikk. Feilkonfigurerte komponenter kan lekke trafikk mellom nettverkene, og for mange løsninger vil en overbelastning i en av de virtuelle forbindelsene også påvirke andre forbindelser negativt. Utviklingen går også i retning av at både servere og tradisjonelle nettverkskomponenter virtualiseres for å gi enda mer fleksibilitet i driften.

Hyllevare

Innenfor virksomhetene BAS5 har vært i kontakt med er det utstrakt bruk av hyllevare (COTS – Commercial Off The Shelf) i IKT-systemene, også i produksjonssystemene. Som regel benyttes standard IP-nettverk med standard nettverkskomponenter, og proprietære og bransjespesifikke protokoller er i ferd med å byttes ut til fordel for (eller legges over) åpne og utbredte protokoller (IP-nettverk, e-post, webtjenester osv.). For endeutstyr ser en også den samme utviklingen – maskinvare, operativsystemer og applikasjoner består i større og større grad av hyllevareutstyr.

Det er både fordeler og ulemper ved at standardutstyr benyttes. Standardutstyr velges som regel på grunn av lavere kostnader, men også bedre tilgang til kompetanse kan være en viktig årsak.. Flere sikkerhetsaspekt dukker imidlertid opp i forbindelse med bruk av hyllevare. Kvaliteten kan bli et problem dersom man ønsker å spare enda mer ved å bruke billige komponenter (et typisk eksempel er nettverkskomponenter). Noen steder fører bruk av hyllevareløsninger også til et stort forbruk av utstyr og programvare, der man stadig og gradvis går over til nyere arkitektur. Et resultat av dette kan være at det blir vanskeligere å få tak i tilsvarende komponenter og reservedeler eller oppdateringer og støtte til programvare. Alt dette fører igjen til at det blir vanskelig å oppnå en homogen plattform.

Hyllevareløsninger har også som regel mer funksjonalitet enn det som er nødvendig for et gitt systemet, og dette fører ofte til at systemene blir mer komplekse og ressurskrevende enn nødvendig. Generelt vil dette påvirke stabiliteten til systemet negativt og samtidig øke systemets sårbarhet overfor ondsinnede handlinger, og dette gjelder både for programvare og maskinvare (brukermaskiner, servere, nettverkskomponenter, overvåkingsutstyr). Slike ubrukte tjenester blir ofte stående uten oppgraderinger og vedlikehold, og i verste tilfelle står de med standard leverandørsatt passord.

Hyllevareløsninger innebærer også at det generelt finnes mye tilgjengelig kunnskap om sårbarheter i systemene. Potensielt kan en derfor stå overfor flere angripere med riktig kompetanse, og man er mer utsatt for tilfeldig ondsinnet kode. På den andre siden har en normalt også mer kompetanse tilgjengelig for beskyttelse av hyllevareløsninger og de vil også ofte ha mer moderne sikkerhetsløsninger. Dette kan for eksempel være moderne autentiseringsmekanismer, som kan brukes i stedet for å stole på gamle protokoller med klartekstpassord.

Et siste viktig punkt er at det som regel også er enklere å etablere integrerte drift- og overvåkingssystemer når komponentene består av standard hyllevareutstyr.

WAN

Av virksomhetene BAS5 har vært i kontakt med er det få som bruker Internett for å koble sammen geografisk spredte nettverk. I stedet er det utstrakt bruk av leide linjer. Disse er i praksis VPN-tunneler gjennom en nettverktilbyders eget kjernenett. Trafikken gjennom disse blir vanligvis ikke kryptert på tilbyders side, men for sensitiv trafikk legger ofte kunden til kryptert VPN på egenhånd. Flere nettverkstilbydere leverer produkter med garantier for oppetid og kapasitet, noen også med garantert fysisk redundans ende-til-ende. Noen organisasjoner leier mørk (ubrukt) fiber fra nettverkstilbyder – da leies kun den fysiske fiberforbindelsen, og kunden må selv stille med nettverksutstyr og all drift og overvåking av nettverket. Et fåtall større organisasjoner eier egen fysisk nettverksinfrastruktur og drifter denne selv.

Oppringt analogt samband over telefoninettet eller ISDN brukes fortsatt noen steder som reserveløsning. Dette vil som regel ikke være nok til å ivareta normal operasjon, men kan være nyttig for å få utført nødvendige drift- og vedlikeholdsoppgaver.

Når det gjelder oppetid og tjenestekvalitet, viser erfaringene fra BAS5-analysene at det forholdsvis store kvalitetsforskjeller mellom de ulike nettverkstilbyderne.

Annen teknologi

PKI

Ingen av casesystemene brukte større integrerte PKI-løsninger. PKI brukes derimot ofte i separate applikasjoner som ikke er integrert med resten av organisasjonens sikkerhetsmekanismer, for eksempel VPN til hjemmekontor osv.

Kryptografi

Utover ulike VPN-system for organisasjonsinterne nettverk, er kryptografisk beskyttelse som for eksempel kryptert og signert e-post eller harddiskkrypto forholdsvis lite i bruk. Sensitiv informasjon sendes dermed i mange tilfeller som ubeskyttet klartekst over Internett og blir ofte lagret i klartekst på bærbare maskiner og lagringsmedia. For informasjon som er beskyttet gjennom annet regelverk enn Sikkerhetsloven er det få eller ingen godkjente mekanismer og standarder for forsendelse over åpne kanaler.

Når det gjelder intern drift og styring av IKT-system er man til en viss grad i ferd med å ta i bruk mer moderne mekanismer for autentisering og autorisasjon, men spesielt i eldre produksjonssystem benyttes fortsatt enkle og forholdsvis usikre mekanismer.

Håndholdte maskiner

Mobiltelefoner og andre håndholdte maskiner er i utstrakt bruk i flere organisasjoner, men de er sjelden tatt inn i organisasjonenes IKT-sikkerhetsregimer. Først og fremst har en i enkelte sammenhenger blitt forholdsvis kritisk avhengig av mobiltelefoner for kommunikasjon, både for normal operasjon og for bruk i forbindelse med feilhåndtering og varsling. Videre tar en også i større grad i bruk enheter med funksjonalitet som vanlige datamaskiner. Dette kan by på flere sikkerhetsrelaterte problemstillinger, spesielt for utstyr som brukes både privat og i organisasjonsdomenet.

Avhengighet av Internett og sektornettverk

Blant de virksomhetene BAS5 har sett på er få direkte avhengige av Internett for kritisk operasjon. Produksjonsnettverkene kan som regel fungere uten tilgang til Internett. Imidlertid blir virksomhetene gradvis avhengig av Internett-tilknytninger for å møte kunder (investorer, pasienter, kraftmeglere osv). I tillegg ser en flere og flere steder at en blir avhengig av at underleverandører og konsulenter kan koble seg til interne system via Internett, for å foreta drift og vedlikehold av spesifikke applikasjoner.

Så godt som ingen produksjonsnettverk er fysisk skilt fra Internett. Dette skyldes som regel behov for å hente sanntids produksjonsdata, for eksempel for å gi kraftmarkedet tilgang til oppdatert status om situasjonen i kraftinfrastrukturen. Det er fortsatt mye perimetertekning her, i den forstand at produksjonssystemer på innsiden av brannmurene ofte består av gammel teknologi som ikke er oppgradert og oppdatert. Feilkonfigurerte eller sårbare nettverkskomponenter, spesielt brannmurer, kan dermed potensielt få meget store konsekvenser.

I stedet for Internett ser en heller utbredelsen av egne datanettverk innenfor de ulike sektorene. Eksempler er SOIL (Secure Oil Information Link) innenfor petroleumsbransjen, FNN (Finansnett Norge) og Nasjonalt Helsenett. Foreløpig varierer størrelse og utbredelsen av disse nettverkene. SOIL har lang tradisjon og stor utbredelse, mens FNN er relativt nytt og har foreløpig få kunder.