Konsekvenser ved samlokalisering av IKT-systemer innen helsesektoren

Eskild Storvik

Masteroppgave
Master i informasjonssikkerhet
30 ECTS
Institutt for informatikk og medieteknikk
Høgskolen i Gjøvik, 2006

Institutt for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Abstract

In modern society, current treatment and management of information is a constant question about security. Raised demand of improving the efficiency of operations, leads frequently to centralization and convergence of unequal systems. A frequently challenge is to fulfil the demand of sufficient security and information security. For example, when information is exchanged in a network, or there are given access to information from different systems. The information itself will have the same security requirements, and because of this, information and security must be managed in a complete and satisfactory way.
The management decide whether the organization have sufficient information security. The management often base such decision on analysis, investigation or exploration. A risk analysis could confirm that the organization fulfil the demands of sufficient security. A risk analysis could also ensure a quality in the project and confirm that the deliverance is in accordance defined by the management. Different kind of factors identified as critical to a project are affecting the choice of methods. The increasing human impact, beside increasing complexity and convergence, often requires knowledge about how to choose the most suitable method. The methods are effective tools for analyzing systems, in order to reduce the likelihood that critical and crucial threats remain unidentified. Which might be achieved by choosing the most effective and suitable method for the project and the organization. For example qualitative methods lack the ability to account the dependencies between events, but are effective in identifying potential hazards and failures within the system, whereas tree-based techniques take into consideration the dependencies between events.

This thesis describes the use of two different methods for analyzing a health-care organization. The two chosen methods are, the quick and easy method «NSM-ROS2004», and the heavier and more extensive method «FTA». The thesis carries out an experiment by using FTA as a method within information security. Both methods are used to uncover the consequences of centralizing critical ICT-systems. The thesis also discuss the benefit of choosing a quick and easy method, instead of an extensive one, the theses will also analysis the result in each method, to disclose in which degree there are subjective or objective parts in the results. A greater subjective part might lead to deceptive conclusions.

Another contribution is to describe the procedure of performing a risk analysis. There is a relative small number of detailed documentation about how to choose a method, employ a method and perform a risk analyse. The whole process and the results are often kept confidential within an organization or consultant firm. The theses give a description on how to choose, perform and analyse the results.

Sammendrag

I dagens samfunnsutvikling er riktig behandling og ivaretakelse av informasjon, et konstant spørsmål om sikkerhet. Økte krav til effektivisering leder ofte til sentralisering og konvergens av parallelle utviklingsløp. Samtidig er det en økende tendens til at ulike informasjonssystemer kobles sammen og tilknyttes Internett. Dette medfører større krav til informasjonstilgjengelighet og nye kommunikasjonsformer. På den andre siden medfører slike krav økt kompleksitet og større angrepsflate. En stadig utfordring er å sikre tilstrekkelig ivaretakelse av informasjonssikkerhet. Når data skal utveksles i et nettverk, eller det skal gis tilgang til data fra forskjellige systemer, vil forskjellige aktører ha forskjellige krav til sikkerhet, mens dataene vil ha de samme behovene for sikkerhet.

Ledelsen i virksomheten er ofte de som avgjør og fastslår hvorvidt virksomheten har tilstrekkelig informasjonssikkerhet. Ledelsen tar ofte sine beslutninger basert på undersøkelser, vurderinger og analyser. En risiko- og sårbarhetsanalyse kan være et hjelpemiddel for å avgjøre om virksomheten har tilstrekkelig sikkerhet og informasjonssikkerhet. En risiko- og sårbarhetsanalyse kan også bidra til å hjelpe prosjektdeltakerne i å sikre kvalitet i prosjektet, og bidra til at den endelige leveransen er i samsvar med krav og målsetting definert av ledelsen. Masteroppgaven benytter metodene NSM-ROS2004 og FTA for å avdekke konsekvenser ved sentralisering av kritiske IKT-systemer innen helsesektoren. Samtidig forsøker oppgaven å besvare hvilken grad av objektivitet eller subjektivitet som ligger i resultatene. Det kan være en tendens til at kvalitative metoder har et preg av personlige vurderinger og personlig empiri, noe som kan medføre misvisende sluttresultater. Masteroppgaven inneholder også et eksperiment ved å benytte FTA som metode innen informasjonssikkerhet. FTA metoden er benyttet i både kvalitativ og kvantitativ tilnærming. Eksperimentet viser at FTA i en kvantitativ tilnærming kan bidra til en mindre grad av subjektivitet i resultatet. Masteroppgaven drøfter også fordeler og ulemper ved en enkel og lett metode, i forhold til en mer omfattende og ressurskrevende metode.

I tillegg er et av rapportens bidrag å gi en beskrivelse og fremgangsmåte for hvordan en risiko- og sårbarhetsanalyse kan gjennomføres. Dette gjøres ved å være prosessorientert i beskrivelsene av fremgangsmåte, og således beskrives begge risiko- og sårbarhetsanalysene detaljert. Det eksisterer relativt lite offentlig tilgjengelig dokumentasjon som beskriver en detaljert fremgangsmåte og bruk av ROS-metoder. Ofte holdes hele ROS-analysen og prosessen konfidensiell innenfor en virksomhet, organisasjon eller konsulentfirma. Rapporten gir således også en kort oppsummering over ulike typer metoder som kan benyttes i forskjellige typer risiko- og sårbarhetsanalyser.

Forord

Denne masteroppgaven er en avsluttende del av min Masterutdannelse ved Høgskolen i Gjøvik. Masterutdannelsen er gjennomført i tidsperioden høsten 2004 til våren 2006. Utdannelsen ved HiG har gitt meg et bredt spekter og solide kunnskaper innen fagområdene IKT-sikkerhet og informasjonssikkerhet.

Ved siden av stor interesse i selve oppgaven, har valget også vært basert på å kunne benytte så mye av de tilegnede teorikunnskapene i praksis. Samtidig å kunne få erfaring i hvordan sikkerhetsarbeid faktisk utføres. Formålet med oppgaven er å identifisere konsekvenser ved samlokalisering av IKT-funksjoner på et regionalt nivå. Problemstillingen og utfordringene som identifiseres er høyst relevant for andre sektorer, virksomheter og organisasjoner som er i samme situasjon. I løpet av perioden jeg har arbeidet med oppgaven, har prosjektet blitt kjent for flere kjente aktører innen helsesektoren og fagområdet risiko- og sårbarhetsanalyse.

En takk rettes til medstudenter, informasjonssikkerhetsmiljøet ved HiG og NTNU/Sintef, Janne Hagen ved FFI og Abie Habtamu ved Norsk Regnesentral for bidrag til oppgaven. Dere alle har gitt verdifulle innspill gjennom samtaler, diskusjoner, forslag og skriftlig korrespondanse.

En stor takk rettes til Håvard Fridheim ved FFI for rådgivning og anbefalning innen risiko- og sårbarhetsanalyse. Videre vil jeg også rette en spesiell takk til veileder Nils Kalstad Svendsen som har bidratt med uvurderlig og konstruktiv veiledning gjennom hele prosjektperioden.

Tusen takk!

> Anything that can go wrong will go wrong.
>
> — *Murphy's Law*

> If you perceive that there are four possible ways in which a procedure can go wrong, and circumvent these, then a fifth way, unprepared for, will promptly develop.
>
> — *Murphy's Law*

Eskild Storvik, 2006/06/01

Innhold

Abstract . . . . . **iii**
Sammendrag . . . . . **v**
Forord . . . . . **vii**
Innhold . . . . . **ix**
Figurer . . . . . **xiii**
Tabeller . . . . . **xv**
1 Innledning **1**
1.1 Nøkkelord 1
1.2 Tema oppgaven dekker 1
1.3 Problembeskrivelse 1
1.4 Motivasjon 2
1.5 Forskningsspørsmål 2
1.5.1 Metode 3
1.5.2 Generelt 3
1.6 Begrensninger 3
1.7 Beskrivelse av disposisjon 4
1.8 Konfidensielt 4
2 Valg av fremgangsmåte **5**
2.1 Forskningsstrategi 5
2.2 Pålitelighet og gyldighet 6
3 Tidligere og relevant arbeid **7**
3.1 IKT og Organisasjon 7
3.2 Beskrivelse av sikkerhet 7
3.2.1 Definisjon av sikkerhet og begreper innen sikkerhet 9
3.3 Sikkerhet og kommunikasjon 9
3.3.1 Generellt om sikkerhet og kommunikasjon 9
3.3.2 Sikkerhet og kommunikasjon for helsesektoren 10
3.4 Risiko 11
3.4.1 Definisjon 11
3.4.2 Risikovurdering 12
3.4.3 Risikovurdering og usikkerhet 13
3.5 Metode og ROS-analyse 14
3.5.1 Om metode 14
3.5.2 Risikoanalyser og Sårbarhetsanalyser 15
3.5.3 Klassifisering av metode 15
3.5.4 Valg av metode 16
3.6 Arkitektur og infrastruktur 17
3.6.1 Infrastruktur 17
3.6.2 Sentralisering eller desentralisering 18
3.7 Modellering og modelleringsspråk 20

4 Beskrivelse av dagens organisasjon og struktur . . . 23
4.1 Hvordan dagens system fungerer . . . 23
4.1.1 Eksisterende infrastruktur innen Helsesektoren . . . 24
4.1.2 Dagens EPJ og system status . . . 24
4.2 Beskrivelse av helseforetaket . . . 25
4.2.1 Server-Klient løsninger . . . 25
4.3 Lovverk/regelverk for helsesektoren . . . 26
4.3.1 Forskjell på helsesektor og annen sektor . . . 27
5 Metoder for ROS-analyse . . . 29
5.1 Metoder . . . 29
5.2 Valg av metoder for ROS-analyse . . . 31
5.2.1 Første ROS-analyse . . . 31
5.2.2 Andre ROS-analyse . . . 32
6 Eksperimentet . . . 35
6.1 Definering av analyse og omfang . . . 35
6.2 Gjennomføring av første ROS-analyse . . . 35
6.2.1 Metoden NSM-ROS2004 . . . 35
6.2.2 Planlegging og organisering . . . 36
6.2.3 Identifikasjon av verdier . . . 37
6.2.4 Identifikasjon av trusler . . . 38
6.2.5 Modellering . . . 38
6.2.6 Hvordan ROS-møtet ble gjennomført . . . 39
6.2.7 ROS-samlingen . . . 39
6.2.8 Etter ROS-samlingen . . . 40
6.3 Gjennomføring av andre ROS-analyse . . . 42
6.4 Beskrivelse av metoden FTA . . . 42
6.4.1 Konstruksjon av feiltrær . . . 42
6.4.2 Analyse av konstruert feiltre, kvalitativ eller kvantitativ . . . 42
6.5 Hvordan har vi benyttet FTA som metode . . . 43
6.6 Innledning . . . 43
6.7 Identifikasjon og kategorisering av feilkilder . . . 44
6.7.1 Vår kategorisering av feilkilder . . . 44
6.8 Beskrivelse av konstruerte feiltrær . . . 45
6.8.1 Gjennomføring av ROS-møte . . . 46
6.8.2 Konvertering av feiltrær til pålitelighetsnettverk . . . 47
6.8.3 Strukturer i feiltrær og konvertering til pålitelighetsnettverk . . . 47
6.9 Teori for å finne pålitelighet i et system . . . 48
6.9.1 Uavhengige hendelser . . . 49
6.9.2 Et beskrivende eksempel . . . 49
6.9.3 Analyse av feiltre . . . 51
6.9.4 Pålitelighetsmessig betydning . . . 53
6.9.5 Eksempel på pålitelighetsmessig betydning . . . 53
6.9.6 Et eksempel på Birnbaums pålitelighetsmessige mål . . . 54
6.10 Et eksempel på analyse av et fremtidig system . . . 59
7 Analyse av resultat og gjennomføring . . . 63
7.1 Erfaringer ved arbeidet som er gjennomført . . . 63

7.2 Kort diskusjon av resultatene . . . 63
7.2.1 Om den kvantitative beskrivelsen . . . 63
7.3 Resultater og erfaringer ved å velge NSM-ROS2004 . . . 64
7.4 Resultater og erfaringer ved å velge FTA . . . 65
7.4.1 Kort om valg av topphendelse . . . 67
7.4.2 Birnbaums mål . . . 67
7.5 Drøfting av metodene . . . 67
7.5.1 Argumentasjon for å benytte FTA innen informasjonsikkerhet . . . 68
7.6 Drøfting av verdier ved tyngre og lett metode og et helhetlig rammeverk . 69
7.6.1 Sikkerhet og sikkerhetspersonell . . . 70
8 Oppsummering og konklusjon . . . 71
8.1 Kunnskapsbidrag . . . 71
8.2 Oppsummerende diskusjon av resultat og oppnådd mål . . . 72
8.3 Besvaring av forskningsspørsmål . . . 72
8.3.1 Konklusjoner ved metodene . . . 72
8.3.2 Subjektivitet og objektivitet i metodene . . . 73
8.3.3 Lettere eller tyngre metode, eller helhetlig rammeverk . . . 74
8.3.4 Konklusjoner ved samlokalisering av IKT-systemer . . . 75
9 Videre arbeid . . . 77
9.1 Evaluering av metodene . . . 77
9.1.1 FTA og informasjonssikkerhet . . . 77
9.1.2 Kost/nytte vurderinger . . . 78
9.2 Konsekvenser ved samlokalisering av IKT-systemer . . . 78
Bibliografi . . . 81
A Lovverk . . . 87
A.1 Personopplysningsloven og forskrift til personopplysningsloven . . . 87
A.2 Helseregisterloven . . . 90
A.3 Helsepersonellloven . . . 91
A.4 Pasientrettighetsloven . . . 92
A.5 Helseforetaksloven . . . 92
A.6 Journalforskriften . . . 92
A.7 Informasjonssikkerhet i helsesektoren . . . 93
A.8 Lov om arkivering (arkivloven) . . . 93
B Appendix . . . 95
C Appendix . . . 111
D Appendix . . . 115
E Appendix . . . 119
F Appendix . . . 121
G Appendix . . . 123

Figurer

1 Forskningsstrategi 6
2 Beskrivelse av sikkerhet. Hentet fra «Security in computing» av Pfleeger. . 8
3 Beskrivelse av Risiko. Hentet fra «Defence-in-depth» av Robichaux og Bass. 11
4 Skissering av forskjellige syn på risiko. Hentet fra [1] av Kuamoto og Henley. 12
5 Skisse av presentert rammeverk. Hentet fra «Methods for risk and vulnerability assessments of infrastructures depending on ICT» av Wiencke m.fl. 17
6 Viser utvikling som har påvirket sentralisering og desentraliseing av applikasjonsprogramvare (Hentet fra Schuff og Louis [2]). 19
7 Viser det presenterte rammeverket(Hentet fra Schuff og Louis [2]). 19
8 Hvordan systemet ser ut i dag. 23
9 Skisse av et mulig fremtidig system. 24
10 Styringssløyfe hentet fra «NSM-ROS2004». 36
11 Oppdeling av systemet. 39
12 Fremgangsmåte beskrevet i NSM-ROS2004 [3]. 40
13 Skisse av risikomatrise for vurdering av konsekvens og sannsynlighet. . . . 41
14 FTA-komponenter. 43
15 Inndeling av soner. Inspirert av Moberg [4]. 46
16 Beskrivelse av feiltre konstruksjon. 46
17 Skisse av feiltre som gir en serie-struktur ved konvertering til pålitelighetsnettverk. 47
18 Skisse av feiltre som gir en parallell-struktur ved konvertering til pålitelighetsnettverk. 47
19 Skisse av feiltre som gir en k-av-n-struktur ved konvertering til pålitelighetsnettverk. 47
20 Feiltre av et tenkt system. 50
21 Pålitelighetsnettverk av feiltreet presentert i figur 20. 50
22 Fremgangsmåte for nedbryting av presentert system, for å finne minimale kuttmengder. 50
23 Viser fremgangsmåte for å finne minimale kuttmengder i systemet. 50
24 k-av-n-struktur ved inndeling av pålitelighetsnettverket i figur 21(X_I). . . 51
25 Serie-struktur ved inndeling av pålitelighetsnettverket i figur 21(X_{II}). . . . 51
26 Parallell-struktur ved inndeling av pålitelighetsnettverket i figur 21(X_{III}). 51
27 Viser pålitelighetsnettverket i et system. 56
28 Pålitelighetsnettverk for et fremtidig system. 60
29 Skissen viser et eksempel på dobbeltlagring av rater. 65
30 Skisse av kunnskapsbidrag. 71
31 Skisse av feiltre. 119
32 Skisse av feiltre. 120
33 Skisse av et revidert feiltre. 121
34 Skisse av revidert feiltre. 122

Tabeller

1 Illustrerer kategorisering verktøyer i forhold til bruksområdet. Hentet fra «Methods for risk and vulnerability assessments of infrastructures depending on ICT» av Wiencke, Aven m.fl. 16
2 Oversikt over pålitelighet i komponentene i systemet. 52
3 Oversikt over pålitelighet i komponentene i systemet med endringer av verdier for $x_7, x_8, x_9 x_{10}$ og x_{11}. Lavere verdi i kategorien «feilrate», vil bety høyere pålitelighet for komponenten i en tidsperiode t_0. 55
4 Oversikt over pålitelighet i komponentene i systemet. Lavere verdi i kategorien «feilrate», vil bety høyere pålitelighet for komponenten. Tallet beskriver pålitelighet over en gitt tidsperiode t_0. (I tabellen brukes «Birn.» som er forkortelse av «Birnbaums mål» og «F.rate» som betyr «feilrate»). . 57
5 Oversikt over pålitelighet i komponentene i systemet. Et sikkerhetstiltak har redusert feilratene for komponentene x_1 og x_2, og krevd innføring av komponenten x_{16}. Lavere verdi i kategorien «feilrate», betyr høyere pålitelighet for komponenten i en tidsperiode t_0. 61
6 Oversikt over loververk. 94
7 Illustrerer kategorisering av trusler og risiko innenfor konfidensialitet. . . 116
8 Illustrerer kategorisering av trusler og risiko innenfor kvalitet. 116
9 Illustrerer kategorisering av trusler og risiko innenfor integrietet. 116
10 Illustrerer kategorisering av trusler og risiko innenfor tilgjengelighet. . . . 117

1 Innledning

I dagens samfunn er trygg og sikker forvaltning av sensitiv informasjon helt avgjørende for de fleste bedrifter og virksomheter. Mange bedrifter og virksomheter behandler og lagrer informasjon av høy sensitiv karakter. Samtidig utvikles det stadig nye og kraftigere verktøy for å innhente, behandle og utveksle informasjon. Resultatet er en økende tendens til at moderne informasjonsteknologi tas i bruk på stadig nye områder. Dette medfører at trygg og sikker forvaltning av informasjon blir stadig viktigere for virksomhetene. Effektivisering resulterer ofte i endringer i virksomhetens infrastruktur og arkitektur. En løsning er å sentralisere systemer. En sentralisering medfører ofte større og viktigere knutepunkter som kan gir større potensial for svikt og dermed større risko.

1.1 Nøkkelord

Risiko- og sårbarhetsanalyse, FTA, NSM ROS2004, IKT-infrastruktur, informasjonssikkerhet, sentralisering, desentralisering.

1.2 Tema oppgaven dekker

Valg av metode for en risiko- og sårbarhetsanalyse(ROS-analyse) er ofte basert på flere forskjellige faktorer som påvirker prosjektet. Noen slike faktorer kan være: ulike sikkerhetsaspekter, problemstilling, ressurser, tid eller juridiske begrensninger osv. Hvor egnet den valgte metoden er, er ofte avgjørende for resultatet i prosjektet. Masteroppgaven tar utgangspunkt i et case ved et helseforetak, hvor ulike informasjonssikkerhetsperspektiver er sentrale elementer, og har med støtte fra FFI identifisert to metoder for gjennomføring av ROS-analyse. Metodene benyttes på et helseforetak for å beskrive konsekvenser ved å samlokalisere systemer på regionalt nivå. Masteroppgaven gir svar på hvilke resultater som foreligger etter en ROS-analyse, og hvilken grad av objektivitet eller subjektivitet som ligger i resultatene.

1.3 Problembeskrivelse

Sentralisering av IKT-systemer er ofte et resultat av effektivisering i en bedrift eller virksomhet. For eksempel har etableringen av Regionale Helseforetak (RHF) og sammenslåing av sykehus til større helseforetak, medført at IKT-funksjoner som lagring og behandling av pasientdata samlokaliseres. Innen helsesektoren er det et økende behov for å utveksle sensitiv og konfidensiell informasjon som følge av moderne pasientbehandling. Fortløpende tilgang til informasjon er en nødvendighet og en forutsetning, for korrekt og effektiv pasientbehandling. For å oppfylle kravene som stilles, er det behov for sikkerhetsmekanismer som sikrer tilgjengelighet, overføring og lagring av opplysningene under etterlevelse av et omfattende regelverk [5]. Samtidig skapes det sentrale problemområder som bør utredes ved en samlokalisering. Påvirkende faktorer identifisert på forhånd, vil ofte være utslagsgivende i valg av metode. Ofte vil valg av metode og sammensetningen av kompetanse i prosjektgruppa være avgjørende for sluttresultatet. PricewaterhouseCoopers [6] beskriver at et av formålene med en metode er at «metoden skal gi ledelsen kunnskap om virksomhetens risikoeksponering ved sikkerhetsbrudd». Det

påpekes også at det bør gjennomføres risikoanalyser for å kartlegge skadevirkninger ved frafall av kritiske virksomhetsprosesser. Vi gjennomfører et eksperiment ved å benytte oss av to forskjellige metoder for ROS-analyse på et case, for så å evaluere hvilket resultat som foreligger etter endt analyse. Samtidig analyserer vi hvilken grad av subjektivitet eller objektivitet som ligger i resultatet. Ledelsen tar ofte beslutninger på bakgrunn av resultatet i analysen, og om resultatet i analysen ikke er godt nok, er verdien av å gjennomføre en ROS-analyse ofte verdiløs[1].

1.4 Motivasjon

Økonomisk innsparing og økt effektivitet er sentrale begreper for å beskrive dagens samfunnsutvikling innen bedrifter, virksomheter og organisasjoner. De siste årene har vi sett en tendens til økt konvergens av parallelle løp innen IKT [7]. Sentralisering og samlokalisering av ulike systemer og applikasjoner er elementer som er bidrar til konvergens. Vår motivasjonen ligger i å benytte to metoder for å analysere konsekvenser ved endring av infrastruktur innen helsesektoren. Dagens system innen helsesektoren er karakterisert som tungvint og vanskelig. Resultatet av analysene vil kunne gi svar eller indikatorer på konsekvenser, risiko og sårbarheter ved samlokalisering av IKT-systemer. En overgang til IKT-løsninger fra papirbaserte systemer, innebærer økt sårbarhet for en eller flere trusler, men også redusert sårbarhet på enkeltområder. Samtidig ligger det et potensial for betydelig effektivisering av virksomhetene [8].
Fra et medisinskfaglig synspunkt vil pasientbehandlingen kunne bedres og effektiviseres dersom all informasjon gjøres tilgjengelig til riktig tid der pasienten behandles. Korrekt og forsvarlig pasientbehandling avhenger av at alle nødvendige opplysninger foreligger for behandlende lege, og ofte er de mest sensitive opplysningene av størst betydning. På den andre siden skal en respektere pasientens rettmessige krav, og av hensyn til personvernet skal ikke opplysningene gjøres tilgjengelig for utenforstående parter eller personer. Dette reiser både tekniske og juridiske utfordringer når det gjelder å finne frem til hensiktsmessige løsninger for å kunne yte pasientene optimal og effektiv behandling [5].

1.5 Forskningsspørsmål

Forskningsspørsmålene deles inn i to deler, en del som omfatter «Metode» og en del som omfatter «Generelt». «Generelt» vil beskrive konsekvenser ved samlokalisering av IKT-systemer. Et helseforetak har stilt sine systemer og maskinpark til disposisjon for case studie. Vi anser det som praktisk å dele inn forskningsarbeidet i tre moduler. En modul med studie og modellering av case (helseforetaket). En modul som omfatter valg, begrunnelse og bruk av metodene. Denne modulen er beskrevet i kapitel 5 og bruk av metodene beskrives utover i kapitel 6. Tilslutt en modul med evaluering av metodene og besvaring av forskningsspørsmålene. Denne modulen beskrives i kapitel 7 og 8. Følgende beskrives forskningsspørsmålene vi ønsker å besvare:

[1] Møte med Janne Hagen, 13.01.2006

1.5.1 Metode

Denne delen vil i hovedsak omfatte et studie av helseforetaket og valg av metode basert på tid, ressurser og begrensninger i analysen. Det ble i samarbeid med FFI identifisert to metoder for ROS-analyse på aktuelt case. Etter endt prosjekt ble det gjennomført en evaluering av de valgte metodene. Denne vil senere også bli benyttet i FFI's BAS5 prosjekt.

- I hvilken grad er resultatet preget av objektivitet og subjektivitet, personlige erfaringer og vurderinger?
- Er det verdt bryet å benytte en tyngre og mer omfattende metode, fremfor en lettere og mindre omfattende?
- Hvordan fungerte metodene med våre ressurser, problemstilling, kriterier og tidsbegrensning?

1.5.2 Generelt

Under dette punktet ønsker vi å få svar på:

- Hvilke gevinster eller konsekvenser ligger det i å samlokalisere IKT-systemer
- Hvilke sikkerhetsfaktorer blir påvirket og fremkommer det nye sårbarheter ved en reorganisering av IKT-infrastruktur

For å kunne gjennomføre ROS-analysen, ser vi det som praktisk å modellere systemet. Arbeidet vil hovedsaklig omfatte et studie av det eksisterende systemet og et fremtidig system. Det er i denne fasen nødvendig å etablerer forståelse og kunnskap vedrørende funksjonalitet til systemene, både ved det eksisterende systemet og det fremtidige systemet. En modell er konstruert på bakgrunn av løsninger og begrensninger ved helseforetaket. Samtidig er det under denne fasen nødvendig å studere spørsmål som «Hva er dagens struktur og hva utveksles av informasjon, format på informasjon og i hvilken grad, størrelse, type osv».

1.6 Begrensninger

Problemstillingen er gyldig og relevant for enhver organisasjon som utfører både ROS-analyse og omorganisering av IKT-infrastruktur. Vi vil primært begrense oss til identifikasjon av konsekvenser ved samlokalisering av IKT-systemer innen helsesektoren. For å gjøre oppgaven håndterbar og begrense omfanget av undersøkelsene, ser vi oss nødt til å konsentrere oss om en virksomhet, og deretter forsøke å generallisere resultatet. Nivået av sikkerhet varierer for ulike systemer, bruksområder og den virksomhet/avdeling som eier dem. For å begrense arbeidet i oppgaven velger vi å benytte akseptkriterier som virksomheten har definert for vurdering av risiko og sårbarhet. Akseptkriteriene er også blitt benyttet til vurdering av eksisterende sikkerhetskrav og sikkerhetsbehov innen helseforetaket.
Videre har vi har valgt å legge oss på et nivå mellom teknologisk og organisatorisk på grunn av begrensninger i tid og ressurser. Et nivå nærmere organisatorisk vil falle utenfor vårt fagområde, og hva oppgaven vil tilføre informasjonssikkerhet. Et nivå nærmere det teknologiske, vil føre til at oppgaven blir for ambisiøs og omfattende, og ofte resultere i «enten/eller»-resultater. Vi har også definert egne kriterier for ressurser, kompetanse og økonomi i samarbeid med helseforetaket, for å kunne gjøre et egnet valg av metode.

1.7 Beskrivelse av disposisjon

Rapporten er delt inn i følgende kapitler. Innledningsvis beskrives problem og problemstilling. Kapittel to beskriver valg av forskningsstrategi som vi velger å benytte for å besvare problemstilling, og begrunnelse for metode for innsamling av informasjon osv. Kapitel tre beskriver relevant arbeid som vi velger å bygge videre på. I kapitel fire beskrives studert helseforetak i generallisert form, som vi har benyttet som case for ROS-analysene. Kapitel fem beskriver metode og valg av metode for ROS-analyse. Kapitel seks og sju beskriver henholdsvis eksperimentet og resultatene av eksperimentet, og kapitel åtte beskriver oppsummering og konklusjoner ved ekseperimentet. Avslutningsvis beskriver kapitel ni videre arbeid.

1.8 Konfidensielt

Under prosjektet har det blitt dokumentert og utarbeidet rapporter for alle prosessene. Disse rapportene er ikke vedlagt i masteroppgaven av konfidensielle hensyn til helseforetak. Rapportene har ikke betydning resultatet som beskrives i rapporten, eller for evaluering av metoden. Disse rapportene er kun beskrivelse av tekniske løsninger, begrensinger, feilkilder, sårbarheter og risiko ved studert helseforetak, og kun er relevant og interessant for IKT-avdelingen ved helseforetaket.

2 Valg av fremgangsmåte

I dette kapitlet drøftes og begrunnes valg for forskningsstrategi for oppgaven.

2.1 Forskningsstrategi

Rapportens forskningsstrategi inkluderer metode for ROS-analyse, valg av metode for gjennomføring av prosjektet, innsamling av informasjon, analyse og vurderinger av erfaringer og sluttresultat. Leedy og Ormord [9] identifiserer to hovedtilnærminger, kvalitativ og kvantitativ tilnærming, og en mulighet for kombinasjon av de to.

En kvantitativ tilnærming benytter primært postpositivisme for å utvikle kunnskap [9]. Dette betyr en tenking som omfatter årsak og effekt, og som benytter måling og observasjon, samt testing av hypoteser og teori. Data samles inn på forutbestemte instrumenter som krever statistiske data. Denne tilnærmingen er også kjent for å gå i bredden, til motsetning til kvalitativ tilnærming som går i dybden.

En kvalitativ tilnærming bygger kunnskap konstruktivt (sosialt, historiske konstruerte meninger, med en hensikt å bygge en teori eller et mønster) og/eller ved et deltakende perspektiv [9]. Kvalitativ metode har til hensikt å fange opp mening og opplevelse som ikke lar seg tallfeste eller måle. Kvalitative tilnærming har som formål å få frem sammenheng og helhet. Ved å benytte en kombinasjon av tilnærmingene, hevdes kunnskap å bli basert på et pragmatisk grunnlag. Foreksempel konsekvensorientert eller problemsentrert. Både nummeriske data og tekstlig informasjon samles inn og behandles slik at både kvantitativ og kvalitativ informasjon er benyttet.

Ved valg av forskningsstrategi er det naturlig å se på hvilken tilnærming som er best egnet til å belyse problemstillingen som er beskrevet. Når det gjelder prosjektets hovedtilnærming er det valgt å benytte kvalitative og kvantitative metoder for ROS-analyse, først og fremst på grunn av at det ikke fins bare ett fasitsvar på problemstillingen. Det beskrives i [10] at «det er svært vanskelig å basere seg på utelukkende kvantitative tilnærminger for hendelser der mennesker er involvert» og de metodene som er funnet relevante for ROS-analyse, er utviklet for å være både kvalitative og kvantitative verktøy [11, 3, 10]. Videre beskrives det at «Konsekvens angis kvalitativt som en beskrivelse av de følger en hendelse kan få», men samtidig «vil det være nødvendig å angi konsekvens som en kvantitativ størrelse» [3]. Den kvantitative angivelsen av konsekvens er et middel for å synliggjøre og oppsummere resultater fra risikovurderingen, og for så å kunne sammenligne vurderinger fra forskjellige hendelser.

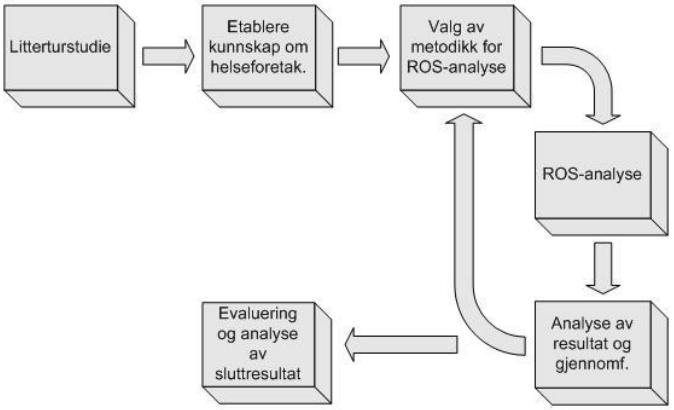
Vurdering av sannsynlighet for at en hendelse inntreffer har som mål å finne svar på spørsmålet «hvor ofte...?». I NSM-ROS2004 [3] beskrives dette ved «at svaret må angis kvalitativt som beskrivelse av hyppighet». For konsekvensvurderinger er det nødvendig å kunne representere graden av sannsynlighet kvantitativt.

Ved gjennomføring av ROS-analysene mener vi det vil være relevant og nødvendig å ha etablert tilstrekkelig kunnskap om forskjellige metoder, systemet, IKT-infrastruktur og virksomheten/organisasjonen. Derfor har det i forskningsstrategien inngått et bredt studie av utvalgt dokumentasjon på: krav til systemene, gjeldende sektor og organisasjonens informasjonssikkerhet, kravspesifikasjoner, system- og applikasjonsbeskrivelser,

og satt disse elementene i sammenheng med standarder og ulike anbefalinger for håndtering av informasjonssikkerhet. Bakgrunnen for denne sammensetningen er å kunne danne et helhetlig risiko- og trusselbilde. Samtidig beskrives det at «Risikobildet vil samtidig være dynamisk, og hendelser som anses som uviktige kan senere bli viktige» [3], vi velger å tolke dette dit hen at en ROS-analyse krever innsikt i hvordan de ulike systemene er relatert til hverandre, og hvordan de påvirker hverandre på tvers av nivåer og på tvers av systemer. En logisk sammensetning av litteraturmaterialet er nødvendig for å dekke kunnskapsbehovet som prosjektet tar for seg. Samtidig bør materialet representere en tverrfaglighet hvor både juss, sikkerhetsfaglig, type av metode og teknologi er tatt med i betraktning og beskriver sine premisser. Det vil også være vesentlig at man benytter et helhetlig syn på de ulike systemene som tilslutt vil gi et dekkende og en komplett karakteristikk av systemet. Det ansees også som nødvendig med enkle «beskrivelser/intervjuer» for å oppnå en utfyllende og fullstendig informasjon om praksis, erfaringer og funksjonalitet til systemene og organisasjonen. Dette vil kunne være en supplerende del og gi viktig informasjon om de valg som er foretatt ved implementering eller utvikling av eksisterende system. Dette er også gjort med tanke på begrunnelse av teknologiske begrensninger eller gevinster, og/eller andre relevante faktorer som foreksempel økonomi. Figur 1 viser forskningsstrategi. «Valg av metode for ROS-analyse»,«ROS-analyse» og «Analyse av resultat og gjennomføring» gjennomføres i to omganger.

2.2 Pålitelighet og gyldighet

I alle typer forskning vil det være relevant å vurdere om sluttresultatet som foreligger har validitet og er reliabelt. I Leedy og Ormod [9] defineres begrepene validitet og reliabilitet til gyldighet eller relevans, og pålitelighet. I den type forskning, som vi tar utgangspunkt i, blir gjerne reliabilitet sammenfallende med validitet og kan derfor vanskelig studeres separat [9]. Vi vil forsøke å oppnå validitet og relevans gjennom bruk av et bredt teoretisk grunnlag satt sammen av flere relevante og valide kilder, samt bygge på forskning som er allerede gjort innen denne sektoren. Samtidig vil det være nødvendig å oppsøke miljøer som har relevant faglig kompetanse på de områdene som oppfattes som utfordrende. På denne måten ønsker vi å danne et relevant, gyldig og pålitelig sluttresultat.



Figur 1: Forskningsstrategi

3 Tidligere og relevant arbeid

Dette kapitlet beskriver tidligere arbeid som vi velger å bygge videre på.

3.1 IKT og Organisasjon

Dagens teknologi gir mulighet for effektivisering og fleksibilitet i arbeidsprosessene. Men for å gi økonomiske gevinster, kreves det ofte en sentralisert tilnærming [12]. Det kan være hensiktsmessig å tenke helhetlig og fokusere på felles løsninger og felles arbeidsrutiner. Bergum [12] beskriver IKT som «elektroniske hjelpemidler for innsamling, bearbeiding, analyse, overføring, lagring og/eller presentasjon av informasjon, for å styre og kontrollere utstyr og arbeidsprosesser, og koble sammen mennesker, funksjoner og ulike enheter både i og mellom organisasjoner». Det beskrives videre at «IKT gir muligheter til å kommunisere bedre og raskere, produsere bedre og raskere, og transportere bedre og raskere». Utviklingen innen IKT påvirker stadig flere oppgaver og områder innen en virksomhet, alt fra innkjøp, lagerstyring, produksjon, distribusjon og til markedsføring, og ikke minst kommunikasjon med kunder, brukere og leverandører.
Limoncelli [13] beskriver oppbygning av organisasjonsstrukturen som en påvirkende faktor for hvordan organisasjonen organiserer sin kommunikasjon med ulike avdelinger. Bergum påpeker også at organisasjoner og medarbeidere har, etter den utviklingen som er skjedd de siste årene, har ført til at organisasjoner og virksomheter kan knyttes sammen i felles kommunikasjonsplattformer relativt uavhengig av tid og rom, på tvers av både organisasjonsmessige, regionale og nasjonale grenser. Bergum konkluderer videre med at «det viktigste ved IKT er at IKT har fått en stadig viktigere og mer strategisk betydning i organisasjonen, og IKT brukes i de fleste funksjoner i organisasjonen». Tidligere var IKT mest benyttet for intern rasjonalisering, mens i dag brukes IKT i større grad for å støtte mer ustrukturerte oppgaver og i kommunikasjon med eksterne samarbeidspartnere. Dette medfører at flere faktorer i organisasjonen blir påvirket.
En av de mest kjente modellene som kan sees i sammenheng med effektivisering av organisasjonen, er Leavitts-diamant [14]. Leavitt hevdet at man ikke kunne se dimensjonene mennesker, system, teknologi, struktur og oppgaver, uavhengig av hverandre. Leavitt beskriver at en endring i en av faktorene medfører endringsbehov i de andre faktorene som også må oppfylles, dersom endringen skal være i samsvar med intensjonen.

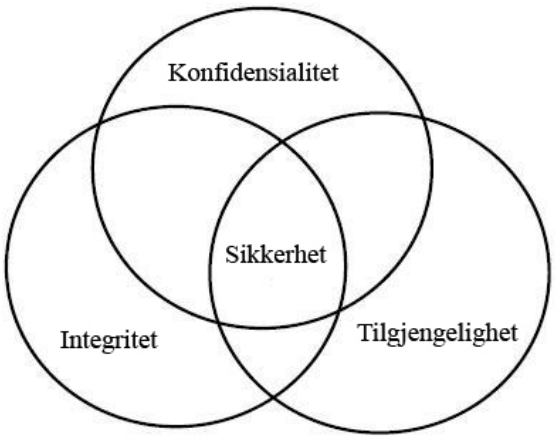
3.2 Beskrivelse av sikkerhet

Krav til sikkerhet finnes i de enkelte virksomheters egne kravspesifikasjoner, sikkerhetspolicyer og gjennom myndighetenes krav i lovverk. Lovverket krever ikke fullstendig spesifikke tiltak implementert, men gir føringer og setter krav for hvordan virksomeheten kan oppnå tilfredsstillende informasjonssikkerhet [15, 16, 17, 18, 19, 20, 21, 22].

Pfleeger [23] beskriver sikkerhet ved oppfyllelse av krav innenfor områdene konfidensialitet, integritet og tilgjengelighet, se figur 2. Det beskrives ofte som vanskelig å finne den rette balansen mellom de tre områdene, fordi informasjonen eller objektet som skal sikres ofte har forskjellige krav til områdene. Dette beskrives for eksempel ved «å sikre

for sterk grad av konfidensialitet til et objekt eller en informasjon, kan det lede til at begrepet tilgjengelighet blir forsømt» [23].

Bakås [24] har i sitt arbeid utført et studie av virksomheter og organisasjoner i Europa som utfører måling av informasjonssikkerhet. Studiet tar for seg hvorfor og hvordan virksomheter utfører måling av informasjonssikkerhet. Bakås gir en oversikt over hvilke metoder som benyttes for måling av informasjonssikkerhetsnivå. Dette kan således gi indikatorer på hvor man finner krav til sikkerhet og videre lede til hva som allment oppfattes ved begrepet «sikkerhet». Begrunnelse for å kunne velge en slik type tilnærming, er at når en skal måle sikkerhet må forstå hva som legges i begrepet sikkerhet og hvor man finner sikkerhet. Flere vil regne overensstemmelse med standarder som foreksempel BS7799 eller ISO/IEC 17799 [25] som en forutsetning for tilfredsstillende sikkerhet og for styring av informasjonssikkerhet i organisasjoner. Ween[26] beskriver at «tradisjonelt retter mange arbeider innen informasjonssikkerhet seg mot et avgrenset system, men omhandler alt i systemet (data, hardware, software og ulike andre fasiliteter ved systemet), og ikke primært mot den informasjonen som flyter i systemet. Informasjonssikkerheten behandles da i et systemperspektiv eller et organisatorisk perspektiv og ikke et datasentrisk, selv om det primært er dataene som har et beskyttelsesbehov». Ween beskriver så videre at «dette gjenspeiles i at en sikkerhetspolicy i hovedsak fokuserer på rutiner, personell og fysisk sikring». En oversikt over hvilken sikkerhet bedriften eller organisasjonen innehar, kan gjøres ved gjennomføring av en risiko- og sårbarhetsanalyse [27]. En risikoanalyse vil normalt gi et bilde av risiko og trusler som virksomheten står overfor. Henriksen [28] beskriver at en risikoanalyse bør skje ved en kvalitativ beskrivelse av sikkerhetssituasjonen, ofte i sammenheng med kvantitative verdier, som for eksempel frekvens eller sannsynlighet. Den kvanititive beskrivelsen kan senere tilordnes til de kvalitative konklusjoner. En risikoanalyse benytter seg ofte av en todimensjonal matrise med akseptverdier for sannsynlighet og konsekvens som uttrykker en samlet risiko. Matrisen kan således gi en representasjon av risikonivået ved en trussel. Dette gjøres ved en total vurdering av de to dimensjonene [27].



Figur 2: Beskrivelse av sikkerhet. Hentet fra «Security in computing» av Pfleeger.

3.2.1 Definisjon av sikkerhet og begreper innen sikkerhet

Fagfeltene «sikkerhet» og «informasjonssikkerhet» benytter flere begreper for å beskrive ulike deler av sikkerhet. Idsø og Jakobsen [29] definerer begrepet informasjonssikkerhet som «forebyggende tiltak som sikrer konfidensialitet, integritet og tilgjengelighet til gradert informasjon gjennom dens levetid». Avizienis, Laprie, Randell [30] beskriver begrepet «availability, reliability, safety, confidensiality, integrity og maintainability» som attributer til begrepet «dependability». Dette er noe som Audestad [7] også beskriver. Det kan ofte være forvirrende med at ulike begreper har overlappende og samme betydning, som foreksempel begrepene «reliability» og «dependability». Sikkerhet blir også ofte delt inn i to grove kategorier, henholdsvis «safety» og «security». Begge begrepene blir benyttet innen fagområdet for sikkerhet og informasjonssikkerhet, og ofte er begrepene benyttet med overlappende betydning. Stølen [31] beskriver et forslag for begge begrepene. Stølen beskriver at det engelske begrepet «safety» er sammenfallende med det norske begrepet «trygghet», og begrepet «security» er sammenfallende med «sikkerhet». Idsø og Jakobsen [29, 27] definerer derimot begrepet «safety» som «sikkerhet mot uønskede hendelser som opptrer som følge av en eller flere tilfeldigheter». Begrepet «security» defineres som «sikkerhet mot uønskede hendelser som er et resultat av overlegg og planlegging».

3.3 Sikkerhet og kommunikasjon

Kommunikasjon kan være et omfattende begrep, og kan være vanskelig å konkretisere og definere [12]. Bergum [12] beskriver at det enkleste kan være å si at formålet med en kommunikasjonsprosess er å overføre informasjon. Bergum beskriver at den informasjonen en organisasjon har behov for, varierer fra en organisasjon til en annen avhengig av beliggenhet i organisasjonsstrukturen, arbeidsoppgaver, omgivelser, styringssystemer, ledelse og teknologiske forhold. Sett i sammenheng med type av informasjon og type av data som skal overføres, vil det innen IKT ofte være et spørsmål om tilstrekkelige sikkerhet. Ween[26] beskriver «Når data skal utveksles i et nettverk, eller det skal gis delt tilgang til data fra forskjellige systemer tilknyttet nettverket, vil de deltagende aktører i forskjellige deler av nettet håndtere og beskrive sikkerhetsspørsmål på forskjellige måter, mens dataene vil ha de samme behov for sikkerhet etter at de er overført eller gjort tilgjengelig i et nytt system». Det er derfor viktig at informasjonssikkerhet og sikkerhet blir ivaretatt i et helhetlig løp [26].

3.3.1 Generellt om sikkerhet og kommunikasjon

Pfleeger [23] presenterer fordeler med å knytte enheter sammen ved kommunikasjon i et nettverks- og sikkerhetsaspekt. Effektivisering av arbeidet krever ofte en tilkoblingen til forskjellige og distribuerte nettverk. Det påpekes flere organisatoriske fordeler, og mindre sikkerhetsfordeler, ved å knytte heterogene nettverk sammen. De positive fordelene er preget av aspekter som: delte ressurser, distribuert «workload», pålitelighet og ekspanderbarhet. Tilmotsetning gir slik tilknytning også nettverket flere og større sårbarheter. De negative sidene som påpekes er blant annet: anonymitet, flere angrepsveier, brukere med tilgang, flere delte enheter, flere forskjellige brukere og brukerkrav, økt kompleksitet og ukjente åpne perimetere. Det beskrives videre at nettverket må tilby integritet, konfidensialitet og sikkerhet for de data som transporteres og behandles. Enhver bruker som

aksesserer et nettverk ved hjelp av en maskin, forventer at maskinen og operativsystemet følger definerte policyer, og at sikkerhet er ivaretatt både i kommunikasjonskanalen, maskinvaren og operativsystemet.

3.3.2 Sikkerhet og kommunikasjon for helsesektoren

KITH [32] beskriver krav til kommunikasjonssikkerhet for EDI-løsninger(EDI-Electronic Data Interchange) innen helsevesenet. De gir anbefalinger vedrørende kvitteringer, loggføring og nøkkelhåndtering. Arbeidet tar for seg konkrete krav rettet mot konfidensialitet, autentisering og meldingsintegritet, og gir samtidig anbefalinger for meldingssikkerhet ved EDI-kommunikasjon. Beskrivelsen av kommunikasjonssikkerhet tilfredsstiller den europeiske standarden «ENV 13608-2: Secure Data Object»(SEC-COM standardserien) som er definert for helsesektoren. SEC-COM serien gir retningslinjer til en rekke kommunikasjonsprotokoller og applikasjoner relevant for helsesektoren, uten å være komplett eller uttømmende. SEC-COM reflekterer en tilnærming drevet av brukerkrav, som er en metode for å analysere sammenhengen mellom brukerkrav og teknologiske løsninger. SEC-COM begynner med en standardisert måte å uttrykke brukerbehov, fortsetter så ved teknologiorienterte suksessive forbedringer av den korresponderende ønskede sikkerhetsløsningen. Metoden ender opp i en standardorientert oversikt over anbefalte sikkerhetsløsninger. En slik metode kan benyttes på flere måter, blant annet som et felles verktøy for nedbryting av brukerkrav til teknologisk løsninger.

Ween [26] foreslår en struktur for å beskrive metadata for sikkerhetskrav. Metadata brukes for å strukturere elementene i sikkerhetskrav, -tjenester, -mekanismer eller -prosedyrer. Dette gjøres ved å benytte en enhetlig formulering og strukturering på en slik måte at sikkerhetskrav fra ulike omgivelser kunne gjøres sammenlignbare. Ween har benyttet en inndeling av sikkerhetskrav etter formaliseringsnivå, spesifikasjonstype og kravtype som er beskrevet i den internasjonale standarden «PrENV 13608:sikkerhet for kommunikasjon i helsenett».

Berglihn og Alsaker [33] identifiserer at dagens EPJ-systemer innholder en for generell aksessrettighet, og at ansvarskravet definert i helsesektoren ikke er oppfylt. Det beskrives at blant annet har doktorer i samme avdeling har tilgang til samme EPJ, selv om det ikke eksisterer noen form for behandlingsrelasjon av pasientene. I lovverket står det beskrevet at leger skal kun ha tilgang til pasientopplysningene om den pasienten som er i en behandlingsrelasjon. Garfurov, Helkala og Svendsen [34] foreslår løsninger på problemet ved bruk av ikke-fornekting og dynamiske aksessrettigheter. Samtidig beskrives det at de lovlige kravene som EPJ er underlagt er svært krevende. De beskriver at en mulig løsning på problemet synes å være PKI(Public Key Infrastrucure). Garfurov, Helkala og Svendsen beskriver også at det kan muligens benyttes en modifisert Bell-La Padula som både identifiserer multinivå sensitivitet og sikkerhetsgradering på informasjonen. Videre foreslåes det også som en mulighet å redusere sårbarheten til systemet ved å ta i bruk Rolle Basert Aksess Kontroll(RBAC).

3.4 Risiko

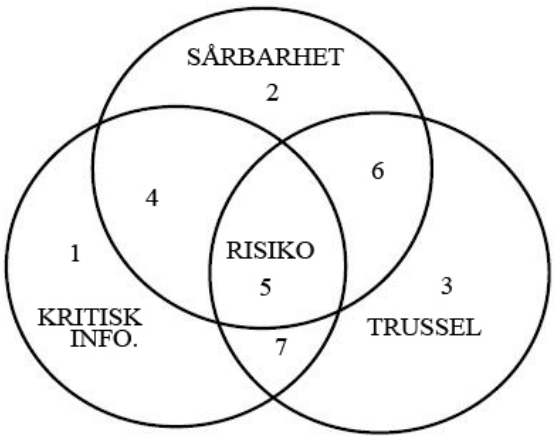
I dette kapitlet beskrives og drøftes risiko, og hvordan risiko vurderes.

3.4.1 Definisjon

Personers oppfattning av risiko er i stor grad individuell og endrer seg gradvis over tid, og fra samfunn til samfunn [23]. Det som kan oppfattes som risikabelt for noen, trenger ikke være risikabelt for andre. Det som ofte er felles, uansett oppfattelse av risiko, er at vi som personer i hverdagen stadig er påvirket av risiko, og gjør ubevisste vurderinger av ulike risikoer. Risiko er ofte definert som en sammensetning av flere faktorer som påvirker hverandre i ulik grad og sammensetning [3][27]. Payne [35] beskriver risiko som en sammensetning av de overordnede elementene verdi, trusler og sårbarhet og at dette kan settes sammen til et totalt risikobilde og der hvor de overlapper hverandre skapes det et risikoområde. Bass og Robichaux [36] beskriver i sitt arbeid at risiko dannes ved sammensetning av trussel, kritisk informasjon og sårbarhet. Det beskrives at arbeidet med risiko er å reduserer alle påvirkende risikofaktorer rundt selve risikoen (del 5. i figur 3) til et akseptabelt nivå. Kriteriene for å kunne akseptere et risikonivå må deretter vurderes opp mot verdiene som skal beskyttes [36]. Figur 3 viser skjematisk de beskrevne faktorene som danner et område som kan beskrives som risiko.

Figur 3 beskriver faktorene trussel, sårbarhet og kritisk informasjon, og hvordan de danner nye overlappende faktorer [36]:

1. Kritisk informasjon og objekter, uten kjente sårbarheter og trusler.
2. Sårbarheter som eksisterer i systemer, utstyr og programvare, som ikke har tiltknytning til kjente trusler.
3. Trusler som ikke har noen tilknytning til kritisk informasjon og objekter eller sårbarhetsinformasjon.
4. Kritisk informasjon og objekter som har kjente sårbarheter men ingen kjente trusler.
5. Kritisk informasjon og objekter, som har kjente sårbarheter og trusler. Dette er det



Figur 3: Beskrivelse av Risiko. Hentet fra «Defence-in-depth» av Robichaux og Bass.

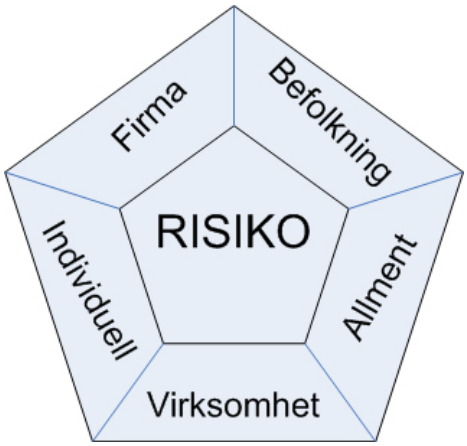
mest kritiske området og utgjør en risiko.

6. En trussel eller antall trusler har tilgang til kunnskap og ressurser til å utnytte en sårbarhet men ikke ved et kritisk informasjon eller objekt.
7. Kritisk objekt som ikke har kjente sårbarheter, men kan bli eksponert for en spesifik trussel.

3.4.2 Risikovurdering

Pfleeger [23] beskriver vurdering av risiko med bakgrunn fra vårt daglige liv. Det beskrives at vi vurderer risiko og tar risiko hver dag, for eksempel når vi krysser en vei, eller kjører til og fra arbeid. Bevisst eller ubevisst, vurdere vi utfall av å ta risikoer. Og selv om det er stor sjanse for et negativt utfall, trenger vi ikke nødvendigvis unngå å ta en risiko. Det beskrives at slike enkle handlinger preger vårt handlingsmønster ulikt i ulike situasjoner.
Innen IKT og system, handler risikoanalyse ofte om å redusere risikofaktorer som påvirker og utgjør en trussel for systemene. Når vi ikke kan eliminere eller håndtere et spesifikt risikoproblem eller en uakseptabel trussel, fordrer vi ofte å overføre risikoen til andre systemer, hvor risikoen er mindre eller hvor vi mener vi har større grad av kontroll. Videre beskrives det at vi gjør ulike vurderinger av risiko i ulike situasjoner, ofte avhengig av hvilke parametre vi velger å vektlegge. For eksempel antallet personer som blir påvirket av en risiko og hvordan de blir påvirket. Kumamoto og Henley [1] beskriver forskjellen for eksempel ved individuell risiko og befolkningsrisiko. Samtidig beskrives det fem forskjellig syn på risiko avhengig av ståsted, se figur 4.

Det som ofte preger ROS-metodene, eksempelvis [10, 3, 27, 11], er at vurderinger og beregning av risiko ofte skjer ved sammensetning av faktorene konsekvens og sannsynlighet. De to dimensjonene bygger ofte på resultatet i en diskusjon, erfaringer og vurderinger av mulige hendelser utført av panelet i referansegruppa. I et samfunn og en virksomhet preget av stadige endringer, vil det i ulike tilfeller være misvisende å benytte seg av historiske fakta og opplysninger som grunnlag for vurdering av fremtidige hendelser [23]. Problemet som ofte blir beskrevet, er graden av unøyaktighet og subjektivitet i vurderinger [23]. En risikoanalyse er ofte en subjektiv vurdering og bygger ikke



Figur 4: Skissering av forskjellige syn på risiko. Hentet fra [1] av Kuamoto og Henley.

på vitenskaplige fakta. Og ofte har vurderingene bakgrunn i empiriske data som ligger i referansegruppa, og kan dermed gi et falskt og unøyaktig risikobilde [23].

Samtidig er begrepet «tilfeldighet» et element som preger sannsynlighetsberegninger, og ofte påvirker i stor grad fastsettelse av risiko og trussel. Det beskrives vanligvis en forskjell i forhold til risiko ved tilfeldige og tilsiktede hendelser, som ofte kategoriseres inn i fagområdene «safety» og «security» [3]. For tilfeldige hendelser avgjøres det ofte hvilken sannsynlighet en trussel har for å inntreffe. Dette gjøres ved å anta at en hendelse inntreffer tilfeldig basert på en historisk frekvens, og analytikere kan ta i bruk stokastiske metoder med estimater for sannsynlighet [37]. Når det gjelder tilsiktede hendelser, vil sannsynlighetsberegninger medføre et gyldighetsproblem [38, 39]. Holm [38] beskriver dette i sitt arbeid ved:«for eksempel vil en sannsynlighet være lik 1 og ikke en statistisk verdi fremkommet av erfaringsdata, når en motstander har bestemt seg for å gjennomføre et angrep. Dette illustrerer svakheten med den tradisjonelle risikodefinisjonen, og gjør det nødvendig å bruke flere perspektiver for å forstå risiko som et uttrykk for det totale trusselbildet og den faren som informasjonssystemer står ovenfor». Audestad [7] beskriver risiko som et produkt av konsekvens og sannsynlighet, og betegner funksjonen ved formelen:

$$R = f(k, s)$$

Hvor R beskriver risiko, og k konsekvens eller utfallet av hendelsen, og s beskriver sannsynligheten.

Aven [39] drøfter og beskriver at risiko ikke er et produkt av konsekvens og usikkerhet/ sannsynlighet(som Audestad [7] beskriver), men en kombinasjon av de to begrepene. Han beskriver at for å utføre en risikoanalyse og evaluere en risikohåndtering, er det nødvendig å forstå hva som ligger i begrepet «risiko». Det er også nødvendig å forstå hvordan risiko blir definert. Det beskrives at det er mulighet for å se sannsynlighet som en relativ frekvens eller en subjektiv sannsynlighet. Aven [39] beskriver videre at analytikere bør konsentrere seg om den mengden hendelser/angrep som faktisk er skjedd over en tidsperiode, og ikke om en tiltenkt frekvens av hendelser.

Aven [37] har også beskrevet en klassisk modell og en subjektiv (bayesiansk)/ subjektivistisk statistikk sannsynlighetsmodell, som kan benyttes ved vurdering av sannsynlighet. Dette er en tilnærming hvor en blander subjektiv informasjon med objektiv informasjon. Den subjektive informasjonen uttrykkes i en sannsynlighetsfordeling selv om man ikke har en kjent datamengde. Metodene kan for eksempel benyttes for å analysere prosjektusikkerhet og nedetider på systemer. Teknikkene og modellene kan således gi kunnskap som kan benyttes i vurdering av risiko eller pålitelighet ved et systemet, som således kan gi grunnlag for å bestemme akseptkriterier for systemet.

Avslutningsvis velger å nevne at risikovurdering er en mulighet for å kunne avdekke og vurdere sannsynligheten for, og konsekvensen av en uønsket hendelse. En risikovurdering i seg selv er ikke et sikkerhetstiltak, men skal kunne danne et fundament for vurderinger av andre nødvendige sikkerhetstiltak for å oppnå et aksepterende nivå av sikkerhet [3].

3.4.3 Risikovurdering og usikkerhet

Det er gjort omfattende forskning på hvordan faktiske beslutninger tas, og utviklet teorier om hvordan valg gjøres under usikkerhet. Teoriene er utviklet for å forsøke å forutsi faktiske valg, og forklare hvorfor velinformerte mennesker ikke bestandig handler i sam-

svar med forventet nytte-teori. «Prospect theory» [40], «Disappointment theory» [41], og «Regret theory» [41] er eksempler på noen teorier. Risiko vil bestandig inneholde en usikkerhet. Når vi vurderer risiko, vurderer vi en form for usikkerhet og hvorvidt en hendelse kan inntreffe. Vi forsøker å ta forbehold om at en hendelse kan skje, ved å vurdere ulike parametere forbundet med risikoen. Eksempelvis parametrene «sannsynlighet» og «konsekvens» i en risikomatrise. von Neumann og Morgensterns [42] «Forventet nytte-teori» er kanskje den mest sentrale teori om beslutninger under usikkerhet. Teorien beskriver at en rasjonell beslutningstaker velger det handlingsalternativet som gir størst forventet nytte. Teorien tar i bruk sju forskjellige aksiomer, og som gjør det mulig for forskere å kunne sammenligne de matematiske prediksjonene fra aksiomene med virkelige beslutningstagere. von Neumann og Morgenstern viste at hvis beslutningstagere bruker disse aksiomene, vil det være mulig å komme frem til nytteverdi, det vil si personlige verdier ved beskrivelse av konkrete tall. Tallene kan således indikere hvilken personlig verdi de ulike beslutningsalternativene har for den personen som skal ta beslutningen.
Gonzalez [43] studerer hvordan mennesker handler og gjør valg under risiko i et IKT-miljø ved bruk av Kahneman og Tversky [40] sin «Prospect»-teori. «Prospect»-teorien beskriver hvordan personer ofte foretrekker å gi det alternativet som gir størst tap mest oppmerksomhet og verdi. For eksempel i en situasjon med høy usikkerhet og med mulighet for å tape penger, gis det større oppmerksomhet til denne delen som inneholder tap, enn et alternativ som kunne gi fortjeneste. Gonzalez presenterer således hvordan handlingsmønstre i et risikobasert IT-miljø kan benyttes for å utvikle sikkerhetspolicy.

3.5 Metode og ROS-analyse

Innledningsvis vil det være naturlig å redegjøre for hva vi legger i begrepet metode. «Metode» betyr systematisk og planmessig fremgangsmåte for å løse et problem eller oppnå et resultat, og stammer opprinnelig fra det å følge en viss vei mot et mål [44].

3.5.1 Om metode

Metoden i seg selv, gir ikke svar på spørsmålene som er definert, men er kun et virkemiddel og redskap som skal gi en bedre og mer riktig forståelse av det problemet en søker kunnskap om [1]. En ROS-analyse er et eksempel på en slik systemorientert fremgangsmåte. En ROS-analyse kan gi en beskrivelse av utfordringer ved sikkerhet som en virksomhet står overfor. Utgangspunktet for å utføre en ROS-analyse er for mange virksomheter og organisasjoner pålagt av lovverket. For eksempel gjennom krav til et Helse, Miljø, Sikkerhetssystem(HMS-system), eller som resultat av retningslinjer fra Datatilsynet. For andre organisasjoner som ikke er underlagt krav fra lovverk, kan utgangspunktet være et internt ønske om å bedre kvaliteten og sikkerheten for virksomhetens kritiske prosesser [3].

Budgen [45] setter risikoanalyse i et historisk perspektiv og beskriver videre «at den moderne utvikling av samfunnet krever gjennomføring av risikoanalyse». Dette er noe som også Guldbrandsen [6] påpeker og understreker. Videre beskriver Bugden at det ikke lenger er godt nok med uttalelser fra eksperter, og det konkluderes med at risikoanalyser ikke bør utelates som en del av design prosessen. Jenkins [46] beskriver en overordnet og stegvis fremgangsmåte for risikoanalyse, samt en beskrivelse av struktur og hva som er vesentlig med den endelige rapporten.

3.5.2 Risikoanalyser og Sårbarhetsanalyser

Idsø og Jakobsen [27] beskriver en forskjell på risikoanalyse og sårbarhetsanalyse. Følgende beskrives forskjellen for å oppklare hva som legges i de to begrepene. «En sårbarhetsanalyse er mer omfattende enn en risikoanalyse, med hensyn til det som skjer etter at ulykken har inntruffet». Når en uønsket hendelse inntreffer blir systemet forskjøvet fra en operativ tilstand, til en uønsket innoperativ tilstand. I motsetning til risikoanalyse fokuserer en sårbarhetsanalyse også på avbruddsperioden og hvordan en ny stabil tilstand kan oppstå.
En risikoanalyse legger normalt mer vekt på trusler enn en sårbarhetsanalyse. Kort sagt har risikoanalyser fokus på skader som systemet blir utsatt for, mens sårbarhetsanalyser har fokus på overlevelsesevnen til systemet. Sårbarhetsanalyser inkluderer også som oftest et bredere trusselspekter enn risikoanalyser» [27]. I den senere tid har disse to begrepene ofte blitt slått sammen til begrepet ROS-analyse (Risiko- og sårbarhetsanalyse) [39, 3].
Risiko- og sårbarhetsanalyser kan videre kategoriseres inn i to forskjellige kategorier under «lette» og «tyngre». Kategoriseringen av en tyngre og en lettere metode, er ofte basert på en vurdering av hvor sofistikert og omfattende metoden er[1]. En lett metode blir ofte karakterisert ved egenskaper ved metoden, som foreksempel enkel i bruk, overordnet analyse egenskaper og krever mindre ressurser i form av tid, økonomi og personell[2]. En tyngre metode er ofte karakterisert ved det motsatte. Den krever en omfattende analyse og langt større grad av ulike ressurser[3]. Innen ROS-analyse, beskrives det av Sintef [47] at de fleste metoder for risiko- og sårbarhetsanalyse omhandler kartlegging av truslene under spørsmålet «Hva kan gå galt?», for deretter å definere graden av begrepene konsekvens og sannsynlighet, ved spørsmålene «Hva er sannsynligheten for at det går galt?» og «Hva er konsekvensene hvis det går galt?».

3.5.3 Klassifisering av metode

ASIS Norway [48] har gjennomført et arbeid med kartlegging av metoder for risikoanalyse. Metodene ble skilt i hovedtrekk mellom sjekklister, kvantitative og kvalitative analyser. Følgende beskrives de forskjellige kategoriene av metode.

Sjekklister blir beskrevet mer som en form for revisjonsverktøy enn risikoanalyseverktøy. ASIS Norway [48] beskriver sjekkliste-verktøyer som raske og ressursmessig «billig». Det beskrives også at de egner seg best når verktøyene er tilpasset den enkelte virksomhet. Det negative med en sjekkliste-metode, er at «de kan medføre unøyaktighet og en risikerer å iverksette tiltak på feil sted», samt at verktøyene ofte krever eksperthjelp ved utvelgelse av kriterier for analyse.

Den neste katergorien som presenteres er kvantitative analyser. Som tilnærmingen tilsier er kvantitative metoder avhengig av et statistisk materiale. Ved bruk av slike metoder forutsettes med tilgang til et stort og godt statistisk datasett. ASIS Norway [48] beskriver en fordel ved denne typen tilnærming ved at en kan oppnå objektivitet i målingene, og at resultatet kan uttrykkes i et mer ledelsesspesifikt språk. Tilnærmingen har også en fordel som kvalitative-metoder mangler, muligheten for å gjøre bedre kost-nytte vurderinger. ASIS Norway [48] beskriver at det negative ved slike metoder er manglen på statisk materiale, og videre at metodene benytter seg av relativt komplekse beregninger.

[1] Møte med Janne Hagen, 13.01.2006
[2] Møte med Håvard Friheim, 12.12.2005
[3] Møte med Håvard Friheim, 12.12.2005

	Action assessment.	**Coarse risk and vulnerability assessment.**	**Model based risk and vulnerability assessment.**
Conceptual phase		X	
Design phase	X	X	X
Operational phase	X	X	X

Tabell 1: Illustrerer kategorisering verktøyer i forhold til bruksområdet. Hentet fra «Methods for risk and vulnerability assessments of infrastructures depending on ICT» av Wiencke, Aven m.fl.

Når det gjelder kvalitative analyser, er disse ofte skjemabaserte, eksempelsvis KITH [10], NSM-ROS2004 [3] og ROSS [27]. Denne formen for analyse har en tilnærming hvor det tas utgangspunkt i de enkelte objekter eller uønskede hendelser. Vurderingene av sannsynlighet og konsekvens blir ofte utført ved hjelp av en risikomatrise. Og ofte blir sammensetningen av kompetanse i refereransegruppa avgjørende for sluttresultatet som foreligger. Det beskrives at ulempen ved en slik tilnærming er mangel på objektive målinger, og at iverksettelse av tiltak mangler kost-nytte vurderinger.

3.5.4 Valg av metode

BAS-forskningen ved FFI har kommet til 5.prosjektgenerasjon, og omhandler informasjon og kommunikasjonsteknologi med fokus på samfunnskritiske funksjoner og infrastruktur. BAS5 er et samarbeid mellom flere aktører blant annet FFI, Universitetet i Stavanger, HiG og NTNU, samt flere bedrifter, departementer og direktorater. BAS5 skal i løpet av våren ferdigutvikle et rammeverk for valg av ROS-metoder. Formålet er å utvikle og anvende en ROS-metode på samfunnsviktige IKT-systemer, og utvikle og anvende en metode for å rangere tiltak som reduserer sårbarheten. Arbeidet som presenteres er basert på sammensetning fra flere fagområder, både risiko og sårbarhet, informasjonssikkerhet, samfunnsmessig sikkerhet og IKT-system sikkerhet. Det presenteres i arbeidet en kategorisering av verktøyene og teknikkene basert på bruksområde, se tabell 1. Kategoriseringen blir deretter delt inn i forskjellige faser, beskrevet som henholdsvis konseptfasen, designfasen, og operasjonellfase.

I den konseptuelle fasen, blir alternative konsepter evaluert. «Input» til valg av det beste konseptet eller løsningen blir foreslått. Når det gjelder designfasen, blir det spesifisert konseptet som ønskes optimalisert. Detaljerte tekniske løsninger og design krav blir i denne fasen spesifisert. Den siste fasen, operasjonellfase, tar for seg den normale operasjonelle funksjonen til IKT-systemet, hvor det vil bli spesifisert ulike krav til IKT-systemet, som hastighet, pålitelighet osv.

Videre kategoriseres metoder avhengig av funksjonalitetsfokus, se figur 5. Figuren 5 skisserer oppbyggning av rammeverk for valg av metode. Metodene deles inn i funksjonalitetskategoriene: handlings-baserte (som foreksempel ved bruk av sjekklister), grovbaserte, og modellbaserte risiko- og sårbarhetsvurderinger. Funksjonalitetskategoriseringen av verktøyene kobles deretter opp mot de fasene som er beskrevet i tabell 1, slik at valg av metode for gjennomføring av ROS-analyse baseres på fasen.

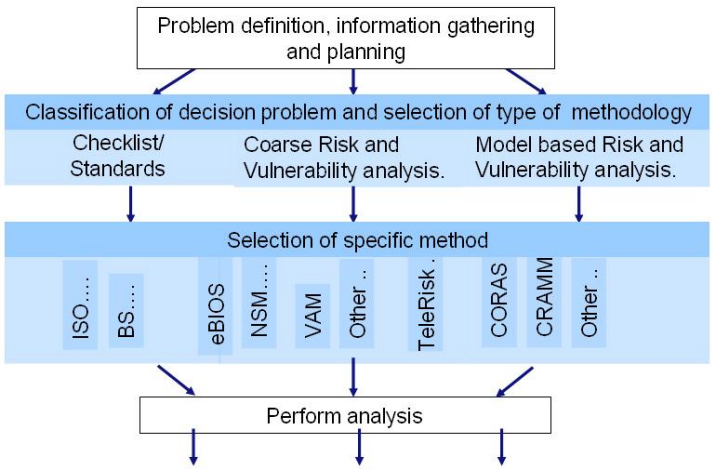
3.6 Arkitektur og infrastruktur

I dette kapitlet beskrives arbeid som er gjort på området arkitektur og infrastruktur. Caplex[44] definerer infrastruktur som: «underliggende struktur, flyplasser, havner, veier, jernbaner, telekommunikasjonsmidler o.a. vitale serviceanlegg i et samfunn».
Limoncelli og Hogan [13] beskriver i sitt arbeid at en nettverksarkitektur bør være enkel og velformet, og bygget for pålitelighet. En enkel og velformet arkitektur omfatter både fysisk og logisk inndeling. Det beskrives også at den teknologiske utviklingen er en stadig utfordring for en enkel og velformet arkitektur, og at antallet forskjellige leverandører er med på å øke kompleksiteten i nettverket.

3.6.1 Infrastruktur

Fridheim [49] beskriver eksempler fra kritisk infrastruktur ved privatisering og effektivisering, og trekker frem dereguleringen av kraftforsyningen i Norge på 1990-tallet. Det beskrives i eksemplet at nedbemanning fører til at en ikke kan drive kraftforsyningen manuelt lenger, som videre medfører redusert vedlikehold og således at infrastrukturen slites ned. Fridheim hevder at effektivisering medfører en knappere margin, slik at overkapasitet og «slakk» forsvinner i infrastruktur. Videre beskriver han ulike effekter som kan knyttes til privatisering og effektivisering, som blant annet sentralisering, reduserte kapasiteter, manglende reserveløsninger og nedslitt infrastruktur.
Når det gjelder hvorfor sårbarhet i kritiske IKT-systemer oppstår, beskrives det faktorer som uforutsigbarhet, kompleksitet og tett koblede systemer. Sårbarhet i kritiske IKT-systemer medfører også flere muligheter for å angripe IKT-systemene, både ved fysiske angrep, angrep gjennom nettverk (ved ikke behov for nærhet til angrepsmålet) og ved at informasjon om enkeltsårbarheter spres raskt. Samtidig vil sentralisering av tjenester og informasjon, ofte kreve en sentralisert lagring av informasjon og større avhengighet av sentrale servere. Noe resulterer i økt sårbarhet i knutepunktene i infrastrukturen.

Nystuen og Hagen [50] beskriver den dramatiske endringen i bruken av telekommunikasjon. «Muligheten til billig og effektiv behandling og utveksling av informasjon



Figur 5: Skisse av presentert rammeverk. Hentet fra «Methods for risk and vulnerability assessments of infrastructures depending on ICT» av Wiencke m.fl.

er i stor grad med på å forme dagens og morgendagens samfunn. Moderne informasjonsteknologi har gjort det mulig å forbedre bedriftenes leveringssikkerhet, samtidig med rasjonalisering». Nystuen og Hagen beskriver videre at «som en følge av dette har intensiteten og pulsen i samfunnets virksomheter økt» og «tid er blitt en meget kritisk ressurs». Det nevnes også at lave kostnader ved behandling og distribusjon av informasjon medfører at informasjonen legges der det både er hensiktsmessig og kosteffektivt å lagre/produsere den. Dette påvirker den totale sårbarheten infrastrukturen. Nystuen og Hagen påpeker videre at sentrale knutepunkter i alle typer nett som oftes er sikret mot ulike former for trusler, men et svakt punkt vil påvirke den totale sårbarheten i nettet. Det beskrives at kompleksitet og konsentrasjon ofte reduserer antallet tjenestenoder i et nett. For eksempel medfører den økende kompleksiteten i nettet at antallet tjenestenoder forsøkes reduseres, og dette medførere en konsentrasjon av knutepunktene til noen få sentrale steder.

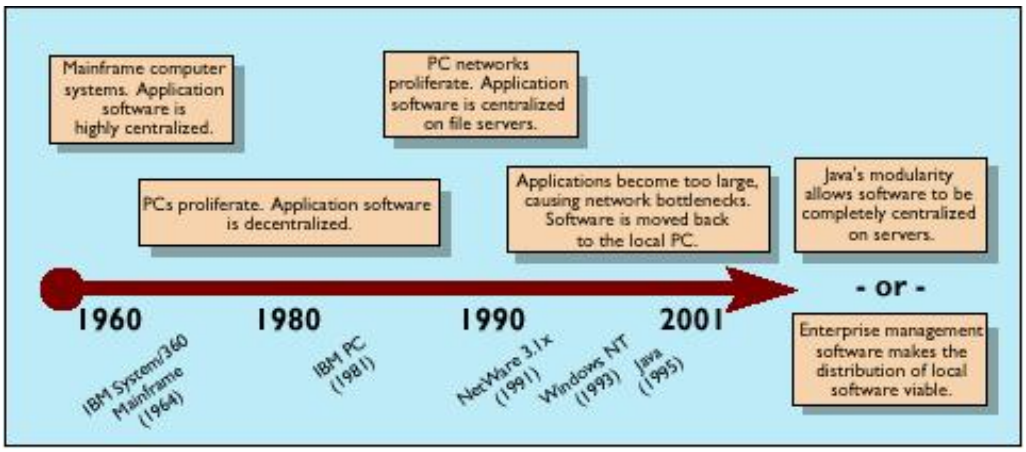
Rodal [51] beskriver sårbarhet ved kraftforsyningnes drift- og styringssystemer. Rodal påpeker i arbeidet en økt sårbarhet som følge av sentralisering. Dette underbygger Rodal ved at større regionale selskaper har et større kommunikasjonsbehov i vanlig drift, enn små lokale selskaper med nær beliggenhet til egne installasjoner og anlegg. Det beskrives at de små selskapene er mindre sårbare overfor kommunikasjonsbrudd enn de store. Samtidig går trenden allikevel mot større og færre aktører innen kraftforsyningen. Rodal forklarer videre at «Konsentrasjon og sentralisering har vært nøkkelord for utviklingen innen kraftforsyningen de siste ti årene. Den enkelte driftssentral bli dermed viktig for kraftforsyningens evne til å fungere, og øker mulighetene til å svekke større deler av kraftsystemet ved få anslag». Rodal påpeker videre at distribuerte driftssentralløsninger for store aktører, gjør at andre driftssentraler kan ta over prosesstyringen dersom en av sentralene faller bort. I en oppsummerende sårbarhetsvurdering av kraftforsyningen forklarer Rodal at det er en betydelig mengde informasjon som skal utveksles mellom et stort antall aktører, og at utviklingen tilsier at informasjonsutvekslingsbehovet i fremtiden vil øke ytterligere. Rodal beskriver videre at «for å oppnå effekt på totalsystemet bør angrepene sannsynligvis helst rettes mot datakommunikasjonssystemene i driftsnettet til de større aktørene», og at «angrep mot mindre informasjonssystemer har liten effekt på totalsystemet, og får sannsynligvis kun lokal virkning i en kortere periode». Dette kan tolkes som at den største sårbarheten ligger i knutepunktene ved en sentralisering. Fridheim [52] beskriver også dereguleringen av kraftforsyningen på 1990-tallet, men setter det i et informasjonsteknologisk perspektiv. Han beskriver hvordan sårbarheten har økt ved å gå fra mindre isolerte systemer, til å koble flere kraftavdelinger sammen ved hjelp av informasjonsteknologi. Noe som han påpeker vil redusere den generelle sikkerheten fordi systemene nå er åpne for angrep utenfra.

3.6.2 Sentralisering eller desentralisering

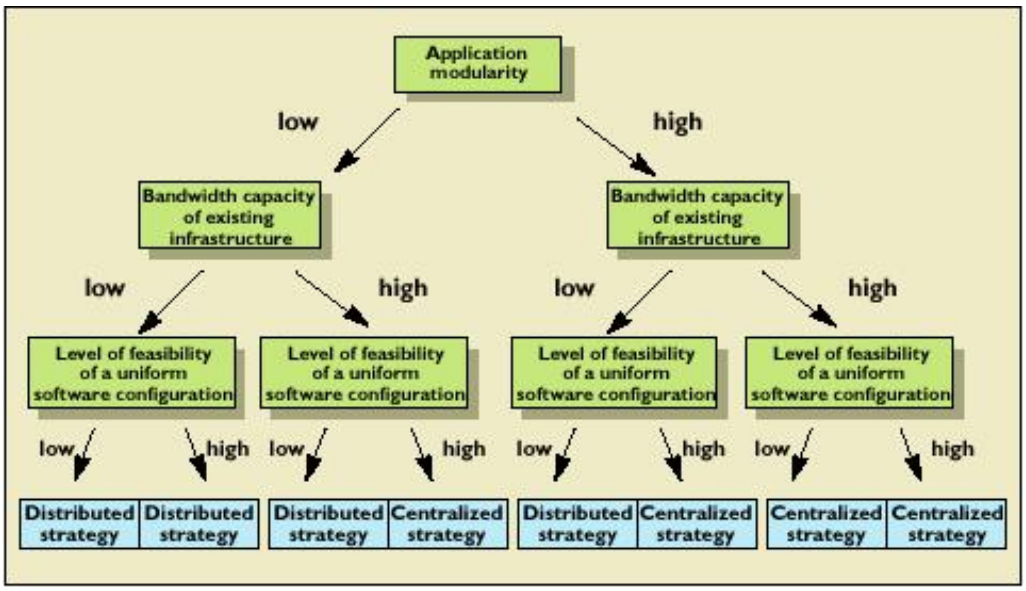
Schuff og Loise [2] forklarer hvordan informasjonsteknologi de siste 50-årene har pendlet mellom sentralisering og desentralisering av programvare, se figur 6. Figur 6 viser forskjellig utvikling som har påvirket sentralisering og desentralisring av programvare.

Schuff og Loise beskriver retningslinjer for valg av sentralisering eller desentralisering av applikasjonsprogramvare. Det presenteres et rammverk, se figur 7, for valg av tilnærming. Rammeverket kan bidra til å identifisere hvilken tilnærming som er mest egnet innen en organisasjon eller virksomhet. Det drøftes også hvordan sentralisering og

desentralisering lar seg påvirke av ulike økonomiske forhold. De beskriver flere positive effekter ved begge tilnærmingene. Ved sentralisering beskrives positive effekter som enklere support, reparasjon, vedlikehold, patching og oppdatering av software, samt økt service til brukerne. Ved desentralisering påpekes det positive effekter ved lavt bruk av båndbredde, større frihet til å skreddersy maskiner til brukere og mindre restriktive krav til programvare. Avslutningsvis påpekes det at sentralisering eller desentralisering bør sees i sammenheng med organisasjonens fremtidige og ønskede utvikling, både innen programvare, maskinvare og maskinutstyr. Samtidig så må det også tas forbehold om enkelte teknologiske begrensninger som for eksempel organisasjonens tilknytning ved båndbredde og krav som settes til systemenes pålitelighet osv. Ved sentralisering kan



Figur 6: Viser utvikling som har påvirket sentralisering og desentraliseing av applikasjonsprogramvare (Hentet fra Schuff og Louis [2]).



Figur 7: Viser det presenterte rammeverket(Hentet fra Schuff og Louis [2]).

det legges tilrette for å oppnå høy pålitelighet til systemet, men resultatet vil ofte gå på bekostning av ytelse. Til motsetning vil desentralisering tilby større grad av ytelse og mindre grad av pålitelighet.

Limoncelli og Hogan [13] beskriver sentralisering og desentralisering med et teknisk og administrativt fokus. Det forklares at nye tekniske paradigmer åpner for sentralisering, og at sentralisering åpner for en større grad av kontroll. Sentralisering kan også beskrives som et forsøk på å øke effektiviteten ved reorganisering av virksomheten. Tilnærmingen blir ofte begrunnet med at det kan være identifisert et potensial for økt økonomisk inntjening. Desentralisering derimot, beskrives som en type tilnærming som kan karakteriseres som et «opprør» for å gå bort fra et byråkratisk system, som ofte er preget av hegemoni. Limoncelli og Hogan begrunner dette med at det ofte oppstår en frustrasjon hos brukerne over at resultatet med sentralisering ofte medfører at «gjør-det-selv»-måten er enklere. Limoncelli og Hogan definerer også kandidater for hver av retningene. Argumenter for sentralisering kan være: sentralisering av systemadministrasjon, enklere arkitektur, samling av flere tjenester på en og samme enhet og sentralisering av ekspertise og kompetanse. Argumenter for desentralisering er: økt feil-toleranse (redusert single-point-of-failure), muligheten for individuell tilpassing av systemer og evne til å møte målgruppen i en større grad. Avslutningsvis beskrives det at eksisterende organisasjonsstruktur ofte danner grunnlag for hvilken tilnærming organissasjonen velger.

Bellika, Hartvigsen m fl. [28] drøfter problematikken ved sentralisering og desentralisert datalagring innen helsesektoren i form av et datavarehus. Det beskrives en oppsummerende konklusjon følgende: «slik vi ser det representerer en sentralisert løsning, der alle helseforetakene sender data til en felles datalagringsenhet, det beste alternativet med hensyn til sikkerhet, sårbarhet og tilgjengelighet». Bellika, Hartvigsen m fl. hevder at en desentralisert løsning vil være den beste med hensyn til mulig funksjonalitetsnivå, men også at det er problematisk med hensyn på å ivareta tilstrekkelig grad av sikkerhet i mindre institusjoner. Det beskrives også bekymring ved tilgjenglighet under driftsavbrudd, kabelbrudd osv. Samtidig blir det også påpekt bekymring ved tilgang til systemressurser for å betjene eksterne institusjoners informasjonsbehov.

3.7 Modellering og modelleringsspråk

Olsen [53] presenterer i utgangspunktet tre forskjellige metoder for å modellere et system med hensyn på identifisering av sikkerhet og for å kunne øke sikkerheten i systemer. Metodene beskrives som «trusselmodellering», «angrepsmodellering» og «protokollanalyse». Trusselmodellering er mest benyttet innen programvare- og systemutvikling, og ofte i den initielle fasen. Trusselmodellering defineres ved en retning som er basert på forståelse av hva en fiende vil oppnå med et angrep på systemet. Til motsetning forsøker angrepsmodellering å identifisere en fiendes fulle angrepsvei til et system ved å identifisere mindre angrepsmål som er identifisert som svakheter. Protokollanalyse har derimot til hensikt å avdekke svakheter ved kommunikasjonen mellom entiteter som benytter seg av systemet. Det beskrives at metoden derfor ikke primært dekker selve systemet. Det beskrives videre at angrepsmodellering og trusselmodellering, er ansett som mest verdifull i designfasen av et system, enn for evaluering av et eksisterende system.

Snekkenes og Olsen [54] presenterer et rammeverk for fiendemodellering. Rammeverket tar for seg fienden eller fiendene et system er utsatt for. Dette karakteriseres ved «fiendemodellen» som systemet må operere under. Videre beskrives det som en stor fordel med god kjennskap til systemet, for lettere å kunne identifisere kommunikasjonkanaler og implementerte sikkerhetsbarrierer. Rammeverket beskrives som verdifullt i situasjoner hvor man ønsker å få oversikt over de antagelser som er gjort med tanke på fienden, og når en virksomhet vurderer en endring i bedriftskritiske systemer.

CORAS-prosjektet [55] har utviklet en metode med et verktøy for modellbasert sikkerhetsanalyse. Verktøyet kan både benyttes for eksisterende og nye IKT-systemer. Modelleringen er utviklet som et PC-verktøy og benytter seg av UML(Unified Modeling Language). Verktøyet gir god støtte for å lagre og gjenbruke beskrivelser og modeller av systemet som analyseres. Det er utviklet UML-profiler for identifisering og analyse av sikkerhetsrisiko. Meta-modeller brukes for å beskrive blant annet kontekster for risikoanalyse. CORAS benytter grafiske modeller i sikkerhetsanalysen for å oppnå presisering av informasjon, og for å oppnå et riktig og bedre abstraksjonsnivå [55]. Videre beskrives det at verktøyet kan være nyttig for helseforetak, helsenett og deres IKT- og nettleverandører for å få oversikt over potensielle sikkerhetstrusler vedrørende IKT-systemene.

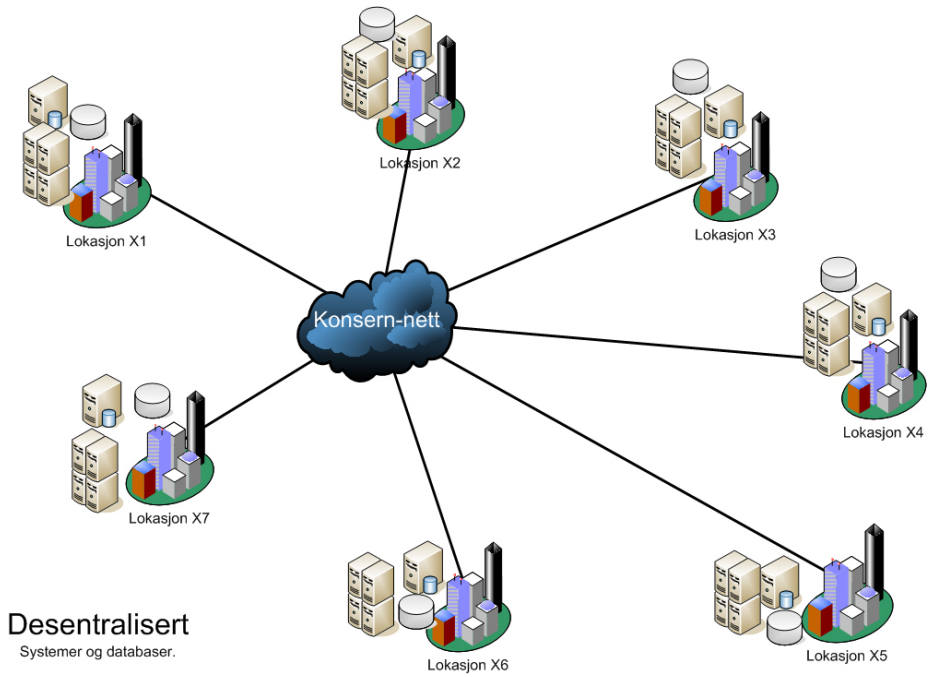
Moore, Ellison og Linger [56] beskriver og illustrere en tilnærming for modellering av angrepsmønstre. I arbeidet beskrives det fordeler ved å dokumentere og å modellere angrep ved bruk av treanalyse og gjenbruk av angrepsinformasjon. Tilnærmingen som presenteres beskriver at «sikkerhetsanalytikere bør identifisere og dokumentere angrepsmønstre som gjentar seg, slik at de kan designe og utvikle informasjonssystemer som er mer robuste». Angrepstre blir beskrevet som en systematisk fremgangsmåte for å karakterisere et systems sikkerhet. Struktur og semantikk benyttes ved bruk av noder i form av trestruktur. Konstruksjon av angrepsscenarioer skisseres ved bruk av «AND»- og «OR»-operatorene som bygges inn i trestrukturen.

4 Beskrivelse av dagens organisasjon og struktur

I dette kapitlet beskrives dagens helsesektor og oppbyggning av IKT-infrastruktur i helsesektoren. Først presenteres dagens system, og deretter hvordan helsesektoren ser for seg å løse de identifiserte problemene. Tilslutt beskrives områder i helsesektoren som både tilrette legger og legger begrensninger på en ønsket løsning.

4.1 Hvordan dagens system fungerer

I dagens system har hvert enkelt helseforetak sitt eget pasientsystem og pasientdatabase, se figur 8. Når pasienten sendes fra en behandlingsinstitusjon til en annen, sendes pasientjournalen/dataen til neste behandlingsinstitusjon med e-post eller faks, og deretter ettersendes med post eller budbil. Dette vanskeliggjør en effektiv funksjonalitet for helsevirksomhetene i en akuttsituasjon, hvor en pasient er sendt fra en behandlingsinstitusjon til en annen. For at en lege skal få innsyn i pasientens journal, må det gis spesifikk tilgang fra den institusjonen som pasienten ble sendt fra. Figur 9 viser en skisse av hvordan et fremtidig system vil se ut, hvor hver behandlingsinstitusjon har tilgang til en sentralisert pasientdatabase og pasientsystem. Helsesektoren ønsker et sentralt system som utfører alle forespørsler fra institusjonene innen en region. Ved en overgang til et fremtidig system, vil pasientdataen og pasientsystemet samlokaliseres ved en geografisk beliggenhet. Dette gjør at budbil, faks eller post ikke lenger er nødvendig.



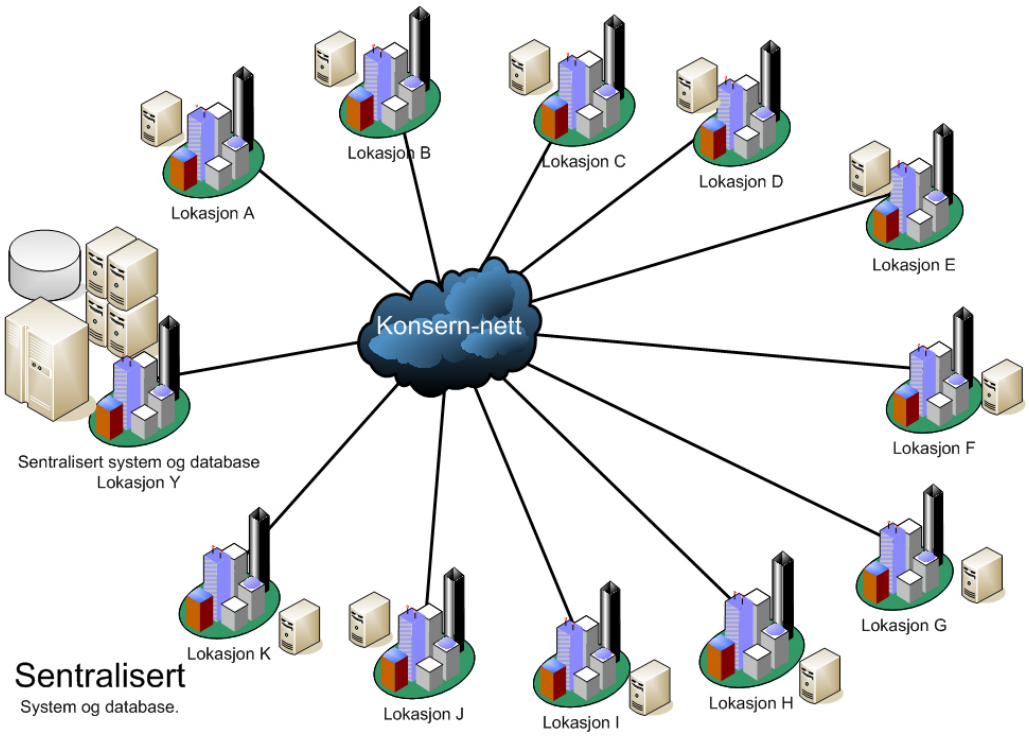
Figur 8: Hvordan systemet ser ut i dag.

4.1.1 Eksisterende infrastruktur innen Helsesektoren

Norsk Helsenett er et lukket nettverk for elektronisk kommunikasjon i helse- og sosialsektoren. Alle sykehusene er koblet opp til Norsk Helsenett. Dette gir muligheter for samarbeid og samordning av IKT-tjenester innenfor sektoren. Samtidig gir det muligheter for samarbeid om drift og vedlikehold av IKT-systemer, og andre kvalitetssystemer.
Både pasientdataen og programvaren som er nødvendig for behandling av pasienter er ofte lokalisert på andre (geografiske) steder enn der hvor pasientbehandlingen foregår. I dagens helsesektor, foregår det også en samlokalisering av data fra forskjellige avdelinger og behandlingsløp, dvs. somatikk, psykiatri og rus. Noen eksempler på denne samlokalisering er Helse Midt-Norge, Helse Vest og Sykehuset Innlandet. da Vinci Consulting [57] påpeker at det finnes et forbedringspotensiale forbundet med utveksling av persondata på nasjonalt nivå. Rapporten beskriver nå situasjon og foreslår muligheter ved økt fokus på riktig bruk av IKT som et hjelpemiddel.

4.1.2 Dagens EPJ og system status

En pasientjournal er en samling av alle opplysninger om en persons sykdom og andre sensitive opplysninger nedtegnet av lege og annet helsepersonell [10]. En «Elektronisk pasientjournal»(EPJ) er en pasientjournal hvor informasjonen er elektronisk lagret på en slik måte at den kan gjenfinnes ved hjelp av et elektronisk verktøy [8]. Informasjonen i en EPJ omfatter alt fra fritekst til strukturert informasjon, bilder, lyd og video [5]. Det er derfor et behov for å utveksle informasjon av enhver type, grad av sensitivitet, størrelse og kvalitet, både innenfor egen institusjon og mellom eksterne institusjoner [5]. Manglende integrasjon mellom EPJ og ulike fagsystemer som røntgen, laboratorium osv., er



Figur 9: Skisse av et mulig fremtidig system.

mange steder et vesentlig problem. Det er derfor en utfordring å utvikle EPJ til å bli et bedre verktøy i behandlingssituasjonen og legge tilrette for at nødvendig informasjon i pasientbehandling kan overføres på en enkel måte [58]. Det beskrives av Nasjonal IKT [59] at «Dagens EPJ-systemer i helseforetak er i liten grad basert på standardiserte krav regionalt og nasjonalt. Systemene som er i bruk på norske sykehus er så forskjellige i struktur og innhold, at det vanskeliggjør standardisering av informasjon som skal utveksles mellom systemene».

4.2 Beskrivelse av helseforetaket

Ved studert helseforetak benyttes det et stort antall forskjellig applikasjoner og systemer, og det er identifisert et stort antall forskjellige brukerbehov og brukere. Institusjonene og avdelingene er svært varierende i størrelse. Lokasjonene er spredt over et stort geografisk område, og med en relativ stor forskjell i linjehastighet som knytter lokasjonene sammen. Kompleksiteten ved maskinvare og maskinutstyr er varrierende fra lokasjon til lokasjon, og sammenkoblingen av systemene medfører totalt sett en stor kompleksitet. Alle kritiske og sensitive data blir det regelmessig tatt backup av.
Siden helseforetaket er spredt over et stort geografisk område, er kommunikasjonen og tjenesteleveransen til brukeren svært kritisk og avgjørende. Kommunikasjonsløsningene er delt inn i to hoveddeler, lokalnett kommunikasjon (LAN) som vanligvis er internkommunikasjon i en bygning eller en lokasjon, mens ekstern kommunikasjon (WAN - Wide Area Network) er kommunikasjon mellom lokasjoner innen institusjon. Arkitekturen og oppbyggningen av kommunikasjonslinjene er en sentral faktor i IKT-infrastrukturen. Leveranse av kommunikasjonstjenesten ut til brukeren blir aldri bedre enn den kapasitet og tilgjengelighet som kommunikasjonsløsningen kan tilby. Kommunikasjonsnettverket er bygget opp rundt 2 hoveddeler, kjernenettet og distribusjonsnettet. Kjernenettet inngår foretakets større lokasjoner, og feil på et samband skal ikke medføre brudd på tjenesteleveranse, dvs at det bestandig eksisterer en reservevei tilgjengelig. Kapasiteten på båndbredden er fibertilknytning med 100 Mbps hastigheter til hovedlokasjonene. Dette er samme hastighet som en bruker(f.eks. doktor) har til sin pc på kontoret, altså innenfor samme institusjonsbygg. Distribusjonsnettet er tilknytningen til kjernenettet ved virksomhetens hovedlokasjoner. Ikke alle enheter tilknyttet distribusjonsnettet har full redundans. Det vil si at feil på samband kan medføre avbrudd i tjenesteleveransen til lokasjonen. Hastigheter for distribusjonsnettene er betydelig mindre enn kjernenettet. Ved nettverkssikkerhet og oppbyggning av organisasjonsstruktur, er det innen helsesektoren ofte benyttet såkalte flersonemodeller. En flersonemodell innebærer at at IKT-nettverket har flere tekniske sikkerhetsbarrierer mot eksterne nettverk.

4.2.1 Server-Klient løsninger

Ved helsefortaket er det, på bakgrunn av ulike behov for den enkelte bruker, valgt tre forskjellige klientløsninger. Når en bruker benytter applikasjoner bruker hun eller han en av de følgende variantene:

1. Programvare er i sin helhet installert og brukes på brukerens pc. Dette er den tradisjonelle og vanligste varianten med bruk av programvare installert på pc'n, og kan beskrives som en hjemme-pc eller en bærbar pc. Denne løsningen er konfigurert slik pga. funksjonelle eller ytelsemessige hensyn.
2. Programvaren installert på en sentral server, og blir kjørt der, dvs at programvaren

ikke installeres på den enkelte pc men det benyttes en terminalserverteknologi, og installasjoner og konfigurasjon av programvare gjøres på et sentral sted.

3. Denne varianten benyttes kun applikasjoner fra terminalserver, som i variant 2. Brukere av denne varianten har ikke behov for en full pc på sin arbeidsplass, men kan bruke såkalte «NC»-maskiner (Network Computer), som er maskiner uten disk, med svært begrenset minne og prosessor kraft.

Variant 1 og 2 krever at må brukeren ha en fullverdig pc med installert software. I variant 3, er det ikke nødvendig for brukeren å ha en fullverdig pc, fordi det ikke er nødvendig å installere programvarre på maskinen.

De forskjellige variantene krever flere forskjellige serverløsninger, både når det gjelder autentisering og autorisering, og behandling av applikasjoner. Derfor har helseforetaket forskjellige typer servere som besvarer forespørslene fra klientene. Følgende beskrives kort de forskjellige typene server:

1. Servere med lokalt disklager. Dette er databaseservere som har lagring internt i serveren, og dedikert for denne serveren alene. Ingen grad av feil-toleranse.
2. Applikasjonsservere, hovedvekten av applikasjonsservere er terminalservere.
3. Servere med sentralt disklager, i hovedsak databaseservere i cluster-teknologi.

4.3 Lovverk/regelverk for helsesektoren

Følgende beskrives lovverket som gjelder for helsesektoren. Det juridiske rammeverket for informasjonssikkerhet og personvern innen helsevesenet er både omfattende og komplisert. Det eksisterer flere standarder, anbefalinger og føringer som er relevant i forbindelse med endring av en virksomhetsstruktur og organisasjonsstruktur [60]. En endring av IKT-infrastruktur medfører ofte en endring av trusselbildet og risiko. Enten som følge av at informasjon kommuniseres på andre måter, i nye kanaler, eller at flere personer får tilgang til mer informasjon. Ved endring av IKT-infrastruktur bør alle berørte faktorer vurderes. KITH [60] beskriver at «Innen helsevesenet er virksomheter pålagt å gjennomføre risikovurderinger, samt å gjenta risikovurderingen ved endringer som har betydning for informasjonssikkerheten».
En endring av IKT-infrastrukturen kommer gjerne av at virksomheten ser et potensial til økt effektivisering ved innføring av et IKT-system [8, 12]. I helsesektoren finnes det flere lover, forskrifter og andre forutsetninger som ligger til grunn og gir føringer når et IKT-system skal innføres. Lovene regulerer krav til virksomheten, til systemet og til brukerne av systemet. En vurdering av konsekvensene ved endring i IKT-infrastrukturen og ved innføring av et nytt IKT-system, er en prosess som bør gjøres kontinuerlig i hele innføringsperioden [60]. KITH [60] beskriver at det bør eksempelvis vurderes hvor kritisk IKT-systemet vil bli for virksomheten, om det skal integreres i andre systemer, og hvor strenge krav til sikkerhet systemet vil få.
Samtidig er det lovpålagt at alle bedrifter, organisasjoner og virksomheter som behandler personopplysninger har dokumentert sikkerheten i informasjonssystemet, og at virksomheten har organisatoriske rutiner og prosedyrer for å ivareta tilstrekkelig sikkerhet. Organisasjonen og bedriften skal også ha utført risikoanalyse og utarbeidet rutiner for systemrevisjoner, vedlikehold og versjonskontroll [61, 62, 15]. Innen helsesektoren er det også viktig å være bevisst på at lover som er som er av mer spesialisert karakter går

foran andre lover. Eksempelvis at helseregisterloven går foran personopplysningsloven men begge er gjeldene.

Sikkerhetsaspekter identifisert i lovverket

Følgende elementer er identifisert i forhold til forskrifter, regelverk og lovverk (se vedlegg A):

1. Konfidensialitet, beskyttelse mot innsyn fra uvedkommende, kun de som er autorisert til innsyn skal ha innsyn.
2. Tilgjengelighet, sikring av at tilstrekkelige og relevante opplysninger er til stede og er tilgjengelige når det er behov for det.
3. Integritet, beskyttelse mot utilsiktet og uautorisert endring av informasjonen, dataen eller systemet.
4. Kvalitet, sikkerhet om at informasjonen innehar den nødvendige kvaliteten slik at informasjonen ikke fører til misvisenhet.
5. Sporbarhet, endringer som er gjort skal kunne spores tilbake til en person.
6. Ikke-fornekting, personer som har gjort endringer skal ikke kunne nekte for dette i ettertid.

Det fremkommer av Helseregisterloven og Helseforetaksloven at pasientinformasjon eller EPJ ikke fritt kan deles mellom flere helseforetak [15, 5, 16]. Dette setter derfor restriksjoner for tilgang til en felles EPJ-løsning og tilgang til informasjon på tvers av helseforetak. Men dersom et helseforetak regnes for å være databehandlingsansvarlig, vil helseopplysninger kunne gjøres tilgjengelig mellom institusjonene i det samme helseforetaket «i den grad dette er nødvendig for vedkommendes arbeid og i samsvar med gjeldende bestemmelser om taushetsplikt» ifølge helseregisterloven § 13 siste setning [15]. SHDir gjør følgende tolkninger: «Et felles pasientjournalsystem innenfor en sikker sone, og med tilstrekkelig systemtekniske sperrer (autorisert tilgang, og med avskilte pc-er og printere i ulike enheter) kan på visse premisser være mulig. En slik løsning må ivareta informasjonssikkerheten og taushetsplikten»[1]. Lovene er identifisert ut i fra [63, 26], samt beskrivelse ved virkeområde [64, 22, 17, 18, 19, 20, 21].

4.3.1 Forskjell på helsesektor og annen sektor

For en alminnelig bedrift vil det ikke være nødvendig med så strenge krav til sikring av informasjon som helsesektoren setter til helseforetakene. Alminnelig bedrifter som behandler sensitive opplysninger, har krav om å etterleve personopplysningsloven og forskrift til personopplysningsloven. Et helseforetak har et langt større og mer omfattende lovverk å forholde seg til. Derfor stilles det forskjellige kriterier til hva som er akseptabel risiko i helsesektoren og i forhold andre sektorer. Det vil sannsynligvis være svært kritisk om det skulle oppstå brudd på tilgjengelighet, integritet og konfidensialitet innen helsesektoren enn annen sektor. Tap av liv, feilmedisinering og feildiagnostisering er mulige hendelser om konfidensialitet, tilgjengelighet, kvalitet, integritet og sporbarhet ikke er ivaretatt. Samtidig er begrepet tilgjengelighet sentralt og viktig. Pasientinformasjon og systemer som behandler pasientinformasjon må til enhver tid være tilgjengelig. Bedrifter og organisasjoner i andre sektorer kan til en viss grad akseptere at systemer er utilgjen-

[1] Dette brevet er innen helsesektoren omtalt som «Helse-vest brevet». Brev fra Sosial- og Helsedirektoratet til Helse Vest 13.05.2005: «Tilgang til pasientinformasjon i helseforetak og på tvers av helseforetak».

gelig i en kortere periode. Og som sannsynligvis kun medfører tap av fortjeneste eller tap av markedsanseelse. Helsesektoren kan derimot ikke akseptere slike tilfeller. Vektlegging av de ulike sikkerhetselementene i lovverket, er imidlertid noe annerledes for en kommunikasjonsløsning enn for selve informasjonsbehandlingen i sluttsystemene.

5 Metoder for ROS-analyse

I dette kapitlet beskrives ulike typer metoder for ROS-analyse. Det er beskrevet noen utvalgte metoder med ulik tilnærming, som er funnet relevant til ROS-analyse. Metodene som er identifisert, er funnet både i kvalitativ, kvantitativ og sjekkliste-basert kategori. Avslutningsvis er det beskrevet en begrunnelse for våre valg av metoder.

5.1 Metoder

Keong [11] oppsummerer flere forskjellige typer risiko- og sårbarhetsmetoder, og kategoriserer metodene i tre forskjellige kategorier: trebaserte, kvantitative og kvalitative. Keong beskriver at metodene FTA (Failure Tree Analysis), ETA (Event Tree Analysis), CCA (Cause- Consequence Analysis), MORT (Management Oversight and Risk Tree) og «SMORT» (Safety Management Organization Review Technique) primært begrenser seg til statisk og logisk modellering av tilfeldige/ulykkes baserte scenarier. Det beskrives at ETA og FTA er de mest benyttede metodene innen risiko- og pålitelighetsanalyse [65]. FTA (Fault Tree Analysis) [66] er en metode som kan benyttes for å påvise pålitelighet i et system. Metoden baserer seg på deduktiv logikk og et logisk diagram som viser relasjonen mellom systemsammenbrudd og komponentsammenbrudd. Diagrammet kan fungere som en beskrivelse over en uønsket hendelse i et system og årsakene til de uønskede hendelsene. Metoden tar forbehold om at årsakene kan både være menneskelige, miljøfaktorer og feilhandlinger. Det vil si at metoden kan benyttes i flere forskjellige perspektiver enn kun i et system-teknisk. Det beskrives også av Rausand [65] at metoden kan benyttes kvantitativ og kvalitativ tilnærming, eller ved en kombinasjon. Keong [11] påpeker videre at det kan være vanskelig å eksplisitt modellere og kvantifisere tilfeller hvor mennesker er involvert. CCA er også en tilnærmet lik metode som FTA. CCA som er to-delt ved hendelse og konsekvens. Teknikken beskrives som en «bottom-up» deduktiv metode. Metoden har et fokus på safety, og er komplementær til andre teknikker som FTA og FMEAC. Metoden er ofte beskrevet som en utvidet treanalyse [11].

Keong diskuterer også tre kvalitative metoder, HAZOP(Hazard and Operability Analysis) [65, 11], FMEA/FMECA (Failure Modes and Effects Analysis) [11], Preliminary Risk Analysis [11]. Følgende beskrives metodene kort. HAZOP [65, 11] er en metode som kan benyttes som et forstudie eller som en fullstendig risikoanalyse. Metoden er ofte benyttet i sammenheng med prosjektering av prosessanlegg for å identifisere kritiske deler/komponenter i prosesser. HAZOP er en formell, systematisk og har grunnleggende mål med å avdekke sikkerhetsmessige eller operasjonelle problemer. FMEA/FMECA [11, 65] er metoder som kan benyttes ved feilmodi og feileffektanalyse. Dette er opprinnelig to forskjellige metoder, men blir som oftest beskrevet som en metode. Rausand [65] beskriver at metodene ofte har en flytende overgang i hverandre. FMEA/FMECA er beskrevet som en systematisk metode for å analysere feil i tekniske systemer, og benyttes primært i design-fasen av et system. FMEA/FMECA defineres som en kvalitativ metode, men innehar ofte et sett av kvantitative elementer ved frekvens og sannsynlighet for feilmodene, og rangering av konsekvensene i feileffektene [65]. Metoden «Preliminary Risk Analysis» er beskrevet som en systematisk tilnærming basert på HAZOP, som har fokus på

analysering av uhell og hendelser som kan oppstå i operasjonell modus. Bruk av metoden genererer en kvalitativ beskrivelse av potensielle problemer som er definert ved en kvanititativ estimering [11]. Ved en oppsummering beskrives det at metoden bør benyttes av personell som har kjennskap til maskinvare og maskinutstyr. Det beskrives avslutningsvis at metodene kan både bli benyttet i både en design-fase og i en operasjonell-fase. Keong [11] konkluderer avsluttningsvis med at kvalitative metoder mangler muligheten til å se avhengigheten mellom hendelser, men er bedre til å identifisere farer og risiko/sammenbrudd i et system enn det de trebaserte metodene.

KITHs metode, presentert av Aksnes, Vestad og Grøtan [10] er en enkel metode for risikoanalyse. Metoden kan benyttes for å identifisere trusler mot en organisasjon eller et informasjonssystem. Metoden [10] baserer seg på vurderinger av sannsynlighet, konsekvens og risiko, og gir råd om hvordan arbeidet kan organiseres. Metoden er skjemabasert og egner seg på områder hvor det er fokus tilsiktede angrep(security). Aksnes, Vestad og Grøtan beskriver og gir råd om hvordan arbeidet med risikoanalyse kan organiseres. De diskuterer også hvordan akseptkriterier benyttes for å avgjøre hvilken risiko organisasjonen er villig til å utsette seg for.

Skavland og Jakobsen har utarbeidet en metode ved navn ROSS [29](Metoden er senere blitt videreutviklet [27]). ROSS er en metode for analyse av objekt- og informasjonssikkerhet. Det beskrives at metoden er generell, og at det er først og fremst tilsiktede handlinger(security) metoden omhandler. Det henvises derfor til analyse som er under safety til bruk av andre metoder tilpasset safety-området. Som KITH sin metode, er ROSS-metoden skjema basert. Metoden er delt inn i separate trinn og drives fram av utfylling av fire forskjellige skjemaer. Det er også beskrevet en fremgangsmåte for utfylling av skjemaene, og en anbefaling for bruk av metoden. Metoden krever visse kunnskaper om sikkerhetsrelatert arbeid og sikkerhetsterminologi, og derfor vil det være virksomhetens sikkerhetspersonell som har best forutsetninger for å benytte metoden. Metoden beskriver risiko, basert på sannsynligheten for, og konsekvensen av de forskjellige handlingsmønstrene.

NSM-ROS2004 [3] er en videreutvikling av ROSS beskrevet overfor. Denne versjonen skiller derimot ikke eksplisitt mellom de tradisjonelle områdene safety og security. Dette begrunnes med at det er at flere trusler påvirker de to fagområdene gjensidig, og det underbygges videre med at «Hensikten med å gjennomføre en analyse vil bl.a være å finne sårbarhetene og iverksette tiltak for disse, uavhengig av om de er forårsaket av en tilfeldig eller tilsiktet handling». En annen forskjell fra de tidligere metodegenerasjonene [27, 29], er at denne metoden inneholder en veiledning for fremgangsmåte og beskrivelse av risikohåndtering. Som de foregående generasjonene, er denne også skjemabasert og drives frem av utfylling av skjemaer.

CORAS [67] er en metode som er rettet mot analyse av risiko. Metoden er bygget opp av flere verktøyer og metamodeller for beskrivelse av risiko, trusler og tiltak. Metoden gir mulighet for å evaluere risiko opp mot hverandre. CORAS har tidligere blitt benyttet til flere lignende case studier som denne oppgaven skisserer [68]. Blant annet er metoden benyttet på Kreta i utviklingen av HYGEIAnet [69] og ved BOJ (Bild och Journal) i

Sverige. Resultater og erfaringer ved CORAS er beskrevet i [69]. CORAS har utviklet metoder og objektorientert modellering for semi-formelle spesifikasjoner, det vil si at krav og ulike løsninger uttrykkes ved hjelp av et ikke-naturlig språk med definert semantikk eller syntaks. Et eksempel på et slikt språk er modelleringsspråket Unified Modeling Language(UML) [70]. UML kombineres deretter med tradisjonelle metoder for risikoanalyse.

Cobit [71] er en internasjonalt anerkjent metode med betegnelsen CobiT for «Control Objectives for Information and Related Technology». Cobit har en en prosess orientert tenkning, som baserer seg på forutsetningen om at virksomheten må ha etablert en definert prosess for å kunne ivareta de ulike IKT-oppgavene. Cobit deler IKT-prosesser inn i 4 hovedområder:

- «Planlegging og organisering» (11 forskjellige prosesser)
- «Anskaffelse og implementering» (6 forskjellige prosesser)
- «Leveranse og støtte» (13 forskjellige prosesser)
- «Overvåkning» (4 forskjellige prosesser)

Disse 4 hovedområdene dekker til sammen 34 IKT-prosesser og omfatter hele IKT-området til en virksomhet. Metoden krever en investering i form av lisens, men Kredittilsynet [72] har laget en alternativ versjon som er kostnadsfri.

Kredittilsynet's variant av metoden er primært er utviklet og tilpasset som et hjelpemiddel for gjennomføringen av tilsyn med finansnæringen. Kredittilsynet [72] har tatt utgangspunkt i metoden Cobit, og utviklet ca 180 kontrollspørsmål som er knyttet til den enkelte prosess på laveste nivå. Disse spørsmålene er relatert til den enkelte IKT-prosess under de 34 IKT-prosessene som er definert i metoden. Det beskrives ved Kredittilsynet at «Metoden baserer seg på risikotenkning og at det er de forretningsmessige mål som i stor grad vil styre omfanget av det sikkerhetsregime som foretaket skal ha etablert» [72].

5.2 Valg av metoder for ROS-analyse

I følgende kapitler beskrives våre valg av metode for gjennomføring av ROS-analyse.

5.2.1 Første ROS-analyse

Følgende beskriver en fremgangsmåte for identifikasjon av metode for ROS-analyse. Metodevalget er basert på en betaversjon av av av rammeverket til BAS5. Figur 5 viser skisse av rammeverket til BAS5. Det ble på forhånd utarbeidet et forprosjekt med identifisering av problemstilling, problemområde og informasjonsbearbeiding. Samtidig ble lovverket studert for identifikasjon av krav som stilles innen helsesektoren. Innledningsvis i forprosjektet ble systemet og tilkobling til andre systemer studert og vurdert, både i forhold til hvor kritisk systemet er for organisasjonen, og i forhold til tap av liv og helse. Omfanget av systemet ble også vurdert i forhold til metodene. Komponenter/delsystemer som var av kritisk funksjonalitet ble studert og gjennomgått.

Valg av hovedtilnærming

På bakgrunn av resultatet fra forprosjektet og begrensninger i tid og ressurser, ble det tatt en avgjørelse å velge en metode av kvalitativ tilnærming. Begrunnelsen for dette var at vi så det som nødvendig med en dypere og mer helhetlig tilnærming til analyse av systemet. Begrunnelsen er også basert på en vurdering og analyse av de kritiske område-

ne i systemet. Eksempelvis ulike scenarier i brukersituasjoner og kritikalitet til sentrale komponenter og systemdeler. Som nevnt, tar den valgte tilnærmingen ofte utgangspunkt i de enkelte objekter og uønskede hendelser. Forprosjektet resulterte i identifikasjon av kritiske objekter og flere uønskede hendelser på et relativt overordnet nivå. De kritiske objektene ble grunnlaget for analysen, og de uønskede hendelsene ble vurdert i forhold til påvirkning på de kritiske objektene.

Sjekkliste-metode og kvantitative tilnærminger, ble vurdert for ikke å være egnet i første ROS-analyse. Begrunnelsen for dette er at sjekklister ofte beskrives som et revisjonsverktøy. Dette vil ofte medføre resultater som dannes på bakgrunn av «manglende tiltak», og derfor ikke være egnet i forhold til vårt fokus ved overgang til et fremtidig system [48]. Ved kvantitativ tilnærming, er metodene ofte avhengig av et stort og godt statistisk materiale [48]. Som beskrevet i kapitel 3.4.2 «Risikovurdering», er det ofte vanskelig å beskrive og kvantisere en frekvens av tilsiktede handlinger. Det ble derfor tatt en avgjørelse på å ikke velge en kvantitativ metode i første ROS-analysen.

De metodene som ble funnet relevante innen kategorien «kvalitativ tilnærming» ble så studert og vurdert i forhold til krav som stilles vedrørende tid, ulike andre ressurser og omfang/dekningsgrad. Valget av metode ble så utført i samråd med ressurspersoner ved FFI. Følgende beskrives valg av metode for første ROS-analyse.

Begrunnelse for metode ved første ROS-analyse

Som beskrevet i forrige kapitel, ble metoden valgt innen kategorien kvalitativ tilnærming. Det ble ved første runde ROS-analyse, valgt å benytte den skjemabaserte metoden NSM-ROS2004 [3] utviklet av Nasjonal Sikkerhetsmyndighet og NTNU. Metoden ble funnet mest egnet både ved begrensinger i tid og tilgjengelig resurser, samt hvor relevant metoden var i forhold til definert problemstilling. Ytterligere begrunnelse for valg av metode, er at denne metoden ikke skiller eksplisitt mellom de tradisjonelle fagområdene safety og security. I samtaler og diskusjon med helseforetaket, kom det frem at det vil være like kritisk for helseforetaket å finne sårbarheter, og iverksette tiltak for disse, uavhengig av om de er forårsaket av en tilfeldig eller tilsiktet handling[1]. Det skal også nevnes at denne metoden har en grundig veiledning og beskrivelse for gjennomføring av ROS-analyse.

5.2.2 Andre ROS-analyse

I dette kapitlet beskrives vårt valg av tilnærming og valg av metode for andre ROS-analyse.

Begrunnelse for tilnærming ved andre ROS-analyse

Det beskrives at «For de fleste komplekse systemer vil det være mulig med bakgrunn i erfaringer å anslå en repetisjonsrate eller sviktintensitet som grunnlag for et sannsynlighetsmål. Det finnes også tyngre teoretiske metoder som kan benyttes der den historiske sviktintensiteten er svært lav. Dette gjør det mulig gjennom tiltak kontinuerlig å avstemme et systems sårbarhet til den til enhver tids gjeldene trusselsituasjonen, gitt at en rår over tilstrekkelige gode metoder for risikoanalyse» [73]. Det beskrives også av Rausand, at det ofte kan det være effektivt og hensiktsmessig å visualisere sannsynligheter for et sikkerhetsbrudd eller systemfeil i et system [65]. FTA er en systematisk metode som både kan benyttes kvantitativt, kvalitativt, eller som en kombinasjon. FTA har til hensikt å evaluere risikoer, for deretter å definere den beste strategien for å beskytte systemet [65].

[1] Møte med det aktuelle helseforetaket, 23.11.2005

Risikofaktorer som er av betydning for systemet kan eksempelvis være miljø, menneskelige eller normale-situasjoner. Det er derfor ikke beskrevet noen begrensninger i metoden for å visualisere systemet. Det er også mulig å ta forbehold om utenforstående faktorer som er av betydning. Metoden er bekrevet som en dybdeanalyse, og Rausand [65] beskriver at det er essensielt og viktig med kjennskap til systemet som skal analyseres. Ved å benytte en slik metode kan vi forstå tilsynelatende enkle problemer i et helt annet perspektiv enn de rent kvalitative metodene [3, 27, 10], som ofte er preget av et relativt «anslag» ved fastsettelse av sannsynlighet og konsekvens.

Noe av problemet med ROS-analyse er at vurderingene ofte tvinges inn det samme metodiske rammeverk fra metode til metode[2]. Dette betyr at en i praksis vurderer en annen form for sannsynlighet og en annen form for konsekvens i alle analyser[3]. For å gå vekk fra denne typen fallgruve har vi valgt å benytte en annen type metode som baserer seg på andre vurderinger av konsekvens og sannsynlighet. FTA er en metode som kan baseres på større grad av probabilistiske vurderinger av sannynlighet og konsekvens. Moberg [4] har i sitt arbeid utført et forsøk med å analysere et informasjonsssystem ved bruk av en trebasert metode. Metoden som benyttes er i utgangspunktet en metode som identifiserer ulike angrepsmåter på et system. Trussel og angriper er identifisert og sett i forhold til angrepsveier. Metoden som Moberg har benyttet vektlegger ikke forskjellen på områdene safety og security, men har kun fokus på angrepsveier og hva som skal til for at en angriper lykkes. Det presenteres også av Helmer m fl. [74] en lignende tilnærming ved bruk av FTA i IDS-systemer.

Begrunnelse for metode ved andre ROS-analyse

Ved å benytte en FTA tilnærming, ønsker vi å visualisere sårbarheter og sammenheng mellom hendelse og konsekvens. Men for å dekke nødvendige deler av systemet, ser vi det som hensiktsmessig å gjøre noen endringer med metoden. FTA er en metode som primært benyttes innen systempålitelighet. To andre trebaserte metoder som kan benyttes er Angrepstre og Trusseltre. Amoroso [75] beskriver trusseltre som en metode som strukturerer identifiserte trusler ved et system i en trestruktur. Truslene blir gradvis inndelt i kategorier. Avslutningsvis vil analytikeren ende opp med et trusseltre hvor bladnodene beskriver ulike trusler ved systemet. Problemet ved trusseltre er å beholde fokus på trusler og ikke gå over til å beskrive angrep.
Schneier [76] beskriver og forklarer i sitt arbeid, hensikt og bruk av angrepstre. Angrepstre har lik tilnærming som Trusseltre, men forskjellen er at angrepstre skisserer veier for ulike angrep på et system. Metoden er også like formell som metoden trusseltre. Ved angrepstre kan analytikeren beskrive angrepsveier en angriper kan gå for å oppnå formålet med angrepet. Det kan også tillegges verdier til bladnodene. Verdiene kan så propageres opp til topphendelsen i treet, som kan gi et anslag på hvilke kostnader det ligger i å utføre angrepet.

Ved å kombinere metoden FTA, med en tankegang som benyttes i angrepstre og trusseltre, mener vi å dekke det som er nødvendig for å oppnå et resultat som kan visualisere både trusler, risiko, sårbarheter og sammenhengen mellom feilkilder. Vi ønsker å benytte FTA som en kombinasjon av kvantitativ og kvalitativ tilnærming. Det beskrives av

[2]Håvard Fridheim ved FFI. 22.02.2006
[3]Håvard Fridheim ved FFI. 22.02.2006

Rausand [65] og Aven [37] at metoden gir et klart og tydelig bilde over hvilke kombinasjoner systemet som kan lede til en uønsket hendelse. Metoden er også beskrevet som enkel å forklare til personer som ikke har kjennskap til metoden [65]. Ved bruk av metoden tvinges deltakerne i prosjektet til å forstå systemet fullt ut [65]. Dette vil også kunne bidra til å identifisere svakheter og feil i systemet i et bredere perspektiv. Både Rausand [65] og Sutton [77] beskriver at ressursbehovet og arbeidsmengden for å benytte metoden i store systemer er omfattende. FTA på et detaljert nivå av et mindre system vil anslagsvis ta 4-10 dager, mens en detaljert analyse av et stort system, kan ta opptil flere uker. Derfor kan det kan være hensiktsmessig å ta utgangspunkt i systemet på et relativt overordnet nivå, og generalisere systemet og deler av det[4]. Sutton beskriver i [77] noen utfordringer ved bruk av metoden, blant annet at metoden kan føre til at analytikeren overser større feilkilder ved å legge seg på et detaljert nivå. FTA legger således ikke begrensninger på faktorer som har betydning for oppbygning av feiltreet. Som for eksempel ulike menneskelige eller miljømessige påvirkninger. Metoden skiller dessuten ikke eksplisitt mellom «safety» og «security».

[4]Håvard Fridheim ved FFI. 22.02.2006

6 Eksperimentet

I dette kapitlet beskrives eksperimentet som vi har utført. Innledningsvis identifiseres verdiene i systemet/virksomheten. Dette gir grunnlag for omfanget av analysen. Samtidig gir dette en oversikt over de kritiske delene av systemet, og forenkler og effektiviserer arbeidet med å identifisere trusler og risiko [3].

6.1 Definering av analyse og omfang

Det å definere omfang og detaljeringsgrad for analysen er beskrevet som et vanskelig punkt ved ROS-analyse [3]. Det beskrives ofte at arbeidet ofte må tilpasses det risiko- og trusselbildet som virksomheten står overfor, samtidig må en også ta høyde for de organisatoriske, tekniske og menneskelige forholdene.
I metoden NSM-ROS2004 [3] beskrives det at det ofte vil være en avhengighet mellom flere av faktorene, for eksempel «størrelse på virksomheten (antall ansatte), risikonivå i virksomheten (verdifulle objekter, sensitiv informasjon), og grad av kompleksitet (mange lokasjoner, komplekse IKT-systemer osv.)».
Vi valgte en avgrensning basert på virksomhetens størrelse, systemets funksjonalitet, ytre grenser, systemets beliggenhet og grad av kompleksitet. For å ha et riktig fokus på informasjonssikkerhet og den definerte problemstillingen, ble det tatt utgangspunkt i begrepene som ble identifisert i lovverket, samt krav og retningslinjer som stilles innen helsesektoren. Geografisk beliggenhet og størrelse på virksomheten gjorde det nødvendig å generalisere resultatet av studiet av en mindre del til å gjelde hele helseforetaket. I diskusjon med helseforetaket, fremkommer det at en lokasjons infrastruktur og oppbygging er generaliserbar til å gjelde alle lokasjoner. Det ble tatt en avgjørelse om å legge seg på en detaljeringsgrad mellom organisatorisk og teknisk, samtidig som det ble bestemt å dekke alle berørte deler i kommunikasjonskanalen. Graden av kompleksitet og hvor uoversiktlig systemet er, legger begrensninger på analysen. Det ble derfor valgt å avgrense analysen til å gjelde all infrastruktur som inngår i EPJ-systemet med overliggende EPJ-applikasjon.

6.2 Gjennomføring av første ROS-analyse

Dette kapitlet gir en beskrivelse av hvordan første ROS-analyse i eksperimentet ble gjennomført. Kapitlet beskriver både arbeid som er gjort på forhånd av ROS-analysen, og gjennomføring av selve ROS-møtet og analysen.

6.2.1 Metoden NSM-ROS2004

Metoden «NSM-ROS2004» beskriver en styringssløyfe for gjennomføring av risikohåndtering i virksomheten. ROS-analysen ble gjennomført i stegene beskrevet i figur 10 under «Planlegging og organisering» og «Gjennomføring av ROS-analyse». Den presenterte modellen er skissert som en kontinuerlig prosess delt inn i fire mindre trinn, se figur 10. Med vårt fokus og begrensning, var det tilstrekkelig å gjennomføre steg 1 og 2 i figur 10.

6.2.2 Planlegging og organisering

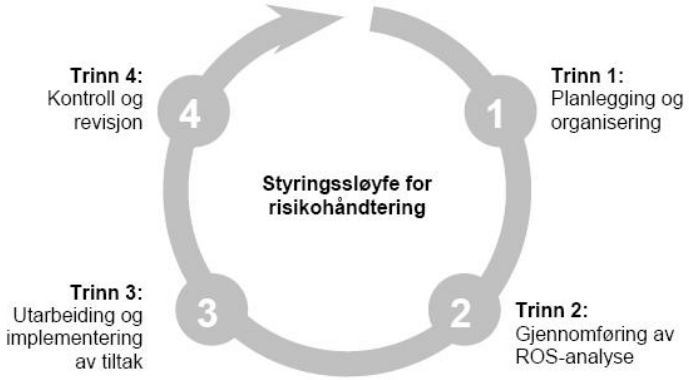
Det beskrives i NSM-ROS2004 [3] at «En risiko- og sårbarhetsanalyse kan organiseres som et prosjekt, og gjennomføres i henhold til en prosjektplan». Det ble derfor valgt å gjennomføre og organisere første ROS-analyse som et prosjekt. Vår begrunnelsen for å gjøre dette valget, er at vi oppfatter det slik at det kan være lettere å strukturere et slikt arbeidet etter en prosjektmodell [78], samtidig som vi ønsket å følge den valgte metoden.

Et prosjekt er ofte karakterisert ved følgende trekk[78]:

- Det er ofte en engangsoppgave som skal utføres.
- Har et bestemt formål og skal lede frem til et resultat.
- Oppgaven er begrenset i tid og har begrensende ressurser.
- Oppgaven utføres oftest sammen med flere personer fra forskjellige fagområder, hvor personene har andre arbeidsoppgaver.
- Arbeidsformen krever sammensetning fra flere ulike fagområder og ressurser.

Det ble definert og satt sammen en referansegruppe bestående av ressurspersoner ved helseforetaket. Referansegruppen ble bevisst satt sammen av personer som hadde relevant fagkunnskap og IKT-kompentanse på de ulike områdene. Sammensetningen av prosjektgruppe er ofte beskrevet som avgjørende og påvirkende for hvilke resultater som foreligger etter endt ROS-analyse [3] [67] [10] og [27].

I veiledning til metoden [3] beskrives det at «Virksomheten må kartlegge de trusler som finnes, både internt og eksternt, slik at virksomheten kan iverksette tiltak for å redusere trusler med uakseptabel risiko». Samtidig beskrives det at «dette forutsetter at det finnes kriterier å styre i forhold til: Det må være mulig å ha holdepunkter for å si når en risiko øker ut over et nivå som på forhånd er definert som akseptabelt». Det ble her valgt å benytte de akseptkriteriene som helseforetaket har definert. Det ble således valgt å konvertere de verdiene som metoden NSM-ROS2004 presenterer, til akseptkriteriene som er definert av helseforetaket (Se vedlegg C). Vår begrunnelse for dette valget, er at metoden poengterer at det å fastlegge et nivå for hvilken risiko en virksomhet kan akseptere er en



Figur 10: Styringssløyfe hentet fra «NSM-ROS2004».

beslutning som bør tas av virksomhetens leder eller ledelse. De akseptkriteriene som vi valgte å benytte er definert av ledelsen ved helseforetaket.

6.2.3 Identifikasjon av verdier

I dette delkapitlet beskrives kartlegging og identifisering av virksomhetens verdier. Begrepet «verdi» er en beskrivelse av det objektet eller den informasjonen som virksomheten eller organisasjonen må sikre konfidensialitet, tilgjengelighet eller integritet for [3]. Hensikten med å identifisere kritiske verdier for virksomheten blir beskrevet som en mulighet for å kunne utelate deler som har lav verdi for analysen, noe som kan effektivisere og samtidig begrense analysen. Informasjonen som har en sikkerhetsverdi og følgelig er skjermingsverdig, vil aldri være statisk over tid [79]. Krav til beskyttelse av kritisk informasjonen vil forandrer seg i takt med organisasjonens utvikling. Samtidig vil det bestandig være et tilsig og frafall av informasjon og nye objekter som har et beskyttelsesbehov. Det beskrives at «Endringer i våre omgivelser, eksempelvis den overordnede sikkerhetspolitiske, teknologiske, samfunnsmessige og økonomiske utviklingen, vil løpende påvirke hva vi ønsker å beskytte» [79]. Samtidig vil det under en utvikling være viktig å kjenne til hvilke faktorer som stadig påvirker en bedrifts- og organisasjons risikobilde og skjermingsverdige verdier.

Følgende beskriver de verdier som ble funnet som kritiske ved helseforetaket i denne ROS-analysen. Fra helseforetaket sitt synspunkt, er den kritiske verdien sikring av «pasientjournal og pasientsystemet», men for at systemet skal bli enklere å modellere er det brutt ned i ytterligere definerbare og konkrete deler. Verdiene som ble identifisert, er funnet i samarbeid med ressurspersoner ved helseforetaket. Verdiene ble forsøkt definert i forhold til inndeling i funksjonalitetsområder ved: «bruker og pasient», «infrastruktur» og «drift, support og maskinvare». De forskjellige områdene har forskjellige synspunkter på verdier avhengig av ståstedet. Eksempelvis har en pasient et syn på hva som har en verdi, og en person som arbeider ved drift et annet. Verdiene er forsøkt sett fra helseforetakets side og fra et funksjonalitetsperspektiv, og ikke et stillingsmessig perspektiv.

Beskrivelse av de 3 områdene

Området «bruker og pasient» er beskrevet ved de personene som skal nyttegjøre seg av foretningsfunksjonene som virksomheten tilbyr. I dette tilfellet, er det «pasientbehandling». Området er identifisert som en verdi for virksomheten, beskrevet ved den tillit og troverdighet en pasient har til helseforetaket under behandling. Helseforetaket skal tilby rettmessig og riktig behandling av pasientene, samt sikring og oppbevaring av pasientinformasjonen. Dette innebærer riktig og forsvarlig sikring av informasjonen, samt etterlevelse av lovverk. Tap av verdien er karakterisert som uakseptabel, og som svært kritisk og avgjørende for helseforetakets virksomhet.

Området «infrastruktur» vil delvis overlappe punktet over under lovverket. «Infrastruktur» er ansett som en kritisk verdi for virksomhetens daglige drift. Virksomheten er avhengig av flere forskjellige faktorer i sin daglige drift. Eksempeler er kommunikasjon, andre leverandører osv. Området er derfor definert som en kritisk verdi for å kunne tilby rettmessig og effektiv behandling. Sett i forhold til punktet over, som er definert ved et tillitsforhold mellom helseforetaket og pasienten. Det er derfor store krav til eksterne leverandører, maskinvare og levering av andre tjenester som inngår i virksomheten.

Det siste området «drift, support og maskinvare», er definert som det utstyret, menneskelige ressurser og kompetanse, som kreves for å sikre optimal drift, samt vedlikehold av helseforetakets daglige funksjonalitet. Området er beskrevet som en verdi for helseforetaket, for at helseforetaket skal kunne opprettholde tilstrekkkelig kvalitet og effektivitet i pasientbehandlingen.

6.2.4 Identifikasjon av trusler

I forkant av ROS-analysen kan det ofte være fornuftig å identifisere mulige kilder som kan utgjøre en risiko for systemet som skal analyseres [3]. Hensikten med en slik gjennomgang er å få oversikt over trusselbildet virksomheten står overfor. For å følge valgt metode, ble det på forhånd gjort en overordnet gjennomgang av ISO/IEC 17799 [25] og IT-Grundschutz Manual 2004(Threats Catalogue Force Majeure) [80]. Dette for å gi et bilde og en oversikt over mulige risikoer som kunne identifiseres. I NSM-ROS2004 beskrives det at hensikten med å gjennomføre et slikt arbeid, er å finne frem til underliggende prosesser, faktorer, elementer og indikatorer som kan føre til hendelse av trusler og som kan medføre konsekvenser for helseforetaket. Det skal også poengteres at det ved en slik type tilnærming, ikke er mulig å definere objektiv eller reell risiko [3].

6.2.5 Modellering

Det ble i «planlegging- og organiseringsfasen» laget en modell av systemet som ble benyttet under ROS-møtet. Det beskrives ved NSM-ROS2004 [3] at det ved bruk av metoden ofte vil være fornuftig å visualisere systemet ved hjelp av en eller flere representasjonsteknikker. Følgende beskriver og begrunner valg av modelleringsspråk (Modellen og presentasjonen fra første ROS-møte er vedlagt i vedlegg B). Det er identifisert flere forskjellige metoder og typer for modellering av systemet. Eksempel på noen forskjellige metoder kan være «trusselmodellering», «angrepsmodellering», «fiendemodellering» og «protokoll analyse». Men som beskrevet tidligere, (i kapitel 3.7 «Modellering og modelleringsspråk») har de forskjellige modelleringsteknikkene forskjellig tilnærming, avhengig av hvilket fokus som analytikerne ønsker.

Det beskrives ved metoden NSM-ROS2004 [3] følgende muligheter på å visualisere systemet:

- Hierarkisk nedbryting
- Kart over fysisk beliggenhet
- Prosesstegninger
- Organisasjonskart

Basert på identifiserte verdier funnet i casestudiet og i samarbeid med helseforetaket, har vi valgt å følge de retningslinjer, råd og henvisninger som metoden gir. Ønsket var at modelleringen ikke skulle få et feil fokus og la elementer som «fiender» og «angrepsveier» prege resultatet og modelleringen. Samtidig la tilgjengelige ressurser begrensninger på hvilket detaljeringsnivå som kunne bli valgt. Det ble derfor valgt å benytte et modelleringsspråk som i utgangspunktet basert på Unified Modeling Language [70].

Analyseomfanget er først og fremst valgt begrenset til systemets hovedfunksjonalitet. Deretter ble systemet brutt ned og modellert i delområdene: «brukersiden», «infrastruktur og kommunikasjon» og «drift/support/server». Se figur 11 for skisse, og vedlegg B for full modell.

6.2.6 Hvordan ROS-møtet ble gjennomført

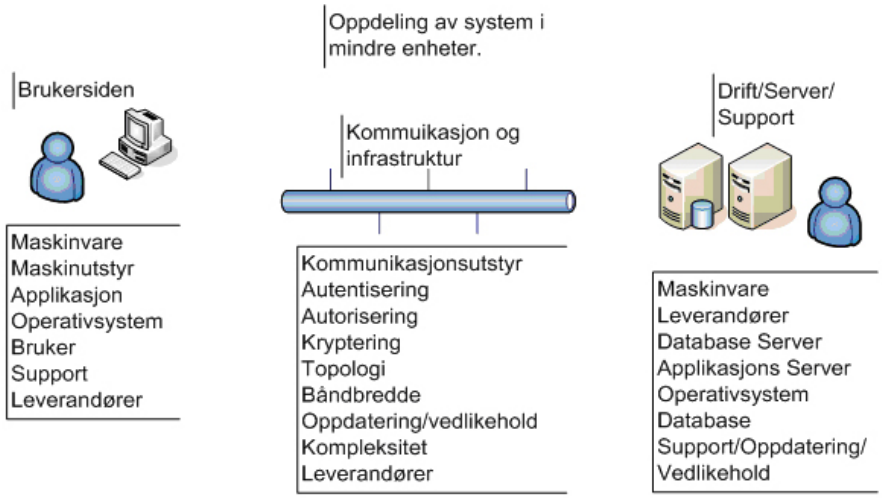
Følgende beskriver de stegene som ble gjennomført i første ROS-analyse. Stegene er skisser i figur 12. Det var vår hensikt å gjennomføre ROS-analysen mest mulig i henhold til valgt metode. Stegene ble gjennomført under selve ROS-møtet. Før ROS-møtet ble det sendt ut innkallelse med informasjon om selve prosjektet, beskrivelse av agenda og valgt metode med veiledning. Dette gjorde det mulig for prosjektdeltakerne å bli kjent med prosjektet og metoden før selve ROS-møtet. I NSM-ROS2004 er det beskrevet at «Arbeidsgruppen/prosjektgruppen bør bestå av personer med kunnskap og erfaring fra arbeid med slike analyser. Arbeidsgruppen bør i tillegg ha nødvendig kjennskap de aktiva og systemer som skal undersøkes» [3]. Alle de innkalte personene hadde kjennskap til gjennomføring av risiko- og sårbarhetsanalyse fra tidligere arbeid, men ikke kjennskap den valgte metoden.

6.2.7 ROS-samlingen

ROS-møtet besto av tre deler,

1. Innledning med presentasjon av prosjektet.
2. ROS-analyse av dagens system.
3. ROS-analyse av fremtidig system.

Innledningsvis ble det foretatt en kort gjennomgang av systemet, tjenesten som systemet leverer, dets omgivelser og funksjonalitet. Deretter ble modellen presentert, med etterfølgende analyse av dagens system. Det ble identifisert kritiske trusler og uønskede hendelser, samt gjort vurderinger basert på en strukturert gjennomgang av presentert modell. Trusselkartleggingen omfattet «hva kan gå galt, hvor, hvorfor og hvordan?». Det ble gjort bevisst valg om å holde et overordnet fokus på de områdene som var viktigst og mest kritisk for helseforetaket. For eksempel at uvedkommende får tilgang til sensitive opplysninger. Gjennomføring av dette punktet er beskrevet som steg 2.1. i figur 12. Det

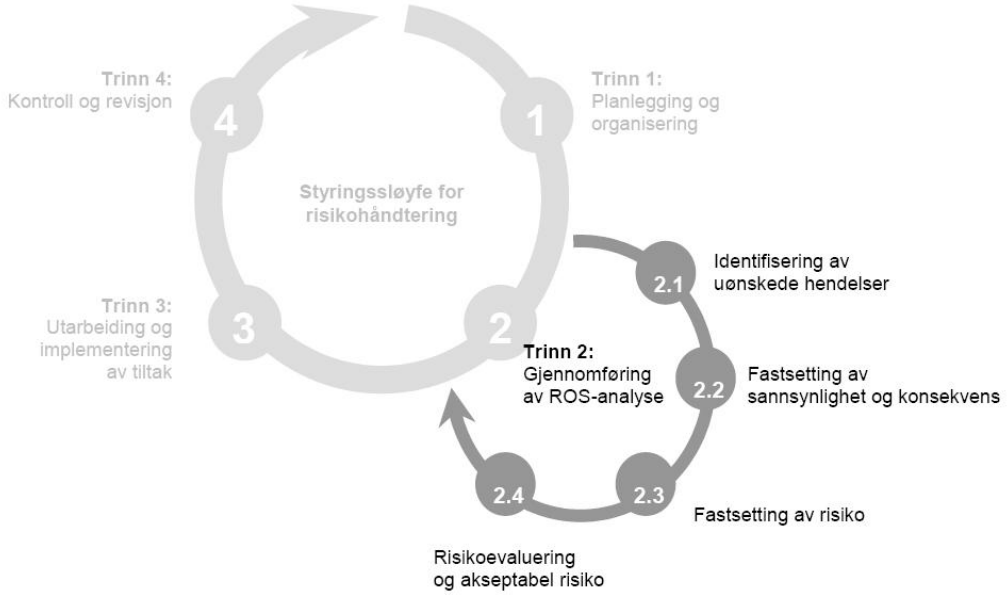


Figur 11: Oppdeling av systemet.

ble kartlagt et variert antall trusler i hver av kategoriene «brukersiden», «kommunikasjon og infrastruktur», og «drift/support/server». Deretter ble det diskutert og vurdert hvor kritisk truslene var for systemet. Prosjektgruppa drøftet at en trussel måtte berør et større antall brukere for å bli kategorisert som kritisk. Etter gjennomført trusselkartlegging, ble det valgt ut et antall trusler, basert på en rangering innad i hver kategori (ved modellen). Trusler som ble kategorisert som kritiske for virksomheten, ble drøftet i en strukturert gjennomgang, og deretter ble det definert et konsekvensnivå og sannsynlighetsnivå for hver av truslene (se figur 13 for skisse av risikomatrise. Tallene identifiserer 5 trusler funnet i en kategori ved modellen). Dette steget er skissert i figur 12 ved steg 2.2. Definisjon av konsekvensnivå og sannsynlighetsnivå ledet frem til et totalt risikonivå for hver av truslene. Dette er skissert som steg 2.3. i figur 12. Etter analyse av dagens system, ble de samme stegene(steg 2.1, 2.2 og 2.3 i figur 12) gjennomført på et fremtidig system. Deretter ble sluttresultatene i begge analysene evaluert og vurdert opp mot hverandre i en og samme risikomatrise, se figur 13.

6.2.8 Etter ROS-samlingen

I etterkant av ROS-samlingen ble det utarbeidet en rapport som beskriver og evaluerer identifiserte trusler og sårbarheter. Hver trussel og sårbarhet ble grundig vurdert og evaluert ved hjelp av en todimensjonal risikomatrise (se figur 13). Vurderingene av dimensjonene konsekvens og sannsynlighet ledet frem til en total risiko. Avslutningsvis ble all risiko beskrevet i eksisterende og fremtidig system, illustrert i to risikomatriser. Sammenligningen av disse risikomatrisne ga mulighet for å kunne illustrere beliggenhet til risikoene ved begge løsningene. Resultatet illustrerte raskt at det var identifisert større konsekvenser og større sannsynlighet for at en risiko skulle inntreffe i en sentralisert løsning. Vår erfaring er at sammensetningen av referansegruppa preger resultatet. Vi mener også at resultatet lar seg prege optimal løsning for aktuell lokasjon, og således kanskje



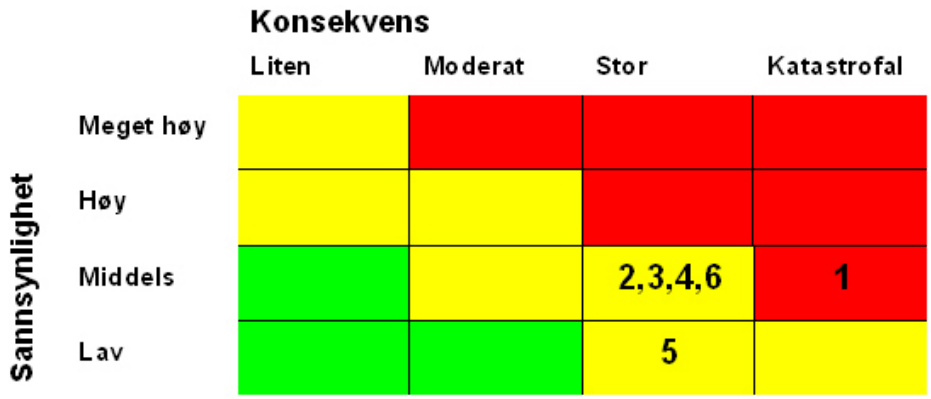
Figur 12: Fremgangsmåte beskrevet i NSM-ROS2004 [3].

ikke gjenspeiler de mindre lokasjonene og de andre delene av organisasjonen. Samtidig var det vanskelig å gjøre gode anslag på eller rangering av kost-nytte vurderinger av tiltak. Vi ønsket videre å kunne identifisere hvilke tiltak som kostet lite og samtidig ga best resultater. Hensikten var å kunne presentere et fullstendig og bedre resultat for ledelsen. Følgende skisserer et eksempel på hvordan vi har benyttet risikomatrise for evaluering og vurdering av trusler og sårbarheter funnet ROS-analysen. Tallene i risikomatrisen representerer trusler og sårbarheter funnet i analysen av en systemdel.

For eksempel kan tallet 5 i risikomatrisen skissert i figur 13 beskrive følgende trussel:

- Større, tyngre, og mer omfattende prosesser for å iverksette tiltak og utføre handlinger. Sentralisering av handlingskraft, og overgang til et mer byråkratisk system:
  Effektiv og rask oppfølging og support krever ofte straks handlinger. Ved en overgang til en sentralisert løsning, vil strakshandlinger ofte kreve lengre, og mer formell form før tiltak iverksettes. Strakshandlinger som i dag kan tas over telefon, vil i fremtiden sannsynligvis kreve dokumentasjon og godkjenning. Noe som kan resultere i en byrde for brukeren som sitter med problemet. Ved en overgang til en sentralisert løsning, vil det sannsynligvis være mest hensiktsmessig å tillegge lokasjonene beslutningsmyndighet for å iverksette strakstiltak. Dette kan bidra til å løse problemer på et lavest mulig organisasjonsmessig nivå. Hendelsen ble vurdert til å ha stor sannsynlighet for å skje. Konsekvensene ble vurdert til å ha en lav følge.

Referansegruppa vurderte så hver av de identifiserte trusselene. Trusselen beskrevet som nummer fem i risikomatrisen, ble vurdert til å ha en lav sannsynlighet for å inntreffe. Men ved å inntreffe ble trusselen vurdert til å ha stor konsekvens. Den totale vurderingen gir punkt 5 den skisserte plasseringen i risikomatrisen (Se figur 13).



Figur 13: Skisse av risikomatrise for vurdering av konsekvens og sannsynlighet.

6.3 Gjennomføring av andre ROS-analyse

Følgende beskriver gjennomføringen av andre ROS-analyse i eksperimentet. Innledningsvis i kapitlet beskrives det hvordan metoden FTA skal benyttes, deretter beskrives det hvordan vi har valgt å benytte FTA som metode.

6.4 Beskrivelse av metoden FTA

Det beskrives av Rausand [65] og Aven [37] at FTA kan gjennomføres i fem trinn. De fem forskjellige trinnene er inndelt i ulike aktiviteter:

1. Definisjon av problem og randbetingelser.
2. Konstruksjon av feiltreet.
3. Bestemmelse av minimale kutt- og stimengder.
4. Kvalitativ analyse av feiltreet.
5. Kvantitativ analyse av feiltreet.

6.4.1 Konstruksjon av feiltrær

Konstruksjonen av feiltreet blir fastsatt med utgangspunkt i topphendelsen, slik at analytikeren arbeider seg suksessivt nedover i treet ved å gjenta spørsmålet «Hva er årsaken?». Dette betyr at metoden har en deduktiv tilnærming [65, 37]. Portene og symbolene som er beskrevet i figur 14, gir mulighet til å kombinere årsaker og hendelser i feil-trærne. Samtidig gir port-egenskapene mulighet for å beskrive sannsynlighet og konsekvens. Dette kan beskrives med for eksempel ved bruk av «OR»-porter, hvor sannsynligheter blir større fordi «OR»-porter representerer en seriell avhengighet. Feil i enten den ene eller den andre, medfører en hendelse. En «OR»-port antar at hendelser er uavhengige av hverandre. Dette betyr at antallet inngangshendelser er kun avhengig av et signal i en av «inputene». En «AND»-port kombinerer sannsynligheter, og sannsynlighetene blir derfor mindre. Dette fordi det kreves inputsignaler i flere inngangshendelser før porten gir et outputsignal. Sammenkoblingen av de logiske portene leder frem til minimale kutt- og stimengder. Med «kuttmengde» menes «mengden av inngangshendelser som ved inntreffer samtidig sikrer for at topphendelsen vil inntreffe» [65]. En kuttmengde kan beskrives for å være minimal hvis «den ikke kan reduseres uten å miste status som som kuttmengde» [65]. En «stimengde» er «en mengde av inngangshendelser som ikke ved å inntreffe samtidig sikrer at topphendelsen ikke inntreffer» [65].

6.4.2 Analyse av konstruert feiltre, kvalitativ eller kvantitativ

Metoden avsluttes med å gjennomføre en analyse av feiltreet, enten kvalitativt, kvantitativt, eller en kombinasjon. En kvalitativ analyse gjøres ved å ta utgangspunkt i de minimale kuttmengdene. Det vil si avhengigheten mellom inngangshendelser i kuttmengde, og sammensetning av dem. Eksempelvis om en «kuttmengde» inneholder to hendelser, vil det si at begge hendelsene må inntreffe for at topphendelsen skal inntreffe [65]. En kvantitativ analyse utføres ved å finne rater/pålitelighet ved komponentene, for deretter å analysere sammensetningen av komponentene og den pålitelighetsmessige betydningen av komponentene.

6.5 Hvordan har vi benyttet FTA som metode

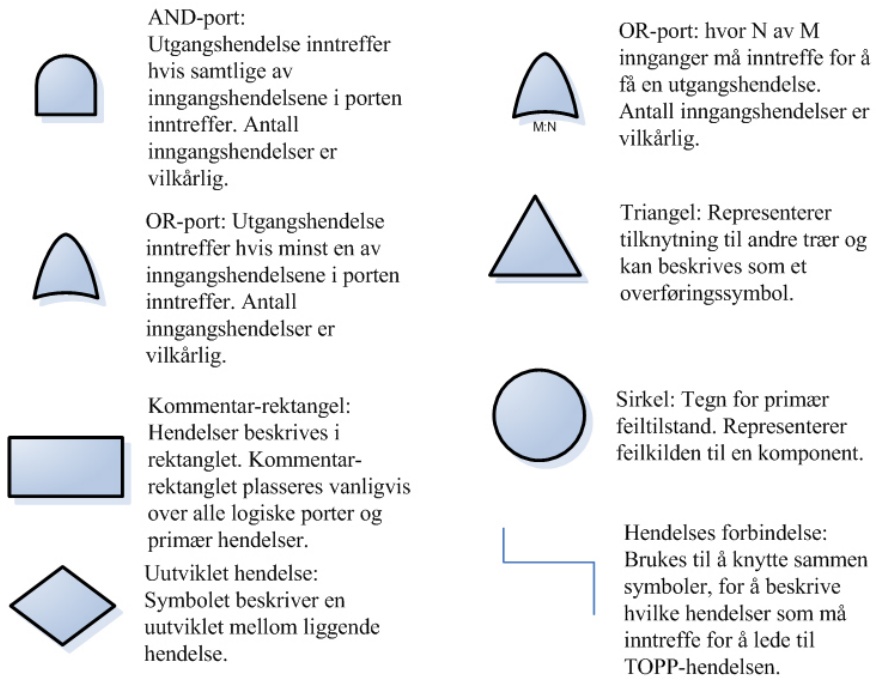
I det følgende beskrives det hvordan vi har benyttet FTA som metode innenfor informasjonssikkerhet.

6.6 Innledning

Vi valgte å ta utgangspunkt i FTA, og samtidig forsøke å kombinere tilnærmingene som benyttes i angrepstre(Attack-tree) [76] og trusseltre(Threat-tree) [75]. Målet er å oppnå en bredere tilnærming for identifisering av både trusler, risiko og angrepsmuligheter ved systemet. Samtidig som vi ønsket å dekke både tilfeldig (safety) og tilsiktet (security).
FTA-analyse er det sentrert rundt problemet som skal analyseres. Dette defineres som topphendelse eller uønsket hendelse i feiltreet. Det ble valgt å dele opp topphendelsen i mindre subtrær, fordi det etter vår oppfatning var for ambisiøst og omfattende å konstruere et feiltre for hele systemet under en topphendelse. Det ble valgt å dele topphendelsen inn i følgende perspektiver: konfidensialitet, integritet og tilgjengelighet. Ønsket var å beskrive en enkel og konkret topphendelse. Det bekrives av Rausand [65] at topphendelsen bør være beskrevet på en klar og tydelig måte. Rausand beskriver videre at «En uklar definisjon av topphendelsen kan medføre at analysen får en begrenset verdi». Hendelsen bør beskrive «Hva», «Hvor» og «Når».

Det ble inndelt i følgende overordnede topphendelser:

- Tap av konfidensialitet ved EPJ-systemet.
- Tap av integritet ved EPJ-systemet.
- Tap av tilgjengelighet ved EPJ-systemet.



Figur 14: FTA-komponenter.

Topphendelsene ble deretter inndelt i mindre og mer oversiktelige deler. Konsistensen i selve analyse, blir beskrevet ved at randbetingelsen må bli klart nok definert [37]. En randbetingelse er beskrevet ved systemets fysiske grenser, definisjonen av initial betingelser (tilstanden som systemet er i for at hendelsen skal inntreffe), avgrensninger ved eksterne belastninger (sabotasje, jordskjelv osv) og fastsettelse av detaljeringsnivå [37]. Det ble valgt å dele systemet inn i mindre og mer oversiktelige deler, og det ble valgt å benytte modellen fra første ROS-analyse. Modellen som ble benyttet ble delt inn i følgende deler: «brukersiden», «nettverk og infrastruktur», og «server/drift-siden». Systemet ble derfor valgt delt inn i følgende mindre deler:

- Tap av konfidensialitet på brukersiden.
- Tap av konfidensialitet ved infrastruktur.
- Tap av konfidensialitet ved server/drift/support.
- Tap av integritet brukersiden.
- Tap av integritet ved infrastruktur.
- Tap av integritet ved ved server/drift/support.
- Tap av tilgjengelighet på brukersiden.
- Tap av tilgjengelighet ved infrastruktur.
- Tap av tilgjengelighet ved server/drift/support.

6.7 Identifikasjon og kategorisering av feilkilder

Det beskrives av Kumamoto og Henley [1] at det primære målet med pålitelighet og sikkerhet er å redusere sannsynlighet for at tilfeldige, menneskelige, miljømessige og økonomiske uhell skal kunne inntreffe. Kumamoto og Henley kategoriserer feilkilder ved:

1. Handlinger utført og relartert til menneskelige feil. Foreksempel operatør feil, design error og vedlikeholdsfeil.
2. Hendelser som skjer på bakgrunn av komponentfeil.
3. Hendelser relatert til miljømessige faktorer som foreksempel jordskjelv, oversvømmelse osv.

Rausand [65] kategoriserer de ulike feilkildene i tre hovedkategorier, primære feilkilder(funksjonsfeil), sekundære feilkilder (feilkilder som inntreffer pågrunn av overbelastninger), og kommandofeil(funksjonsfeil på utstyr som opererer på feil tidspunkt).

6.7.1 Vår kategorisering av feilkilder

Vi valgte å definere ulike kategorier av feilkilder til systemet for å oppnå en bredere tilnærming ved konstruksjon av feiltrærne. Kategoriene konfidensialitet, integritet og tilgjengelighet ble valgt som topphendelser og feiltrærne ble konstruert ved å gå i dybden og finne feilkildene for at topphendelsen skal kunne inntreffe. Det ble beskrevet enkle scenarier for hver av kategoriene. Scenariene ble deretter brutt ned i mindre feilkilder (Se tabell 7, 8, 9, og 10 i vedlegg D). Det var et ønske at feiltrærne dekket både tilsiktede- og utilsiktede hendelser.

Følgende presenteres vår kategorisering av feilkildene:

1. Infrastruktur, som har følgende under underkategorier: strøm/UPS, flom, vann, bygning/byggmasse, nettverkstopologi osv.
2. Menneskelig involvering. Med følgende underkategorier: utilsiktet, tilsiktet, internt, eksternt.
3. Software. Med følgende underkategorier: virus, sikkerhetshull.
4. Hardware. Med følgende underkatergori: komponentlevetid, sviktfrekvense.

Ved å kategorisere feilkildene fikk vi mulighet til å definere forskjellige tilnærminger til sikkerhet. Kategoriene 1, 2, og 3 dekker det som er beskrevet i teoridelen ved «tilsiktet angrep/hendelser» (security), og kategori 4 beskriver området «ikke-tilsiktet» (safety).

6.8 Beskrivelse av konstruerte feiltrær

Vi valgte å ta utgangspunkt i Moberg [4] sitt arbeid ved inndeling av systemets logiske og fysiske avgrensninger. Moberg beskriver inndeling av systemets grenser ved fysisk og logisk inndeling. Moberg har i sitt arbeid valgt å fokusere på systemtekniske avgrensninger. Det ble tatt et valg om å fokusere både på systemtekniske og fysiske avgrensninger, samt hvilken tilgang de ansatte i virksomheten har. Utgangspunktet var at en person har bestandig en «plassering» i forhold til en virksomhet. Enten det er internt i virksomheten som forvalter, eller som bruker av tjenestene som virksomheten leverer. Således har en ansatt i en virksomhet nesten bestandig et forhold til et informasjonssystem. Enten som autorisert bruker eller kun som ansatt uten autorisert tilgang. Systemet har også forskjellige avgrensninger (eksempelvis bygningsmessige forhold) som avgjør hvilken tilgang de ansatte har til systemet. Det ble derfor identifisert forskjellige kategorier ved de ansattes tilgang og forhold til systemet:

- Ansatt med logisk tilgang (Autorisert tilgang).
- Ansatt uten logisk tilgang.
- Leverandører av utstyr og material (med og uten logisk tilgang).
- Bruker av virksomhetens tjenester (eksempelvis pasient).
- Ekstern person (eksempelvis en ondsinnet person).

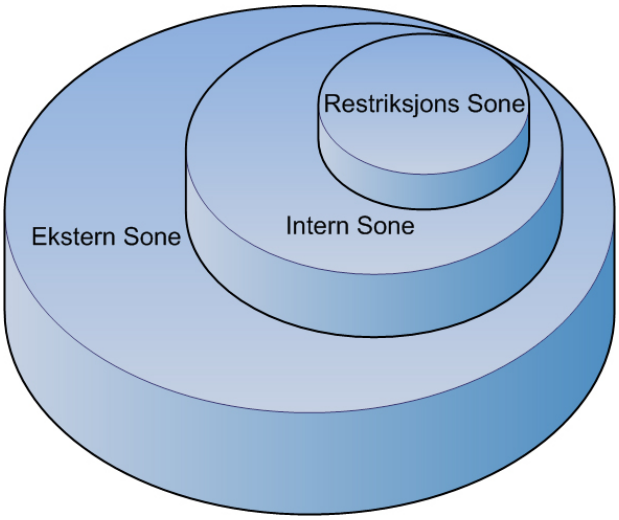
På bakgrunn av kategoriseringen over, ble det valgt å dele systemet i forskjellige soner:

- Ekstern sone: Som er utenfor virksomhetens fysiske avgrensning, dvs. utenfor bygninger osv. Det eksisterer ingen informasjon som er konfidensiell i denne sonen. Dette kan betraktes som den sonen hvor brukerne av systemet vanligvis ferdes og oppholder seg (her:pasienter).
- Intern sone: Det stedet hvor de ansatte i virksomheten befinner seg. De ansatte i denne sonen har ikke logisk tilgang til systemet som skal analyseres. Personene har fysisk tilgang til systemet, men mangler logisk tilgang.
- Restriksjons sone: Dette er sonen hvor de ansatte som både har logisk og fysisk tilgang befinner seg. Her finnes den informasjonen som kan kategoriseres som kritisk og sensitiv for virksomheten. Denne sonen er fysisk og logisk atskilt fra den eksterne sonen, og kun logisk atskilt fra den interne sonen.

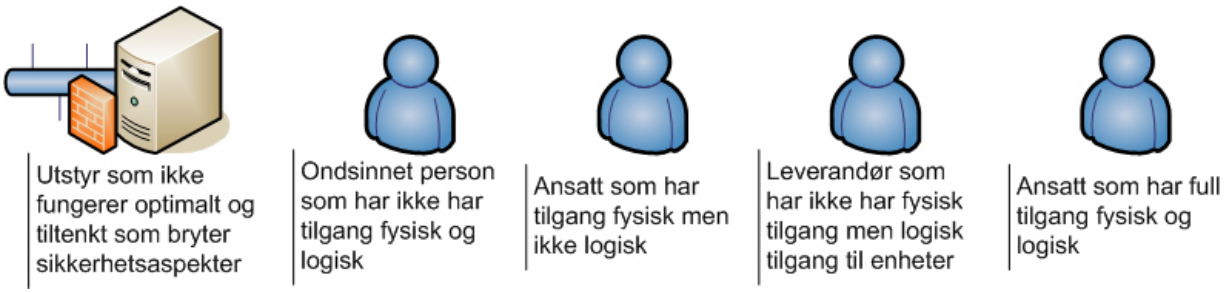
Feiltrærne er konstruert med bakgrunn i kategoriseringen beskrevet over og inndelingen av soner i figur 15. Personer med få sikkerhetsbarrierer er beskrevet på høyre del av feiltreet. Slik at personer som må bryte færrest sikkerhetsbarriere beskrevet fra høyre mot venstre. Eksempelvis, en doktor eller IKT-ansatt har tilgang til både rom med EPJ-pc og tilgang til pc og EPJ-applikasjon. Personen har derfor færrest sikkerhetsbarrierer å bryte. En person som må bryte seg inn på et rom, videre bryte den logiske tilgangskontrollen osv. er plassert mot venstre side av feiltreet. Tap av sikkerhet som er forårsaket av komponentfeil, systemfeil og tap av enheter osv. er skissert på venstre side av feiltreet. Se figur 16.

6.8.1 Gjennomføring av ROS-møte

Før ROS-møtet ble det presentert et utkast av feiltrærne til helseforetaket. Det ble innhentet statistisk materiale på ulike områder ved systemet (for eksempel antall angrep på server, antall virusangrep og antall hacking tilfeller osv). Selve ROS-møtet ble gjennomført i to deler. En innledning med presentasjon av FTA, og en ROS-analyse med gjennomgang av feiltrærne. Verdiene presentert av helseforetaket ble deretter vurdert og beskrevet ved feilkildene i trærne. Områder som var vanskelig å kvantifisere, ble det forsøk anslått relative verdier. Samtidig ble forsøkt innhentet verdier fra andre kilder.



Figur 15: Inndeling av soner. Inspirert av Moberg [4].



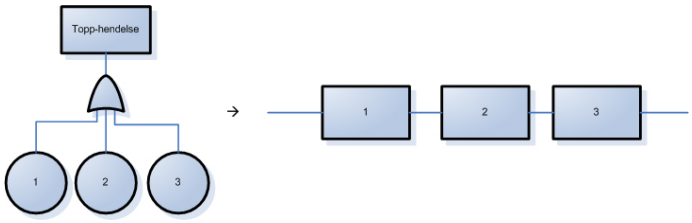
Figur 16: Beskrivelse av feiltre konstruksjon.

6.8.2 Konvertering av feiltrær til pålitelighetsnettverk

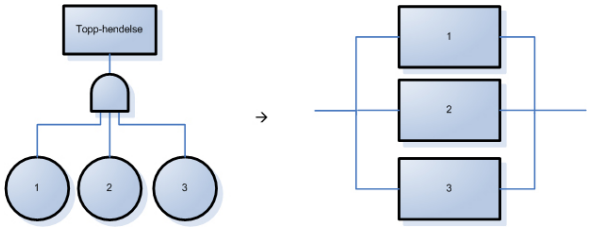
For å kunne gjennomføre en kvantitativ analyse av feiltrærne, er det nødvendig å konvertere feiltrærne til pålitelighetsnettverk. På bakgrunn av den strukturelle relasjonen mellom feilkildene, kan feiltreet konverteres til et pålitelighetnettverk [65]. Ved å konvertere feiltrærne til pålitelighetsnettverk, kan analytikere finne minimale kuttmengder. En minimal kuttmengde er en mengde av inngangshendelser, som ved å inntreffe sikrer at topphendelsen inntreffer. En minimal kuttmengde kan således analyseres og gi indikatorer på hvor i systemet det eksisterer svakheter og hvor det bør iverksettes tiltak.

6.8.3 Strukturer i feiltrær og konvertering til pålitelighetsnettverk

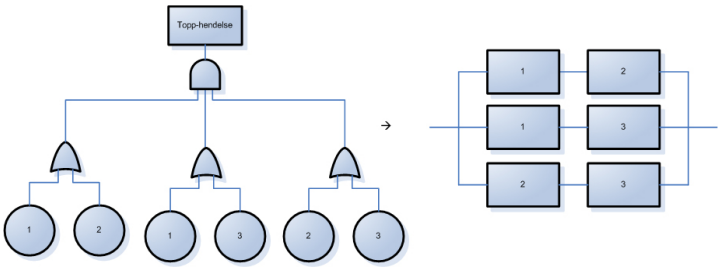
På bakgrunn av den logiske koblingen mellom komponentene, er det mulig å konstruere noen forskjellige strukturer. Strukturene kan beskrives som henholdsvis serie-struktur, parallell-struktur, og k-av-n struktur. I en serie-struktur kreves det kun at en av komponentene slutter å funksjonerer for at topphendelsen skal inntreffe. I en parallell-struktur kreves det at samtlige komponenter skal inntreffe for at topphendelsen skal inntreffe [81]. Figurene 17, 18 og 19 beskriver eksempler på konvertering av enkle feiltrær til pålitelighetsnettverk.



Figur 17: Skisse av feiltre som gir en serie-struktur ved konvertering til pålitelighetsnettverk.



Figur 18: Skisse av feiltre som gir en parallell-struktur ved konvertering til pålitelighetsnettverk.



Figur 19: Skisse av feiltre som gir en k-av-n-struktur ved konvertering til pålitelighetsnettverk.

6.9 Teori for å finne pålitelighet i et system

Teorien som beskrives utover er hentet fra «Pålitelighets analyse» [81] av Holen, Høyland og Rausand. Et system som er sammensatt av n komponenter er et system av orden n. Komponentene kan nummereres fra 1 til n. Hver komponent kan enten være funksjonsdyktig eller ikke-funksjonsdyktig. Dette kan beskrives ved en binær representasjon, ved 0 og 1.

Tilstanden til en x_i beskrives da som følger:

$$\mathbf{x_i} = \begin{cases} 1 \text{ om komponent nr. i er funksjonsdyktig.} \\ 0 \text{ om komponent nr. i er i feiltilstand.} \end{cases}$$

Strukturfunksjonen $\phi(\underline{X})$, er 1 om systemet er funksjonsdyktig og 0 ellers. Strukturfunksjonen $\phi(\underline{X})$ i en serie-struktur blir:

$$\phi(\underline{X}) = x_1 \cdot x_2 \cdot ...x_n = \prod_{i=1}^{n} x_i, \tag{6.1}$$

og i en parallell-struktur blir strukturfunksjonene følgende:

$$\phi(\underline{X}) = 1 - (1 - x_1)(1 - x_2)...(1 - x_n) = 1 - \prod_{i=1}^{n}(1 - x_i) = \amalg_{i=1}^{n} x_i \tag{6.2}$$

og i en k-av-n-struktur blir

$$\phi(\underline{\mathbf{X}}) = \begin{cases} 1 \text{ når } \sum_{i=1}^{n} x_i > \text{eller} = k \\ 0 \text{ når } \sum_{i=1}^{n} x_i < k \end{cases}$$

For en parallell-struktur som vist i figur 26 med kuttmengde (1,2), blir utledet strukturfunksjon følgende:

$$\begin{aligned} x_1 \amalg x_2 &= 1 - (1 - x_1)(1 - x_2) \\ &= 1 - (1 - x_2 - x_1 + x_1x_2) \\ &= (x_2 + x_1 - x_1x_2) \end{aligned}$$

En utledet k-av-n struktur skissert i figur 24 med kuttmengdene (1,3)(2,3)(1,3), gir følgende strukturfunksjon:

$$\begin{aligned} &x_1x_2 \amalg x_2x_3 \amalg x_1x_3 \\ &= 1 - (1 - x_1x_2)(1 - x_2x_3)(1 - x_1x_3) \\ &= 1 - [(1 - x_1x_2 - x_2x_3 - x_1x_2^2x_3)(1 - x_1x_3)] \\ &= 1 - [1 - x_1x_2 - x_2x_3 - x_1x_2^2x_3 - x_1x_3 + x_1^2x_2x_3 + x_1x_2x_3 + x_1^2x_2^2x_3^2] \\ &= x_1x_2 + x_2x_3 + x_1x_2x_3 + x_1x_3 - x_1x_2x_3 - x_1x_2x_3 - x_1x_2x_3 - x_1x_2x_3 \\ &= x_1x_2 + x_2x_3 + x_1x_3 - 2x_1x_2x_3 \end{aligned}$$

Siden vi opererer med binære representasjoner, vil $x_i^2 = x_i$.

6.9.1 Uavhengige hendelser

Hvorvidt en komponent ikke vil være funksjonsdyktig i et tidstrom t_i, kan en vanligvis ikke si noe sikkert om [81]. Ofte benyttes det statistiske data/regelmessigheter for å anslå sannsynlighet for at en komponent ikke er funksjonsdyktig. Holen [81] beskriver at «det derfor er naturlig å oppfatte så vel tilstandsvariablene til de n komponentene som den tilhørende strukturfunksjonen som stokastiske variable». Dette kan beskrives med følgende [81]:

$$X_1(t), X_2(t)...X_n(t), \text{ og } \phi(\underline{X}(t))$$

og er da interessert i å bestemme sannsynlighetene:

$$p_i = P(X_i(t) = 1);\ i = 1, \ldots, n \text{ og}$$

$$p_S(t) = P(\phi(\underline{X}(t) = 1))$$

I systemer hvor «svikt» i forskjellige komponenter inntreffer som uavhengige hendelser, vil det medføre at tilstandsvariablene $X_1(t)$, $X_2(t) \ldots X_n(t)$ ved hvert tidspunkt t oppfattes som stokastiske variable. Påliteligheten i systemer beskrevet ved pålitelighetsnettverk blir da følgende:

Siden tilstandsvariablene $X_i(t)$; $i = 1 \ldots n$ er binære, vil vi ha at:

$$E[X_i(t)] = 0 \cdot P(X_i(t) = 0) + 1 \cdot P(X_i(t) = 1) = p_i(t); i = 1, 2, \ldots, n.$$

Analogt blir systempåliteligheten ved tidspunkt t:

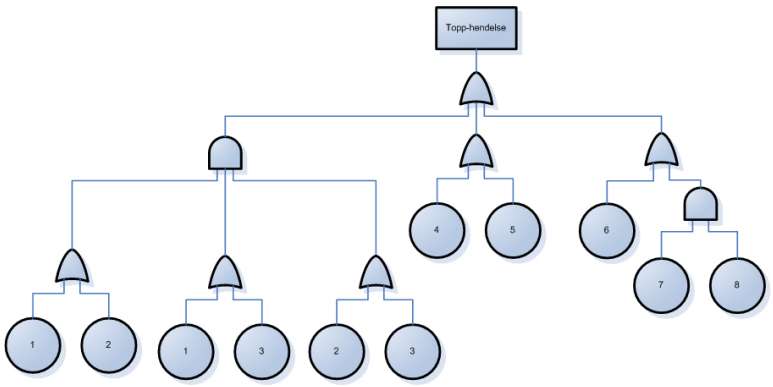
$$p_S(t) = E[\phi(\underline{X}(t))].$$

Når komponentene er uavhengige vil systempåliteligheten, $p_S(t)$, bli en funksjon av $p_i(t)$-ene alene (Se [81] for bevis). Slik at

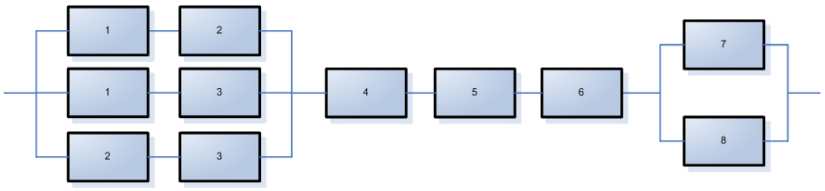
$$p_S(t) = h(p(t)) = h((p_1(t)), p_2(t), \ldots, p_n(t)).$$

6.9.2 Et beskrivende eksempel

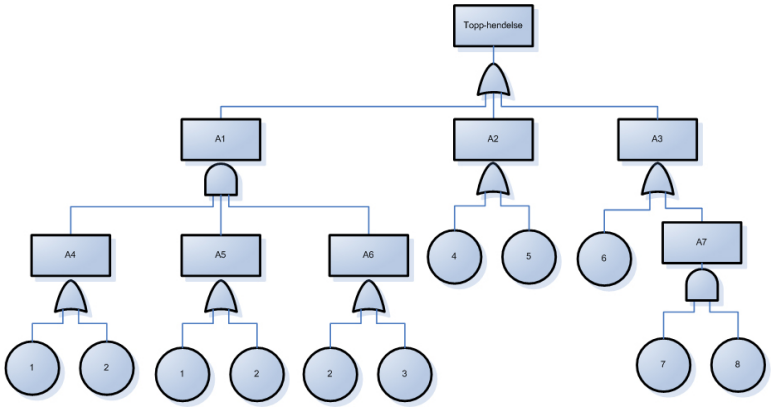
I figur 20 presenteres det et feiltre av et tenkt system. Sammenkoblingen av komponentene i systemet gir feiltreet i figur 20. Feilkildene 1, 2 og 3 er komponenter som forekommer flere steder i systemet, og derfor beskrevet som en k-av-n struktur. Feiltreet blir deretter konvertert til et pålitelighetsnettverk i presentert i figur 21. Ved å finne pålitelighetsnettverket i feiltreet, kan de minimale kuttmengdene i systemet identifiseres. Minimale kuttmengder finner vi ved å benytte oss av MOCUS (Method for Obtaining CUt-Sets) [81]. I MOCUS tildeles hver port et navn ($A1, A2....A_n$). Hvis porten er en «OR»-port, skrives hver inngang til porten under hverandre. Om porten er en «AND»-port, skrives inngangene på samme linje. Radene som fremkommer vil da gi kuttmengdene i systemet [81]. Ved bruk av MOCUS finner vi følgende minimale kuttmengder i systemet (1,2),(1,3),(2,3),(4),(5),(6) og (7,8), se figur 23. Videre kan pålitelighetsnettverket deles inn i mindre komplekse strukturer ved: En serie-struktur(Se figur 25), en parallell-struktur(Se figur 26) og en k-av-n-struktur (Se figur 24). Ved å dele inn pålitelighetsnettverket (figur 23) i mindre deler, kan en enklere beregne påliteligheten til systemet. Dermed blir definisjonen på strukturfunksjonen til modul i, i = I, II, III.



Figur 20: Feiltre av et tenkt system.



Figur 21: Pålitelighetsnettverk av feiltreet presentert i figur 20.



Figur 22: Fremgangsmåte for nedbryting av presentert system, for å finne minimale kuttmengder.

A1 A2 A3	A4, A5, A6 A2 A3	(1,2)(1,3) (2,3) A2 A3	(1,2)(1,3) (2,3) A2 A3	(1,2)(1,3) (2,3) 4 5 A3

(1,2) (1,3) (2,3) (4) (5) (6)	(1,2)(1,3) (2,3) (4) (5) (6) A7	(1,2)(1,3) (2,3) (4) (5) (6) (7, 8)

Figur 23: Viser fremgangsmåte for å finne minimale kuttmengder i systemet.

La ω være den samlede strukturfunksjonen ved:

$$\omega(X_I, X_{II}, X_{III}) = X_I \cdot X_{II} \cdot X_{III} \tag{6.3}$$

Som gir oss følgende deler

$$\begin{aligned} x_I(\underline{X}) &= X_1X_2 \amalg X_1X_3 \amalg X_2X_3 = X_1X_2 + X_1X_3 + X_2X_3 - 2X_1X_2X_3 \\ x_{II}(\underline{X}) &= X_4X_5X_6 \\ x_{III}(\underline{X}) &= X_7 \amalg X_8 = X_7 + X_8 - X_7X_8 \end{aligned}$$

Systemets strukturfunksjon utlede blir følgende:

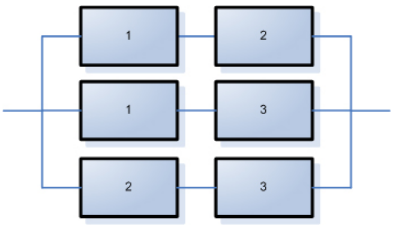
$$\phi(\underline{X}) = (X_1X_2 + X_1X_3 + X_2X_3 - 2X_1X_2X_3)(X_4X_5X_6)(X_7 + X_8 - X_7X_8) \tag{6.4}$$

Hvis komponentpåliteligheten ved tidspunkt $t = t_0$ for komponent i betegnes med $p_i, i = 1, i = 2, \ldots$ og $X_i, \ldots, X_n$ er uavhengige, får vi at systempåliteligheten ved tidspunktet t_0 blir:

$$p_S(t) = (p_1p_2 + p_1p_3 + p_2p_3 - 2p_1p_2p_3) \cdot p_4p_5p_6(p_7 + p_8 - p_7p_8) \tag{6.5}$$

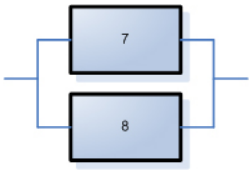
6.9.3 Analyse av feiltre

Ved å utføre en kvantitativ analyse av feiltrærne kan analytikere finne frem til komponenter eller hendelser, som har stor betydning for systemet. Samtidig kan analytikere finne frem til områder hvor det bør iverksettes tiltak for å redusere en uønsket hendelse. Vi vet at en kjede aldri er sterkere enn det svakeste leddet. Vi kan derfor også anta



Figur 24: k-av-n-struktur ved inndeling av pålitelighetsnettverket i figur 21(X_I).

Figur 25: Serie-struktur ved inndeling av pålitelighetsnettverket i figur 21(X_{II}).



Figur 26: Parallell-struktur ved inndeling av pålitelighetsnettverket i figur 21(X_{III}).

Komponent:	**Feilrate:**
$p_1(t_0)$	0.98
$p_2(t_0)$	0.96
$p_3(t_0)$	0.94
$p_4(t_0)$	0.91
$p_5(t_0)$	0.99
$p_6(t_0)$	0.98
$p_7(t_0)$	0.97
$p_8(t_0)$	0.95

Tabell 2: Oversikt over pålitelighet i komponentene i systemet.

at det svakeste leddet har stor sikkerhetsmessig betydning for den totale sikkerheten i systemet [81]. Ved å redusere de svake områdene i systemet kan vi øke systemets totale pålitelighet og sikkerhet. Det kan benyttes ulike probalistiske metoder for å måle pålitelighetenen til et system. Fo eksempel ved antall virus angrep, hacking forsøk, komponentlevetid, antallet svikt pr. tidsenhet og sannsynlighet for at systemet er funksjonsdyktig ved tidspunkt t. Vi antar at enhetene i systemet svikter/feiler i henhold til en Poisson-prosess [81]. La T betegne tidspunktet i Poisson-prosessen når en enhet feiler for første gang. T er da en stokastisk variabel med forventningsverdi

$$\mathbf{F_T(t)} = \begin{cases} 0, \text{ for } t \leq 0 \\ P(T \leq t) = 1 \text{ - } P(T > t) = 1 \text{ - } p(0,t) = 1 - e^{\lambda t} \text{ , for } t > 0 \end{cases}$$

T sies da å være eksponensialfordelt med parameter $\lambda, T\ exp.(\lambda)$.

Betrakt et system med pålitelighetsnettverk skissert i figur 20 ved et tidspunkt t_0. Vi innfører tilstandsvariablene:

$$\mathbf{X_i} = \begin{cases} 1, \text{ om komponent nr. i er funksjonsdyktig ved tidspunkt } t_0 \\ 0, \text{ ellers for } i = 1, 2 \ldots, 8 \end{cases}$$

Ved å benytte Poisson-prosess, kan vi finne verdier for at topphendelsen i feiltreet inntreffer. Følgende får vi da systemstrukturen:

$$p_S = (p_1p_2 + p_1p_3 + p_2p_3 - 2p_1p_2p_3) \cdot p_4p_5p_6(p_7 + p_8 - p_7p_8) \tag{6.6}$$

Verdier i komponentene p_i kan finnes i rater eller empiriske/ statistiske data ved systemet. For eksempel en hendelse som inntreffer 2 ganger pr. døgn, vil gi følgende verdi ved bruk av Poisson prosess:

$$\lambda = 2, t = 0$$

$$1 - e^{\lambda t} = 0,864664717$$

Ved å finne påliteligheten til hver komponent i systemet kan vi beregne den totale systempåliteligheten, gitt ved verdiene i tabell 2. Verdiene settes så inn i strukturfunksjonen p_S

$$\begin{aligned} p_S &= (p_1p_2 + p_1p_3 + p_2p_3 - 2p_1p_2p_3) \cdot p_4p_5p_6(p_7 + p_8 - p_7p_8) \\ &= (0.98 \cdot 0.96 + 0.98 \cdot 0.94 + 0.96 \cdot 0.94 - 2 \cdot 0.98 \cdot 0.96 \cdot 0.94)0.91 \\ &\quad \cdot 0.99 \cdot 0.98(0.97 + 0.95 - 0.97 \cdot 0.95) \\ &= 0.8777634528 \end{aligned}$$

6.9.4 Pålitelighetsmessig betydning

Den kvantitative beskrivelsen av påliteligheten i komponentene, kan gi indikatorer på hvilken pålitelighetsmessig betydning komponentene har. Slike mål kan gi indikatorer på hvilke komponenter i systemet som bør utbedres, og bidra til å identifisere systemområder hvor det bør iverksettes tiltak. Tiltakene som iverksettes, bør iverksettes på bakgrunn av en analyse. Analysen kan således gi svar på hvilke tiltak som har størst potensial for å være mest hensiktsmessig. Samtidig vil plasseringen av komponentene i systemet også være av pålitelighetsmessig betydning. For å finne hvilke komponenter i systemet som bør utbedres, er Birnbaums mål beskrevet for å være den mest egnede [81]. Birnbaum foreslo i 1969 en mulighet for å finne den pålitelighetsmessige betydningen av komponent nr.i ved tidspunkt t_0. Birnbaums mål beskrives følgende:

Betrakt et system som består av n uavhengige komponenter, og la $p_i(t)$ betegne påliteligheten til komponent i ved tidspunkt $t, i = 1, 2, \ldots, n$. Systempåliteligheten betegnes som før ved:

$$p_S(t) = h(p(t)) = h(p_1(t), p_2(t), \ldots, p_n(t))$$

Den pålitelighetsmessige betydningen av komponent i ved tidspunkt t_0:

$$I^B(i|t_0) = \frac{\partial h(\underline{p}(t_0))}{\partial p_i(t_0)}$$

for $i = 1, 2, \ldots, n$.

Vi finner Birnbaums mål ved å utføre partialderivering av systempåliteligheten med hensyn på p_i. Dersom $I^B(i|t_0)$ er stor, vil en liten endring i påliteligheten til komponent i medføre en stor endring i systempåliteligheten ved tidspunkt t.

6.9.5 Eksempel på pålitelighetsmessig betydning

I det følgende skisseres noen eksempler på andvendelse av Birnbaum mål på ulike strukturer for å finne den pålitelighetsmessig betydning av komponentene.

En serie-struktur med to uavhengige komponenter, i et gitt tidspunkt t_0 med følgende komponentpålitelighet $p_1(t_0) = p_1 = 0.98$ og $p_2(t_0) = p_2 = 0.96$, hvor $p_1 > p_2$.

Systempåliteligheten blir ved tidspunkt t_0:

$$h(p_1(t_0), p_2(p_2(t_0)) = h(p_{1\cdot 2}) = p_1 \cdot p_2 = 0.9408$$

Birnbaums mål for den pålitelighestmessige betydningen av komponentene nr.1 og nr.2., blir ved tidspunkt t_0:

$$I^B(1|t_0) = \frac{\partial h(p_1, p_2)}{\partial p_1} = p_2 = 0.96$$

$$I^B(2|t_0) = \frac{\partial h(p_1, p_2)}{\partial p_2} = p_1 = 0.98$$

Vi ser at i en serie-struktur er den komponenten med lavest pålitelighet, den komponenten med størst betydning.

I en parallell-struktur med to uavhengige komponenter, gitt samme pålitelighet som i eksemplet over, vil systempåliteligheten ved t_0 være:

$$h(p_1(t_0)), p_2(p_2(t_0)) = h(p_1, p_2) = p_1 + p_2 - p_1 \cdot p_2 = 0.9992$$

Birnbaums mål for den pålitelighetsmessig betydningen, blir i en parallell-struktur gitt den samme pålitelighet i komponentene som i eksemplet over:

$$I^B(1|t_0) = \frac{\partial h(p_1 + p_2 - p_1 \cdot p_2)}{\partial p_1} = 1 - p_2 = 0.04$$

$$I^B(2|t_0) = \frac{\partial h(p_1 + p_2 - p_2 \cdot p_2)}{\partial p_1} = 1 - p_1 = 0.02$$

Den komponenten i parallell-strukturen som har høyest pålitelighet, er den komponenten som er viktigst.

Gitt en tredje komponent med pålitelighet $p_3(t_0) = p_3 = 0.94$, i en k-av-n-struktur er da systempåliteligheten ved tidspunkt t_0 gitt ved:

$$h(p(t_0)) = h(\underline{p}) = p_1p_2 + p_1p_3 + p_2p_3 - 2p_1p_2p_3 = 0.9957,$$

mens Birnbaums mål for pålitelighetsmessig betydning blir:

$$I^B(1|t_0) = \frac{\partial(p_1p_2 + p_1p_3 + p_2p_3 - 2p_1p_2p_3)}{\partial p_1} = p_2 + p_3 - 2p_2p_3 = 0.0952$$

$$I^B(2|t_0) = \frac{\partial(p_1p_2 + p_1p_3 + p_2p_3 - 2p_1p_2p_3)}{\partial p_2} = p_1 + p_3 - 2p_1p_3 = 0.0776$$

$$I^B(3|t_0) = \frac{\partial(p_1p_2 + p_1p_3 + p_2p_3 - 2p_1p_2p_3)}{\partial p_3} = p_1 + p_2 - 2p_1p_2 = 0.0584.$$

Slik at vi i k-av-n-strukturen får følgende avtagende pålitelighetsmessig betydning i komponentene:

$$I^B(1|t_0) > I^B(2|t_0) > I^B(3|t_0).$$

6.9.6 Et eksempel på Birnbaums pålitelighetsmessige mål

I det følgende beskrives et eksempel på hvordan vi har benyttet Birnbaums mål for å finne sårbarheter og risikoområder i et system. Det presenteres et pålitelighetsnettverk for et system (se fig 27), med feilrater funnet i de forskjellige komponentene i systemet. Først skisseres det et eksempel på iverksettelse av tiltak på bakgrunn komponenter med høy feilrate. Deretter beskrives det iverksettelse av tiltak på bakgrunn av Birnbaums mål. Strukturfunksjonen for systemet er beskrevet ved:

$$\phi(\underline{X}) = X_1X_2X_3X_4((X_5X_6(X_7 \amalg X_8)(X_9 \amalg X_{10})) \amalg X_{11}X_{12}X_{13}X_{14}X_{15}) \tag{6.7}$$

Utledet strukturfunksjon blir:

$$\begin{aligned} p_S(t) \quad = \quad & x_1x_2x_3x_4(x_5x_6(x_7 + x_8 - x_7x_8)(x_9 + x_{10} - x_9x_{10}) \\ & + x_{11}x_{12}x_{13}x_{14}x_{15} - x_5x_6(x_7 + x_8 - x_7x_8) \\ & (x_9 + x_{10} - x_9x_{10})x_{11}x_{12}x_{13}x_{14}x_{15}) \end{aligned}$$

Ved bruk av Poisson prosess [81] har vi funnet feilratene til komponentene i systemet (se tabell 3, rad«Feilrate før endring»).

Komponent nr.:	**Feilrate før endring:**	**Feilrate etter endring:**
$x_1(t_0)$	0.86	0.86
$x_2(t_0)$	0.63	0.63
$x_3(t_0)$	0.63	0.63
$x_4(t_0)$	0.99	0.99
$x_5(t_0)$	0.63	0.63
$x_6(t_0)$	0.86	0.86
$x_7(t_0)$	1	0.63
$x_8(t_0)$	0.99	0.63
$x_9(t_0)$	1	0.63
$x_{10}(t_0)$	1	0.63
$x_{11}(t_0)$	1	0.63
$x_{12}(t_0)$	0.95	0.95
$x_{13}(t_0)$	0.99	0.99
$x_{14}(t_0)$	0.63	0.63
$x_{15}(t_0)$	0.63	0.63

Tabell 3: Oversikt over pålitelighet i komponentene i systemet med endringer av verdier for x_7, x_8, x_9x_{10} og x_{11}. Lavere verdi i kategorien «feilrate», vil bety høyere pålitelighet for komponenten i en tidsperiode t_0.

Verdiene settes så inn i systemets strukturfunksjon: Utledet strukturfunksjon blir:

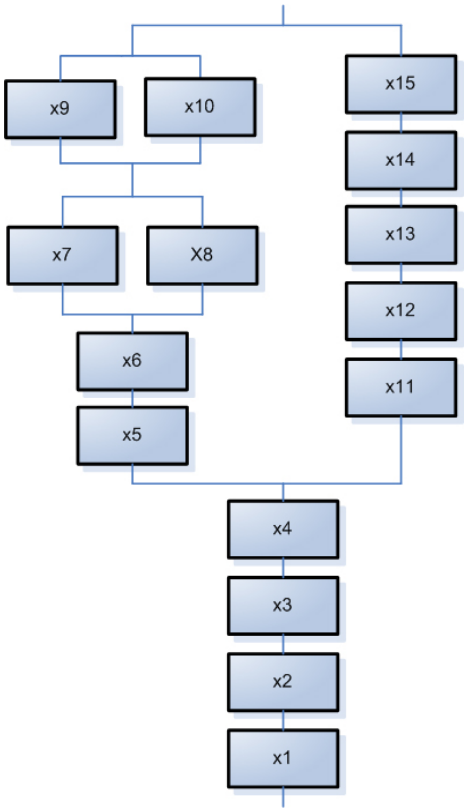
$$\begin{aligned} p_S(t) &= 0.86 \cdot 0.63 \cdot 0.63 \cdot 0.99(0.63 \cdot 0.86(1 + 0.99 - 1 \cdot 0.99) \\ &\quad (1 + 1 - 1 \cdot 1) + 1 \cdot 0.95 \cdot 0.99 \cdot 0.63 \cdot 0.63 - 0.63 \cdot 0.86 \\ &\quad (1 + 0.99 - 1 \cdot 0.99)(1 + 1 - 1 \cdot 1)1 \cdot 0.95 \cdot 0.99 \cdot 0.63 \cdot 0.63) \\ &= 0,247920453 \end{aligned}$$

Vi finner at systemet har en total pålitelighet på ca 0,248. Det presenterte tallet gir oss et anslag på total pålitelighet ved systemet. Tallet beskriver at det er mulighet for at en feilkilde kan inntreffe hver fjerde dag, og således medføre at systemet svikter.

Ved å utføre en analyse av påliteligheten til komponentene, finner vi at x_7, x_8, x_9, x_{10} og x_{11} inntreffer ofte og medfører at vi kan identifisere komponentene som å ha svak pålitelighet, og sannsynligvis områder hvor det bør vurderes tiltak. Tar vi utgangspunkt i tabell 3 kan vi lett oppfatte det som mest hensiktsmessig å utbedre eller iverksette tiltak på komponentene/områdene x_7, x_8, x_9, x_{10} og x_{11}, fordi områdene har høy feilrate.
La oss anta at vi velger å innføre tiltak på nevnte områder på bakgrunn av feilratene. Over en tidsperiode har vi redusert feilratene til 0.63 på henholdsvis alle komponentene x_7, x_8, x_9, x_{10} og x_{11} (Se tabell 3 rad «Feilrate etter endring»). Ved å innføre de nye feilratene i strukturfunksjonen kan vi beregne ny total systempålitelighet.
En innsetting av de nye ratene i utledet strukturfunksjon gir følgende resultat:

$$\begin{aligned} p_S(t) &= 0.86 \cdot 0.63 \cdot 0.63 \cdot 0.99(0.63 \cdot 0.86(0.63 + 0.63 - 0.63 \cdot 0.63) \\ &\quad (0.63 + 0.63 - 0.63 \cdot 0.63) + 0.63 \cdot 0.95 \cdot 0.99 \cdot 0.63 \cdot \\ &\quad 0.63 - 0.63 \cdot 0.86(0.63 + 0.63 - 0.63 \cdot 0.63) \\ &\quad (0.63 + 0.63 - 0.63 \cdot 0.63)0.63 \cdot 0.95 \cdot 0.99 \cdot 0.63 \cdot 0.63) \\ &= 0,21823742 \end{aligned}$$

Vi finner at systemet, etter innføring av tiltak, har en total pålitelighet på ca 0,218. Tidligere hadde systemet en total pålitelighet på ca 0,248. Ved å iverksette tiltak som senker feilratene på feilkildene x_7, x_8, x_9, x_{10} og x_{11}, har vi fått en kvantitativ beskrivelse av at systemet har en bedre pålitelighet, og således kan det i utgangspunktet se ut som tiltakene har vært effektive og hensiktsmessig. Før vi iverksatte tiltak viste den pålitelighetsmessige beskrivelsen at en feilkilde kunne inntreff ca hver fjerde dag. Etter iverksettelse av tiltak, viser den pålitelighetsmessige beskrivelsen at systemet kan feile omtrent hver femte dag.
Den strukturmessige plasseringen av komponentene av stor betydning for systemets pålitelighet, og derfor noe som bør tas i betraktning ved vurdering av pålitelighet. Ved å benytte Birnbaums pålitelighetsmessige mål kan vi utføre en bedre analyse av systemet. Ved å partialderivere systemstrukturen på komponentene, kan vi finne den komponenten som har størst betydning for påliteligheten i systemet. (I stedet for å ta utgangspunkt i feilraten til komponentene og iverksette tiltak på bakgrunn av den kvantitative beskrivelsen av feilratene).
La oss anta at vi istedet velger å benytte oss av Birnbaums pålitelighetsmessige mål. Vi lar feilratene på komponentene x_7, x_8, x_9, x_{10} og x_{11} være slik de i utgangspunktet var før en endring (se tabell 4 ved raden «F.rate$_0$»).



Figur 27: Viser pålitelighetsnettverket i et system.

Komp.nr.:	**F.rate$_0$:**	**Birn.$_0$:**	**F.rate$_1$:**	**Birn.$_1$:**	**F.rate$_2$:**	**Birn.$_2$:**	**F.rate$_3$:**	**Birn.$_3$:**
$x_1(t_0)$	0.86	0.2800	0.86	0.1911	0.86	0.1804	0.63	0.1304
$x_2(t_0)$	0.63	0.3823	0.43	0.3823	0.43	0.2609	0.43	0.1911
$x_3(t_0)$	0.63	0.3823	0.63	0.2609	0.43	0.2609	0.43	0.1911
$x_4(t_0)$	0.99	0.2433	0.99	0.1660	0.99	0.1133	0.99	0.0830
$x_5(t_0)$	0.63	0.1821	0.63	0.1243	0.63	0.0848	0.63	0.0621
$x_6(t_0)$	0.86	0.1334	0.86	0.0910	0.86	0.0621	0.86	0.0455
$x_7(t_0)$	1	0.0011	1	0.0007	1	0.0005	1	0.0003
$x_8(t_0)$	0.99	0	0.99	0	0.99	0	0.99	0
$x_9(t_0)$	1	0	1	0	1	0	1	0
$x_{10}(t_0)$	1	0	1	0	1	0	1	0
$x_{11}(t_0)$	1	0.0577	1	0.0394	1	0.0269	1	0.0197
$x_{12}(t_0)$	0.95	0.0608	0.95	0.0415	0.95	0.0283	0.95	0.0207
$x_{13}(t_0)$	0.99	0.0583	0.99	0.0398	0.99	0.0271	0.99	0.0199
$x_{14}(t_0)$	0.63	0.0917	0.63	0.0626	0.63	0.0427	0.63	0.0313
$x_{15}(t_0)$	0.63	0.0917	0.63	0.0626	0.63	0.0427	0.63	0.0313
Iterasjon	1		2		3		4	
Tot.Sys. pålitelig.	0.24792		0,164412		0.112217		0.0822	

Tabell 4: Oversikt over pålitelighet i komponentene i systemet. Lavere verdi i kategorien «feilrate», vil bety høyere pålitelighet for komponenten. Tallet beskriver pålitelighet over en gitt tidsperiode t_0. (I tabellen brukes «Birn.» som er forkortelse av «Birnbaums mål» og «F.rate» som betyr «feilrate»).

Vi velger deretter å innføre tiltak på områdene/komponentene som har høy Birnbaums mål. Dette finner vi ved å utføre partialderivering av komponentene x_i på strukturfunksjonen:

$$p_S(t) = I^B(i|t_0) = \frac{\partial h(\underline{p}(t_0))}{\partial p_i(t_0)}$$

for $i = 1, 2, \ldots, 15$.

Dette gir den pålitelighetsmessige betydningen av komponentene ved tidspunkt t_0. Vi finner følgende betydning av komponentene beskrevet i tabell 4 ved raden «Birn$_0$». Ved å studere raden «Birn$_0$» identifiserer vi at komponentene x_2 og x_3 er utsatte systemområder (fordi Birnbaums mål er høy). La oss anta at vi har iverksatt tiltak slik at feilraten er redusert fra 0.63 til 0.43 for komponent x_2 (Beskrevet i tabell 4 ved andre iterasjon og raden «F.rate$_1$»). Vi setter således den nye feilraten inn i systemets strukturfunksjon:

$$\begin{aligned} p_S(t) &= 0.86 \cdot 0.43 \cdot 0.63 \cdot 0.99(0.63 \cdot 0.86(1 + 0.99 - 1 \cdot 0.99) \\ &\quad (1 + 1 - 1 \cdot 1) + 1 \cdot 0.95 \cdot 0.99 \cdot 0.63 \cdot 0.63 - 0.63 \cdot 0.86 \\ &\quad (1 + 0.99 - 1 \cdot 0.99)(1 + 1 - 1 \cdot 1)1 \cdot 0.95 \cdot 0.99 \cdot 0.63 \cdot 0.63) \\ &= 0,164412 \end{aligned}$$

Vi finner at systemet, etter innføring av tiltak, har nå en total pålitelighet på ca 0,164. Ved å kun å innføre tiltak på bakgrunn av feilratene identifiserte vi at systemet totale pålitelighet økte fra ca 0,248 til ca 0,218. Men ved å innføre et tiltak på bakgrunn av Birnbaums mål som reduserte feilraten på feilkilden x_2, har vi fått en kvantitativ beskri-

velse av at systemet har en bedre pålitelighet (ca 0,164). Dette kan indikere at systemet er redusert fra å svikte hver femte dag, til kun å kunne svikte hver 6-7 dag. Således har tiltaket fungert mer hensiktsmessig enn ved å innføre tiltak på komponenter med høyest feilrate. Vi gjentar den samme prosessen ved å identifisere den neste komponenten med høyest Birnbaums mål. Dette gjøres ved å gjenta partialderivering med den nye feilraten. Vi identifiserer at komponenten x_3 er den komponenten som har høyest Birnbaums mål. Anta at vi igjen har innført et tiltak som senker feilraten på komponenten til fra 0.63 til 0.43. Vi innfører igjen ratene i systemstrukturen, og får følgende resultat:

$$\begin{aligned} p_S(t) &= 0.86 \cdot 0.43 \cdot 0.43 \cdot 0.99(0.63 \cdot 0.86(1 + 0.99 - 1 \cdot 0.99) \\ &\quad (1 + 1 - 1 \cdot 1) + 1 \cdot 0.95 \cdot 0.99 \cdot 0.63 \cdot 0.63 - 0.63 \cdot 0.86 \\ &\quad (1 + 0.99 - 1 \cdot 0.99)(1 + 1 - 1 \cdot 1)1 \cdot 0.95 \cdot 0.99 \cdot 0.63 \cdot 0.63) \\ &= 0,112217 \end{aligned}$$

Ved å innføre tiltak som reduserte feilratene på komponentene x_2 og x_3, redusert vi systemet fra å svikte hver femte dag (beskrevet ved total system pålitelighet på 0,24792, ved iterasjon 1 i tabell 4), til kun å svikte ca hver niende dag (total system pålitelighet ca 0,112, beskrevet ved iterasjon 2 i tabell 4).
Ved å gjenta den samme prosessen, kan vi kontinuerlig identifisere den neste komponenten som det bør iverksette tiltak på. Vi studerer på nytt tabell 4 og raden «$Birn_2$», og identifiserer at komponent x_1 er den komponenten som har høyest Birnbaums mål. Og hvor det enda ikke er iverksatt tiltak. Anta at vi har iverksatt tiltak slik at feilraten på komponent x_1 er redusert fra 0.86 til 0.63. Vi setter de nye feilratene inn i systemets strukturfunksjon:

$$\begin{aligned} p_S(t) &= 0.63 \cdot 0.43 \cdot 0.43 \cdot 0.99(0.63 \cdot 0.86 \\ &\quad (1 + 0.99 - 1 \cdot 0.99)(1 + 1 - 1 \cdot 1) + 1 \cdot 0.95 \cdot 0.99 \cdot 0.63 \cdot \\ &\quad 0.63 - 0.63 \cdot 0.86(1 + 0.99 - 1 \cdot 0.99)(1 + 1 - 1 \cdot 1)1 \cdot \\ &\quad 0.95 \cdot 0.99 \cdot 0.63 \cdot 0.63) \\ &= 0,082206 \end{aligned}$$

Ved å innføre tiltak på komponent x_1 har vi økt systemet pålitelighet ytterligere. Det kan beskrives at en uønsket hendelse er redusert fra å inntreffe ca hver niende dag(0,112) til hver tolvte dag(0,082). Dette viser at det kan være mer hensiktsmessig å iverksette tiltak på en sentralt plassert komponent med middels feilrate, i forhold til en komponent er usentralt plassert med høy feilrate.
I et tilfelle der to komponenter er plassert i en parallell-struktur, vil den komponenten som har høyest feilrate være den viktigste. Om to komponenter er plassert i en serie-struktur, vil den komponenten med lavest pålitelighet være den komponenten som har størst betydning for systemet. Noe som stemmer med at vi kan anse en serie-stuktur som en kjedestruktur, og en kjede er aldri sterkere enn det svakeste leddet. Samtidig vil denne komponenten være mer utsatt enn komponenter i en parallell-struktur. Fordi det i en parallell-struktur er nødvendig at flere hendelser inntreffer.

6.10 Et eksempel på analyse av et fremtidig system

Med utgangspunkt i dagens modell kan vi utføre en analyse på et fremtidig system. Det er nødvendig å konstruere feiltrær som stemmer overens med ny IKT-infratruktur, organisasjonsoppbygning osv. Deretter konverteres feiltrærne til et pålitelighetsnettverk, som i figur 28.
Ved å skalere opp antallet brukere, arbeidsstasjoner osv, og skalere ned antallet servere, tekniske installasjoner osv., kan det utføres en analyse av det fremtidige systemet. En slik analyse kan bidra til å identifisere ny, og synliggjøre allerede kjent sårbarhet og risiko et fremtidig system. Vi identifiserer følgende alternativer for å studere et fremtidig system:

- Forsøke å redusere feilkildene med høy feilrate.
- Benytte Birnbaums mål for å heve påliteligheten til systemet.
- Analysere effekten av å skalere systemet ved bruk av Poisson prosess.
- Endre og analysere systemstrukturen (oppbygning av infrastruktur osv.).

Det første punktet er beskrevet tidligere i oppgaven og viste relativ liten positiv effekt på systemets totale pålitelighet. Punkt 2 skissert i kap. 6.9.6 har gitt gode resultater. Ved å skalere systemet etter fremtidig løsning, kan vi bekrefte sårbarhet og få fremhevet allerede kjent sårbarhet. Denne type tilnærming vil sannsynligvis kun resultere i en økt feilfrekvens ved feilkildene. Ved å benytte oss av det siste punktet kan vi redusere feilratene på komponentene i systemet. Deretter kan vi måle den totale systempåliteligheten og se hvilken effekt endringen har.

Følgende skisserer hvordan det kan utføres analyse av et fremtidig system. Anta at vi har innført et tiltak på komponentene x_1 og x_2. Tiltaket har innført en ny komponent, x_{16}. Innføring av tiltaket har identifisert systemstrukturen $\phi(\underline{X})$ på bakgrunn av pålitelighetsnettverk i figur 28. Deretter har vi identifisert at de forskjellige komponentene/systemdelene har følgende feilrater presentert i tabell 5 raden «Feilrater etter endring».

Strukturfunksjonen blir:

$$\phi(\underline{X}) = (X_{16} \amalg (X_1X_2))X_3X_4((X_5X_6(X_7 \amalg X_8)(X_9 \amalg X_{10})) \amalg X_{11}X_{12}X_{13}X_{14}X_{15}) \quad (6.8)$$

Utledet strukturfunksjon blir:

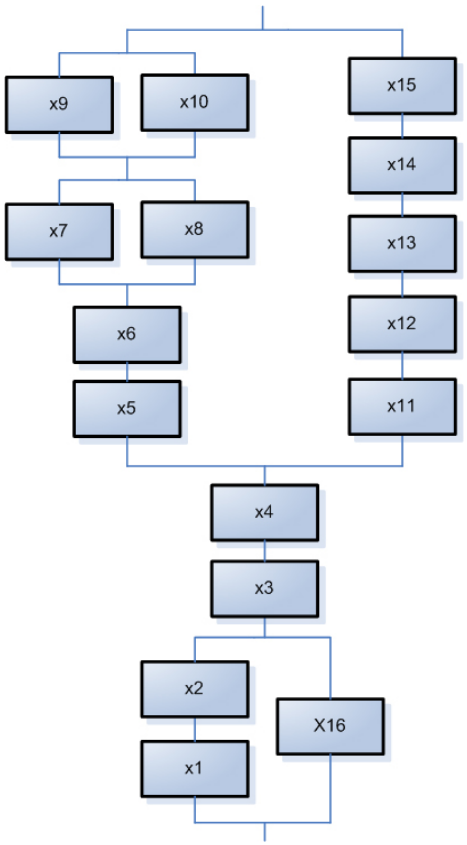
$$\begin{aligned} p_S(t) \quad = \quad & (x_{16} + (x_1x_2) - x_{16}(x_1x_2))x_3x_4 \\ & (x_5x_6(x_7 + x_8 - x_7x_8)(x_9 + x_{10} - x_9x_{10}) \\ & +x_{11}x_{12}x_{13}x_{14}x_{15} - x_5x_6(x_7 + x_8 - x_7x_8) \\ & (x_9 + x_{10} - x_9x_{10})x_{11}x_{12}x_{13}x_{14}x_{15}) \end{aligned}$$

Ved å benytte Poisson prosess [81] har vi funnet feilratene til komponentene i systemet (se tabell 3 rad«Feilrate før endring»).

Feilratene settes så inn i systemets strukturfunksjon:

$$\begin{aligned} p_S(t) &= (0.36 + (0.36 \cdot 0.36) - (0.36 \cdot (0.36 \cdot 0.36)) \\ & \quad 0.63 \cdot 0.63 \cdot 0.99(0.63 \cdot 0.86(1 + 0.99 - 1 \cdot 0.99) \\ & \quad (1 + 1 - 1 \cdot 1) + 1 \cdot 0.95 \cdot 0.99 \cdot 0.63 \cdot 0.63 - 0.63 \cdot 0.86 \\ & \quad (1 + 0.99 - 1 \cdot 0.99)(1 + 1 - 1 \cdot 1)1 \cdot 0.95 \cdot 0.99 \cdot 0.63 \cdot 0.63)) \\ &= 0,19804 \end{aligned}$$

Vi ser at ved å innføre et tiltak på komponentene x_1 og x_2 har vi økt pålideligheten til systemet til ca 0,198. Dermed kan vi se at feilraten til systemet er redusert fra henholdsvis ca 0,248 til 0,198. Dette skisserer at ved å innføre et tiltak på komponentene x_1 og x_2, kan vi sannsynligvis øke systemets totale pålitelighet. Dette kan illustrere at det kan være hensiktsmessig å endre systemstrukturen i et fremtidig system. Videre kan vi finne den pålitelitelighetsmessige betydningen av komponentene ved bruk av Birnbaums målendre.
Denne typen tilnærming tilrettelegger for å kunne identifisere svakheter, risiko og sårbarhet ved et fremtidig system, slik at analytikerne kan justere og endre et fremtidig system før en løsning implementeres. Utfordringen med en slik type tilnærming, er å kunne konstruere riktige feiltrær. Det er beskrevet at det ofte kan være vanskelig å konstruere et feiltre av et system som er i konseptfasen [65]. Samtidig kan det ofte være vanskelig å



Figur 28: Pålitelighetsnettverk for et fremtidig system.

Komponent nr.:	**Feilrate før endring:**	**Feilrater etter endring:**
$x_1(t_0)$	0.86	0.36
$x_2(t_0)$	0.63	0.36
$x_3(t_0)$	0.63	0.63
$x_4(t_0)$	0.99	0.99
$x_5(t_0)$	0.63	0.63
$x_6(t_0)$	0.86	0.86
$x_7(t_0)$	1	1
$x_8(t_0)$	0.99	0.99
$x_9(t_0)$	1	1
$x_{10}(t_0)$	1	1
$x_{11}(t_0)$	1	1
$x_{12}(t_0)$	0.95	0.95
$x_{13}(t_0)$	0.99	0.99
$x_{14}(t_0)$	0.63	0.63
$x_{15}(t_0)$	0.63	0.63
$x_{16}(t_0)$	-	0.36

Tabell 5: Oversikt over pålitelighet i komponentene i systemet. Et sikkerhetstiltak har redusert feilratene for komponentene x_1 og x_2, og krevd innføring av komponenten x_{16}. Lavere verdi i kategorien «feilrate», betyr høyere pålitelighet for komponenten i en tidsperiode t_0.

kvantifisere korrekte rater på enkelte områder. Men ved å konstruere feiltrær og å utføre partialderivering med gode feilrater, kan vi identifisere systemområder som det kan være hensiktsmessig å utarbeide tiltak for. Samtidig kan en slik tilnærming tilrettelegge for å vurdere andre og bedre løsninger, eller hvilke tiltak som bør iverksettes før systemet er ferdig utviklet.

7 Analyse av resultat og gjennomføring

I dette kapitlet beskrives og diskuteres erfaringer og resultater ved metodene.

7.1 Erfaringer ved arbeidet som er gjennomført

Vi begynte vår undersøkelse ved å studere lovverket innenfor helsesektoren. Lovverket la retningslinjer og definerte krav til IKT-sikkerhet og informasjonssikkerhet. Deretter ble det gjennomført et studie av helseforetaket. Studiet ga svar på teknologiske begrensninger og løsninger. Raskt erfarte vi at lovverket la ytterligere premisser og styrte både krav til organisering og struktur. Det ble vurdert hvilken metodisk tilnærming som kunne gi best resultat, basert på begrensninger og ressurser i prosjektet. Vi vurderte ulike alternative tilnærminger, eksempelvis analyse av brukerkrav, kravspesifikasjoner, ulike standarder for sikkerhet osv. Det ble valgt en tilnærming satt sammen av flere forskjellige områder. Bakgrunnen og ønsket var å oppnå en bredde i resultatet. Det var essensielt å forstå hvordan systemene og arbeidsoppgavene var relatert til hverandre, både infrastrukturmessig og hvordan systemene påvirker hverandre på tvers av virksomhetsnivåer. Samtidig var det nødvendig å forstå dette ut fra et juridisk perspektiv.

7.2 Kort diskusjon av resultatene

Sluttresultatet i analysen lar seg prege av løsninger ved studert helseforetak. Det vil sannsyndligvis være både sårbarhet og risiko for helsesektoren i en overgang til en sentralisert løsning som ikke kommer frem i vår analyse. For å bekrefte identifiserte sårbarheter og risiko kan det være nødvendig med en mer detaljert og dypere analyse, både av geografisk beliggenhet, kabling, valg av komponenter og oppbygning av infrastruktur osv. En detaljert analyse av hver lokasjon vil sannsynligvis avdekke, bekrefte eller påpeke risiko og sårbarhet som er spesifikk for hver lokasjon. Dette er trolig et arbeid må utdypes. Samtidig bør arbeidet gjennomføres av personer som har inngående kjennskap til systemet/ene. De presenterte analyseresultatene kan således benyttes som en supplerende og beskrivende del, og kan sannsynligvis ansees som en del av et større arbeid eller et utgangspunkt for en dypere og mer detaljert analyse.

7.2.1 Om den kvantitative beskrivelsen

Den kvantitative beskrivelsen av pålitelighet gir et anslag på total pålitelighetenen til systemet. Feilkildene identifisert i systemet er beskrevet som vanskelig å kvantifisere med korrekte beskrivelser. Dette vil redusere analyseresultatets pålitelighet. Vi velger å beskrive noen punkter som vanskeliggjør en korrekt kvantitative beskrivelse:

- Høy menneskelig involvering.
- Liten grad av automasjon i systemet.
- Strukturell plassering av komponenter og enheter i systemet.
- Høy kompleksitet i systemet.

Ved konstruksjon av feiltrærne er det tatt utgangspunkt i både tilsiktede (security) og ikke-tilsiktede (safety) hendelser. Menneskelig involvering kombinert med den strukturelle plasseringen av komponentene påvirker den kvantitative beskrivelsen [81]. Sikkerhet må beskrives for å være dynamisk [43]. Det er beskrevet at det er vanskelig å gjøre en god analyse av et system som har stor grad av dynamiske hendelser [65]. Ved å utføre en analyse av et system som har større grad av automasjon og mindre grad av menneskelig involvering, vil tallet sannsynligvis være mer korrekt. Samtidig vil en analyse av et system som har en mindre kompleks systemstruktur gi et mer pålitelig resultat. Det vil også være vanskelig å utføre en god analyse av et fremtidig system [65]. Det kan beskrives at prediksjon av fremtidige egenskaper som er basert på måling av observerte egenskaper ved et eksisterende system, kan medføre og resultere i store unøyaktigheter. Dette vil trolig vanskeligjøre muligheten til å utføre en god analyse, og samtidig medføre en ugyldighet i resultatet.

7.3 Resultater og erfaringer ved å velge NSM-ROS2004

Det ble diskutert at «generelt sett, blir risiko- og sårbarhetsvurderinger i noen virksomheter gjennomført svært enkelt, og ofte veldig overordnet»[1]. Den kanskje mest vanlige formen for analyse ved mindre bedrifter som ikke benytter seg av et rammeverk, er at driftspersonell i en bedriften setter seg ned en stund og tenker høyt rundt hvilke trusler de ser for seg som mest relevante, og hvor sannsynlig det er at systemet bryter sammen som følge av disse.
Vi ønsket å gjennomføre en friere og mer overordnet analyse av systemet, for å avdekke om en slik type analyse ville resultere i andre funn enn en dypere og mer omfattende metode. Det ble derfor valgt å benytte den kvalitative metoden NSM-ROS2004.

Det første vi erfarte med NSM-ROS2004 var at metoden verken definerer strenge krav eller legger bestemte føringer for hvordan og hvilke systemområder skal analyseres. Derimot beskriver metoden hvordan analytikerne selv kan prioritere arbeidet. Metoden tilrettelegger for å kunne fokusere på områder referansegruppa selv mener er av kritisk betydning. Dette betyr at referansegruppa har relativt frie muligheter for å identifisere risiko og trusler. Prosjektdeltakerne i referansegruppa bør derfor ha god kjennskap til systemet, slik at fokuset blir på de «riktige» områdene. Samtidig oppfatter vi det som en fallgruve at de erfaringer som referansegruppa sitter med, ofte ikke medfører identifisering av nye sårbarheter og risikoer. Vår oppfatning var at diskusjonen under ROS-møtet ofte resulterte i en ny vurdering av allerede kjent sårbarhet eller risiko, og at diskusjonen ofte ble dratt ut til områder som var delvis utenfor diskusjonstemaet.

Ved vurdering og definisjon av sannsynlighet og konsekvens oppfattet vi raskt at vurderingene ble preget av erfaringer som referansegruppa satt med. Vurderinger ble fastsatt ved at referansegruppa diskuterte og vurderte sannsynlighet og konsekvens seg i mellom. Ofte ble fastsetting av konsekvens og sannsynlighet gjort på bakgrunn av personlige vurderinger og svært lite statistisk/dokumentert materiale. Noe som vi oppfatter som manglende sikkerhet i de empiriske dataene. Keong [11] beskriver at slike typer kvalitative metoder mangler muligheten til å se avhengighet mellom hendelser, noe som i vårt tilfelle ofte kanskje ble avgjørende for en helhetsvurdering av konsekvenser.

[1] Møte med Håvard Fridheim, 12.12.2005

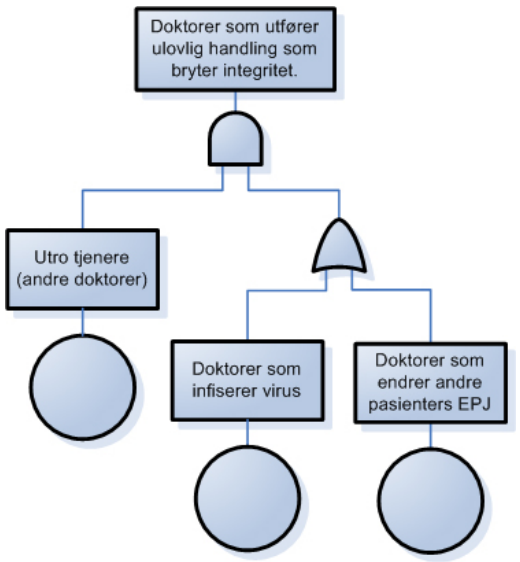
7.4 Resultater og erfaringer ved å velge FTA

Hensikten med å velge FTA som metode var primært å kunne visualisere kombinasjoner av sårbarheter og trusler. Ved å kombinere en tankegang som benyttes i trusseltre, angrepstre og feiltre ønsket vi å dekke et bredere aspekt i analysen. Samtidig var det også et mål å dekke både tilsiktet (security) og ikke-tilsiktet (safety) angrep. Som beskrevet er det ofte et resultat at analytikere tvinges inn i et det metodisk rammeverk, og at dette preger resultatet[2]. Vi valgte å benytte oss av en annen type tilnærming enn det vi hadde benyttet ved den kvalitative NSM-ROS2004. Ved å benytte en tilnærming basert på både angrep, trusler og risiko, ønsket vi å kunne oppnå en bredere og mer helhetlig tilnærming enn det vi oppnådde med NSM-ROS2004-metoden.

FTA er en metode vi kunne benytte som kombinasjon av kvalitativ og kvantitativ tilnærming. Vår måte å benytte FTA i en kvalitativ tilnærming, utfordret oss til å forstå en mer helhetlig tilnærming til kombinasjoner av trusler og risiko. Dette fordret oss til å bevege oss til systemområder som ikke ble belyst i første ROS-analyse. Den deduktive tilnærmingen som FTA benytter ved å gjenta spørsmålet «Hva er årsakene?», ga mulighet for å identifisere flere potensielle feilkilder i forskjellige systemdeler. Noe som således resulterte i identifisering av nye sårbarheter og trusler. Et eksempel på dette er kombinasjonene av aspektene «ansettelses forhold» og «tilgangskontroll». Denne type tilnærming og kombinasjon ga oss som analytikere bedre syn på hvor sårbar virksomheten var for virksomhetens praksis ved informasjonssikkerhet.

FTA i en kvantitativ tilnærming ble gjennomført ved å tillegge bladnodene rater. Feiltrærne kunne for eksempel inneholde en kombinasjon av feilkildene «Utro tjenere», «Infisering av virus» og «Uautorisert endring av andre pasienters EPJ»,se figur 29. Ved en kvalitativ analyse kunne en slik tilnærming visualisere hvilke elementer som kreves for å gjennomføre et angrep. Ved den kvantitative analyse ser vi raskt at det blir en dobbeltlagring av ratene. Kombinasjonen «Utro tjenere» og «Infisering av virus», og «Utro

[2]E-post Håvard Fridheim, 22.02.2006



Figur 29: Skissen viser et eksempel på dobbeltlagring av rater.

tjenere» og «Uautorisert endring av andre pasienters EPJ», vil hver for seg inneholde en rate som beskriver samme feilkilde. «Infisering av virus» vil være en rate som beskriver antallet doktorer som har infisert nettverket med virus over en tidsperiode. Samtidig vil feilkilden «Utro tjener» inneholde samme rate. Det vil også skje en dobbeltlagring ved identifisering av de minimale kuttmengdene i feiltreet. Slik at verdiene i kuttmengden blir feil. Derfor valgte vi å revidere feiltrærne for å gjennomføre en kvantitativ analyse av systemet. Den kvantitative analysen og beskrivelsen av rater, resulterte i identifisering av både nye, og en markering av sårbarheter funnet i den kvalitative analysen. Disse sårbarhetene ble bedre visualisert i den kvantitative analysen. Eksempelvis hvor mange ganger det hadde oppstått tap av strøm på en server i løpet av en tidsperiode, eller hvor mange ganger et antall brukere har mistet passordet i løpet av en tidsperiode. Ved å tillegge feilkildene rater og utføre partial-derivering av verdien kunne vi finne hvilken betydning av feilkildene har for systemet. Ved å justere parametere i strukturfunksjonen kunne vi videre utføre en følsomhetsanalyse av feiltrærne. Følsomhetsanalysen kunne således beskrive hvilken betydning den enkelte feilkilden har for den totale påliteligheten i systemet. Ved å utføre en følsomhetsanalyse kunne vi beskrive hvilke systemområder/feilkilder som burde utbedres for å gi mest økning i den totale påliteligheten til systemet, eller områder hvor det burde innføres ny rutine/praksis i sikkerhetsarbeidet.

Vår erfaring er at den kvalitative tilnærmingen, ble den analysen som ga mest utbytte med tanke på tid og ressurser. Konstruksjonen av feiltrærne visualiserte sårbarheter og trusler på en relativ enkel måte. Denne typen analyse ga muligheter for å se systemet fra flere forskjellige aspekter, og krevde således at vi som analytikere ble tvunget til å se systemet og systemområder fra forskjellige perspektiver. Den kvantitative tilnærmingen ved FTA ble et tidkrevende og omfattende arbeid. Det var vanskelig å beskrive eksakt hvordan systemet burde bygges opp med det fokuset vi hadde. Den største utfordringen var involveringen av menneskene som forvalter eller som bruker av systemet. Det er vanskelig å gjøre gode kvantitative estimeringer og beskrivelser hvor den menneskelige faktor er betydelig involvert. Den kanskje største utfordringen med FTA i en kvantitativ tilnærming, var å kunne konstruere riktig og gode feiltrær. Utfordringen ble ytterligere vanskelig ved konstruksjon av feiltre for et fremtidig system. Det er beskrevet at det ofte vanskelig å konstruere et riktig feiltre av et system som er i konseptfasen [65]. Plasseringen av feilkildene i feiltreet ble ofte avgjørende for hvilken pålitelighetsmessig betydning feilkilden fikk. Spørsmålet som vi ofte resulterte i å spørre oss selv, var om feilkilden var riktig plassert i systemet, og hvilken betydning dette medførte. Dette, i kombinasjon av lite statistisk materiale, gjorde den kvantitative analysen vanskelig. Vår erfaring er at FTA egner seg bedre på mindre systemer. Samtidig er det en stor fordel om det eksisterer gode statistiske data ved systemet, og at involvering av den menneskelige faktor er minimal.

En svakhet eller manglende del ved metoden, er å kunne gjøre vurderinger av hvilke tiltak som er mest hensiktsmessig med tanke på kostnad. Kostnad er en essensiell del i vurdering av alternative tiltak. De fleste sikringstiltak har en kostnad. Investeringskostnadene ved tiltakene må veies mot det potensielle tapet som et sikkerhetsbrudd kan medføre. Det kan også i visse tilfeller være vanskelig å kvantifisere hvilke kostnader et eventuelt sikkerhetsbrudd kan påføre virksomheten. Dette er noen metoden ikke tar forbehold om, og dermed vanskeliggjør vurdering og valg av hensiktsmessige tiltak og løsninger.

7.4.1 Kort om valg av topphendelse

I vår tilnærming til FTA valgte vi å beskrive en topphendelse til å være brudd på elementene konfidensialitet, integritet og tilgjengelighet. Det var i utgangspunktet to hensikter med denne tilnærmingen. Den først hensikten var å kunne beholde fokus på informasjonssikkerhet i hele prosessen. Den andre hensikten var å kunne bryte ned systemet i mindre og mer oversiktelige deler. I vår tilnærming valgte vi å definere et brudd på elementene som en uønsket hendelse, og således meføre tap av informasjonssikkerhet. Ved å ta utgangspunkt konfidensialitet, integritet og tilgjengelighet, og for så å dele systemet inn i bruksområder («brukerside», «infrastruktur og kommunikasjon», og «drift/serverside»), kunne vi enklere identifisere konkrete uønskede hendelser. Et annet alternativ kunne være å ta utgangspunkt i indikatorer for informasjonssikkerhet [82], og benytte indikatorene som topphendelser i kombinasjon ulike måleparametere.

7.4.2 Birnbaums mål

Vi valgte å benytte Birnbaums mål for å finne den pålitelighetsmessige betydningen av komponenter i systemet. Det finnes flere forskjellige probalistiske varianter for å finne pålitelighetsmessig mål. To andre alternativer som ofte blir benyttet er «Kritisk betydning» og Vesely-Fussells mål [81]. Valg av definisjoner for å finne pålitelighetsmessig betydning, vil ofte være avhengig av hvilken interesse som foreligger. Holen [81] m.fl. beskriver at «om analytikerne ønsker å finne ut hvilke komponenter som bør forbedres, er Birnbaums mål mest egnet. Ønsker en derimot å finne hvilke komponenter som er årsak til at systemet får en svikt, er Kritisk betydning, eller Vesely-Fussells bedre alternativer». Hvert av alternativene har opp igjennom årene fått noe kritikk. Birnbaums mål har fått noe kritikk for at det ikke tas hensyn til kostnadene ved å utbedre komponentene. Et eksempel er om kostnadsrammene er satt, så kan det i noen situasjoner være langt mer hensiktsmessig å utbedre andre komponenter som har mindre betydning for systemet.

7.5 Drøfting av metodene

En bedrift som har bygget opp sin virksomhet rundt et IKT-system, vil sannsynligvis være forberedt på at organisatoriske forandringer vil medføre forandringer for systemet. Informasjonen som har et sikkerhetsbehov og som er skjermingsverdig, vil aldri være statisk over tid. Det vil ofte være et tilsig av ny informasjon og nye objekter som har behov for beskyttelse og sikkerhet. Derfor vil det under organisatoriske og IKT-messige endringer være viktig å kjenne til hvilke faktorer som stadig påvirker en virksomhets risikobilde og skjermingsverdig informasjon. Ved bruk av mindre frie metodiske tilnærminger blir de personene som sitter i referansegruppa tvunget til å forstå og vurdere flere risikoområder. Samtidig vil det være mindre muligheter for å kunne utelate deler som har lav verdi for analysen. På den andre siden vil et slikt arbeid sannsynligvis kreve mer tid og flere ressurser. Slik at valg av tilnærming og metode ofte baseres på tilgjengelige ressurser og tid.

NSM-ROS2004 er en metode som tilrettelegger for at analytikerne selv kan prioritere og velge systemområder som er av størst betydning. Den frie tilnærmingen og vurderingen av områder, kan føre til at referansegruppa raskt kommer frem til formålet med analysen. Og dermed raskere oppnår resultater, for å kunne ta beslutninger om hvor tiltak bør iverksettes. På den andre siden kan det være en fallgruve at referansegruppa selv velger å prioritere områder, eller velger bort områder, og dermed ikke blir «tvunget» ut

på områder som kan inneholde uidentifiserte og kritiske risikoer/trusler. Resultatet kan være at de erfaringer og vurderinger som blir gjort i referansegruppa ofte gjengår i hver ROS-analyse.

Vår tilnærming ved å benytte FTA som en delvis kombinasjon av trusseltre, angrepstre og feiltre, ga oss mulighet til å se avhengighet mellom faktorer, komponenter og systemer. Samtidig ga tilnærmingen muligheten til å visualisere systemet gjennom et feiltre. Konstruksjonen av feiltreet var uavhengig av om feilkildene var en risiko, en trussel eller en angrepsvei. Noe som tilrettela for at vi kunne se avhengigheten mellom hendelser og feilkilder, og hvilke forutsetninger som kreves for at en hendelse skal inntreffe. Samtidig kunne vi beskrive rater på bladnodene/feilkildene i feiltreet. Ratene kunne indikere om området var et utsatt området, og kunne således bli vurdert i forhold til hva virksomheten eller driftpersonellet kunne akseptere. Samtidig kunne vi identifisere hvilke deler av systemet som var potensielt mer utsatt for angrep enn andre. Den kvantitative beskrivelsen av systemområder kunne også beskrive systemområder som ikke fungerte optimalt, for eksempel nedetid på servere. Det kan være vanskelig å kvantifisere hvilken kostnad som kreves for at en angriper skal lykkes i et angrep. En virksomhet bør ha et grovt anslag på hvor mange angrep som lykkes, og hvor mange som mislykkes. Dette kan virksomheten benytte i form av statistikk og rater på bladnodene. Samtidig så skal det påpekes at angrep ikke bestandig blir oppdaget og forblir «mørketall». Dette er noe som gjør det vanskelig med å vurdere hvor riktige ratene er. Vi opplevde det som vanskelig å kvantifisere og beskrive ulike antall angrep ble vellykket gjennomført, som for eksempel ved «Social Engineering». Slike typer angrep, inneholder ofte et tall som forblir mørkt. Samtidig vil vi poengtere at dette ofte er et resultat av den praksis som bedriften og virksomheten legger til grunn ved sikkerhet. Det kan ofte ligge et potensial i kun å forbedre holdningene til de ansatte, og jevnlig gjøre dem bevisst på hva sikkerhet betyr for virksomheten. Dette er noe som ikke enkelt lar seg beskrive i feiltreet.

7.5.1 Argumentasjon for å benytte FTA innen informasjonsikkerhet

For å gjøre korrekte vurderinger av risiko er det ofte nødvendig med et godt og riktig datasett. Ofte er vurderingene av sannsynlighet og konsekvens grunnlaget for å bestemme og avgjøre en risiko. Å basere vurderinger på subjektiv eller personlig empiri, kan ofte medføre at risikovurderinger kan bli misvisende og ugyldige. Erfaringer som referansegruppa i sitter med, kan ofte bli liggende i sluttresultatet av analysen. Metoden FTA legger tilrette for å kunne basere vurderinger med utgangspunkt i statistiske data eller å kunne måle reelle data identifisert ved systemet. Eksempelvis, antall virusangrep, eller antallet tap av strøm på en server. En slik type tilnærming kan gi et bedre grunnlag for å gjøre korrekte vurderinger av konsekvens og sannsynlighet, og dermed en mer gyldig vurdering av risiko.

Bakås [83] har i sitt arbeid studert hvordan måling av informasjonssikkerhet utføres i virksomeheter. Undersøkelsen viser at så mange som 85 % av virksomhetene bruker kvantitative metoder i sine målinger, og at over halvparten kombinerer kvantitative og kvalitative målinger. Resultatene viser at de viktigste formålene med å måle er å kommunisere status på informasjonssikkerhet til ledelsen og å vise til samsvar med informasjonssikkerhets standarder, samt å gi ledelsen grunnlag for beslutninger. National Institute of Standards and Technology (NIST) [84] har utarbeidet retningslinjer som kan bistå ledelsen i å gjøre beslutninger om hvor iverksettelse av tiltak er mest hensiktsmessig,

forekempel ved bruk av sikkerhetsmetrikker og annen kvantifiserbar informasjon. Internasjonale standarder for informasjonssikkerhet, som ISO/IEC 17799 [25] og «Standard of Good Practice» [85], er utarbeidet fra praktiske erfaringer og har således gitt indikatorer på hvilke sikkerhetstiltak som er mest effektive.
For å kunne benytte slike retningslinjer og standarder er det ofte nødvendig med gyldige og korrekte kvantitative beskrivelser. Informasjonssikkerhet kan måles ved bruk av indikatorer for informasjonssikkerhet [82], og således kan det beskrives hvorvidt en virksomhet innehar tilstrekkelig informasjonssikkerhet. Vi har benyttet FTA i en tilnærming som tilrettelegger for å kvantisere informasjonssikkerhet basert på større grad av objektivitet. Dette ved å benytte en tilnærming som baserer seg på en større grad av statistiske data, og ikke subjektive vurderinger. Ved å identifisere indikatorer for informasjonssikkerhet kan en slik type tilnærming tilrettelegge for å kunne gjøre mer gyldige vurderinger av risiko, og således gi et mer gyldig resultat for å vurdere hvor det bør iverksettes tiltak.

7.6 Drøfting av verdier ved tyngre og lett metode og et helhetlig rammeverk

Erfaringen vår er at en enklere og mindre omfattende metode som NSM-ROS2004, gir raskt resultater basert på få ressurser. Slike typer metode er enkle å benytte og enkle å forstå[3]. Ofte kan det være nødvendig å gjennomføre korte og raske ROS-analyser. For eksempel i nødstilfelle eller ved rask endring av systemer som krever iverksettelse av strakstiltak. Begrensninger i ressurser som tid og tilgjengelig personell er kanskje de faktorene som legger størst press på å velge en enkel og mindre ressurskrevende metode. I slike tilfeller vil en enkel og rask metode være mer hensiktsmessig og verdifull for virksomheten. En tyngre og mer omfattende metode har ofte en tilnærming som går bredere og dypere tilverks, for eksempel CORAS [67]. Således kan trolig en slik type analyse gi økt pålitelighetsmessig verdi i resultatet. Men samtidig krever en slik type tilnærming flere ressurser i form av personell, tid, kompetanse og økonomi.
De fleste virksomheter står overfor en konstant usikkerhet og en stadig forandring i trussel- og risikobilde. Utfordringen for ledelsen kan være å avgjøre hvor mye usikkerhet og risiko virksomheten kan akseptere. En etablering av et helhetlig rammeverk for risiko- og sårbarhetsstyring med en gjennomarbeidet ROS-metode kan ofte være utfordrende både økonomisk og resurssmessig. Men det vil sannsynligvis ofte være hensiktsmessig og verdifullt for ledelsen i å evaluere og kontinuerlig forbedre risikostyringen i virksomheten. En helhetlig risikostyring med både intern kontroll og mulighet for å avdekke uakseptabel risiko i form av måling av informasjonssikkerhet, kan muligens bidra til at virksomheten kan være bedre rustet til å imøtekomme uforutsette og katastrofelignende situasjoner. Videre kan også et helhetlig rammeverk og risikostyring bidra til effektiv rapportering og etterlevelse av både lover og regler.
For en større bedrift eller virksomhet som konstant lever under et stort trussel- og risikobilde, kan det trolig være mer hensiktsmessig å etablere et helhetlig og effektivt rammeverk for risikostyring. For en mindre bedrift eller virksomhet med relativt stramme økonomiske budsjetter, kan det derimot være mer hensiktsmessig med en godt innarbeidet og effektiv ROS-metode som er tilpasset virksomhetens begrensede ressurser. For å

[3]Kategorisering av hvorvidt en metode er tung eller lett, er ofte basert på hvor ambisiøs og omfattende metoden er. Det eksisterer svært lite artikler som dokumentere og beskriver denne forskjellen. Men termene «tung» og «lett» metode blir ofte allikevel benyttet. E-post, Håvard Fridheim 18.01.2006

oppnå kvalitet i resultatet, er det ofte nødvendig at de som sitter med kompetanse og har inngående kjennskap til systemet deltar i ROS-analysen. Det kan derfor være nødvendig frigjøre ressurspersoner fra de vanlige arbeidsoppgavene for å kunne utføre en bedre ROS-analyse. Dette vil trolig også kunne gi analyseresultatet bedre pålitelighetsmessig verdi for ledelsen og virksomheten.

7.6.1 Sikkerhet og sikkerhetspersonell

Det beskrives det at «bevisstheten og kunnskapen om IKT-sårbarhet og sikkerhet er generelt for lav i mange organisasjoner og virksomheter» [73]. Det kan kanskje være lite hjelp i gode riskiko- og sårbarhetsmetoder om det ikke finnes tilstrekkelig kompetanse og personell til å benytte metodene. Personer som arbeider med sikkerhet og informasjonssikkerhet er beskrevet som «enslige svaler» innen virksomhetene. Det påpekes hvor viktig det er å etablere et nettverk til andre som arbeider innen samme område, både for å beholde motivasjonen og for å få faglige oppdateringer. Dette vil trolig kunne bidra til at personene kan gjøre et bedre arbeid. Samtidig kan det bidra til å besvare gapet i forhold til komplekse IKT-systemene, og til utfordringene som det nye trusselbildet gir. Kompleksiteten som ligger i systemer og infrastruktur, er etter hvert blitt så stor at ingen kan ha full oversikt [73]. Det er beskrevet at «Utdanningstilbudet innen IKT-sikkerhet bør styrkes, og det bør bygges opp mer spissede utdanningstilbud ved enkelte av institusjonene» [73]. Når det gjelder forskning innen samme område beskrives det at «mye av det som foregår er lite tilgjengelig fordi det foregår i lukkede kommersielle miljøer». Videre ble det i samme rapport påpekt det at det norske fagmiljøet på området er relativt svakt, selv om det er under oppbygning. Det kan derfor fortsatt være et behov for å besvare et fremtidig spørsmål om tilstrekkelig fokus på risiko- og sårbarhet i forhold til IKT og kompetanse, og nok sikkerhetpersonell/ledere.

8 Oppsummering og konklusjon

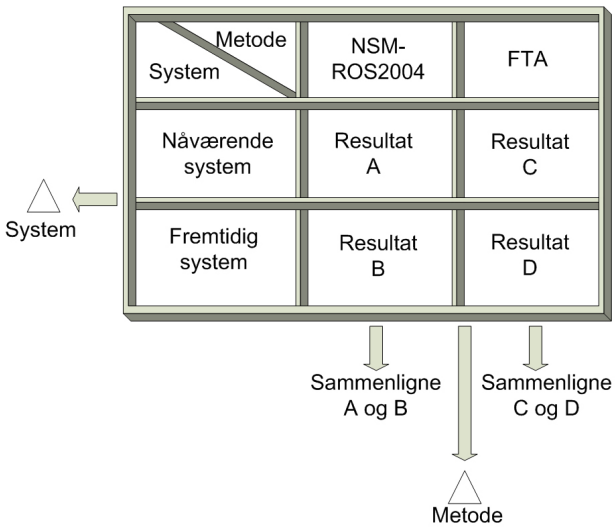
I dette kapitlet drøftes erfaringer fra arbeidet og hvor vidt vi har oppnådd vårt formål og målsetting. Avslutningsvis gis det en kort oppsummering og trekkes noen konklusjoner av arbeidet.

8.1 Kunnskapsbidrag

For å bedømme om oppgavens kunnskapsbidrag er oppnådd bør kunnskapsbidraget stilles i relasjon til målgruppen for oppgaven. Målgruppen for denne oppgaven er først og fremst innenfor fagfeltet risiko- og sårbarhetsanalyse. Vi vil også anse arbeidet som verdifullt for helsesektoren og studert helseforetak i deres overgang fra et relativt tungvindt system til et mer effektivt og enklere system. Problemstillingen er i seg selv gjeldende for enhver virksomhet og organisasjon som står overfor endring av både infrastruktur eller organisasjonsstruktur. Endringer i et turbulent samfunn setter stadige spørsmål både ved konsekvenser og gevinster ved samlokalisering og samordning av IKT-systemer.

Vår oppfatning er at oppgavens totale kunnskapsbidrag kan nyttegjøres av samtlige virksomheter og organisasjoner som står overfor samme utfordring, uavhengig av målgruppe. Dette fordi oppgaven omfatter ulike risikoaspekter og former for risikostyring som en generell ledelsesutfordring. Samtidig inneholder oppgaven en beskrivelse av konkrete problemområder ved endring av både organisasjonsstruktur og infrastruktur. Eksempelvis at en endring i IKT-infrastruktur vil prege en rekke forskjellige aspekter for en virksomhet, som for eksempel drift og support, organisasjonsoppbygning, overføring av beslutningsmyndighet osv.

Som forskningsbidrag begrenser oppgaven seg til å beskrive bruk av metoder og evaluere metodene, og et forsøk ved å benytte FTA som en metode innenfor fagområdet



Figur 30: Skisse av kunnskapsbidrag.

informasjonssikkerhet. Oppgaven inneholder også en begrunnelse for valg av metodene. Forskningsbidraget ansees som verdifullt for personer med mindre eller liten erfaring ved ROS-analyse. Det eksisterer relativt lite tilgjengelig materiale som beskriver detaljert fremgangsmåte og bruk av metoder. Ofte holdes hele ROS-analysen og prosessen konfidensielt innenfor en bedrift, organisasjon eller konsulentfirma.

8.2 Oppsummerende diskusjon av resultat og oppnådd mål

Oppgavens hovedintensjon er å gjøre en sammenligning av to relativt forskjellige metoder for å se hvilke resultater de gir. Dette utførte vi ved å gjennomføre et case studie av helseforetak med to metoder for risiko- og sårbarhetsanalyse. Samtidig ønsket vi at resultatet i ROS-analysene skulle beskrive konsekvenser ved samlokalisering av IKT-systemer. Vi mener vi har oppnådd det som var vår intensjon med oppgaven.

Oppgaven bygger i stor grad på evaluering og bruk av metoder, tekniske rapporter, forskningsarbeider, artikler og bøker, men også egenskaper og løsninger ved studert helseforetak. Resultatet i studiet av helseforetaket ga svar på konsekvenser ved samlokalisering av IKT-systemer ved det aktuelle helseforetaket. Resultatet vil vi beskrive som ikke å være av en fullstendig generell karakter for helsesektoren, fordi resultatet lar seg prege av løsninger og begrensninger ved det studerte helseforetaket. Vi valgte derfor å sammenligne resultatet med teori funnet i litteratur og artikler. Sammenligningen bidro i stor grad til å bekrefte funnene i ROS-analysene, samtidig ga dette også en dypere innsikt i hvilke deler av resultatet som vil prege en overgang.

8.3 Besvaring av forskningsspørsmål

I dette del kapitlet vil vi besvare forskningsspørsmålene i oppgaven. Først presenteres konklusjoner ved metodene, deretter presenteres konklusjoner ved samlokalisering av IKT-systemer. Hovedkonklusjonene ved samlolkalisering av IKT-systemer presenteres i del kapitlet 8.3.2. I tillegg er det vedlagt en detaljert beskrivelse i «vedlegg G, Rapport til SHDir».

Forskningsspørsmål ved metode

- Hvordan fungerte metodene med våre ressurser, problemstilling, kriterier og tidsbegrensning?
- I hvilken grad er resultatet preget av objektivitet og subjektivitet, personlige erfaringer og vurderinger?
- Er det verdt bryet å benytte en tyngre og mer omfattende metode, fremfor en lettere og mindre omfattende?

8.3.1 Konklusjoner ved metodene

Metoden NSM-ROS2004 er en metode som er lett å forstå og enkel å bruke i form av en stegvis fremgangsmåte. Metoden er tilrettelegger for at analytikerne kan prioritere områder og systemer som er av stor betydning, samtidig som metoden legger tilrette for å velge bort områder som er av lav betydning. Således kan metoden raskt gi resultater ved bruk av få ressurser og kort tid. NSM-ROS2004 mangler mulighet for å kunne se hvilken effekt iverksettelse av tiltak har. Ofte kan det være hensiktsmessig og nødvendig

for analytikere å se effekten av tiltak. En løsning synes å være å benytte metoden som en del av et rammeverk for ROS-analyse i en virksomhet. Ved å identifisere og å måle ulike parametere over tid, kan analytikerne se effekten av implementerte tiltak. De aller fleste tiltak har en kostnad, både ved implementering og drift. Metoden drøfter og beskriver kort en kost/nytte-vurdering ved implementering av tiltak. Metoden vil, etter vår mening være mest egnet i bruk ved raske og mindre ROS-analyser.
Vår tilnærming til FTA som metode, ga mulighet til å se risiko og sårbarheter fra forskjellige synspunkter, både i en kvalitativ og kvantitativ form. Metoden kan benyttes raskt og effektivt ved en kvalitativ tilnærming. Samtidig kan den kvalitative tilnærmingen skissere og visualisere risiko og sårbarhet, og sammenhengen mellom feilkildene. Ved å se sammenhengen mellom feilkildene, kan analytikere identifisere og implementere tiltak som dekker en mer helhetlig tilnærming til identifisert risiko og sårbarhet.
Ved å benytte metoden i en kvantitativ form, kreves det et mer omfattende arbeid, større ressurser og mer tid. Den kvantitative tilnærmingen vil sannsynligvis være mest verdifull for en virksomhet som allerede har etablert et godt rammeverk for risiko og sårbarhetsarbeid, og som jevnlig utfører analyser. Verdien vil ligge i å kunne måle hvilken betydning endringene vil ha for systemet. Samtidig kan analytikerne i etterkant se hvorvidt tiltakene har noen effekt.
Ved bruk av metoden i en kvantitativ tilnærming vil det være helt nødvendig om virksomheten har et reelt system å kunne utføre analysen på. Samtidig er det en fordel om det kan identifiseres gode statistiske data ved systemet. Det er også en stor fordel om det er høy grad av automatisering i systemet, og mindre grad av menneskelig involvering.
Ved en slik type tilnærming vil det være nødvendig å kunne gjøre vurdering av hvilken kostnad tiltakene har. Vurdering av kostnader ved iverksettelse av tiltak blir ikke tatt med, i vurdering av hvilke tiltak som er mest lønnsomme når kostnadsrammene er satt. Dette er noe som må vurderes utenfor metoden.

8.3.2 Subjektivitet og objektivitet i metodene

Hvorvidt metodenes resultat er preget av subjektivitet eller objektivitet, vil sannsynligvis være basert på hvilken type tilnærming som benyttes. Metoden NSM-ROS2004 legger tilrette for at det kan bli større grad av subjektive vurderinger i resultatet. Vurderinger av konsekvensnivå og sannsynlighetsnivå er basert på høy grad av personlig empiri i referansegruppa. Kombinasjonen av konsekvens- og sannsynlighetsnivå presenteres ofte i en risikomatrise, og sluttresultatet vil ofte være basert på kvaliteten i referansegruppa og de erfaringer prosjektdeltakerne sitter med. NSM-ROS2004 er også en metode som tilrettelegger for at analytikerne selv kan prioritere, og velge systemområder som er av større betydning. Således kan dette medføre at referansegruppa kan velge bort områder som er av kritisk betydning. Det kan være hensiktsmessig at sammensetningen av referansegruppa bør være forskjellige fra ROS-analyse til ROS-analyse, slik at referansegruppa ikke utfører samme vurderinger i hver ROS-analyse.
FTA er en metode som tilrettelegger for å kunne utføre vurderinger basert på statistiske data. Således kan analyseresultatet være preget av mindre subjektivitet og større grad av objektivitet. Ved å identifisere gode parametere og indikatorer som kan brukes til måling av sikkerhet og informasjonssikkerhet, kan resultatet i metoden gjøres ytterligere objektivt. Den kanskje største fordelen med objektivitet i målinger er at resultatet kan uttrykkes i et mer ledelsesspesifikt språk med mulighet for kost/nytte vurderinger. Ulem-

pen ved en slik tilnærming er at det sjelden eksisterer tilgang til stort statistiske datasett, og at metoden kan kreve relativt komplekse beregninger. Samtidig kan det være vanskelig å vurdere hvor korrekt den kvantitative beskrivelsen av feilkilden er.
Alternativt finnes det også noen metoder som blander subjektiv informasjon med objektiv informasjon. Dette gjøres ved at subjektiv informasjon uttrykkes i en sannsynlighetsfordeling, selv om det ikke finnes noen kjent datamengde. Dette kan beskrives som Bayesisk eller subjektivistisk statistikk. Slike typer metode benyttes blant annet for å analysere usikkerhet ved prosjekter eller foreksempel nedetid [37]. Ved å velge en tilnærming som er basert på større grad av objektive datakilder, kan sannsynligvis resultatet være mer pålitelig, enn ved en ren subjektiv tilnærming.

8.3.3 Lettere eller tyngre metode, eller helhetlig rammeverk

Styret og ledelsen setter stadig større krav til at virksomheten skal kunne ha tilstrekkelig informasjonssikkerhet. Risiko og sårbarhetsstyring blir i økende grad tatt i bruk som en del av virksomhetens strategiske og operative styring [46]. Samtidig blir virksomhetene bedre til å identifisere og styre sine risikoer, både operasjonelt og finansielt. Ledelsen vil bestandig kreve å ha tilstrekkelig og korrekt informasjon, slik at de sammen med øvrig ledelsesinformasjon kan forutsi og reagere overfor raske endringer og kriselignende situasjoner. På en slik måte kan en tilnærming til proaktiv risiko- og sårbarhetsstyring bidra til at virksomheten kan prioritere ulike trusler og risikoområder, og samtidig identifisere risiko som kan hindre virksomheten i å nå sine mål. En etablering av et helhetlig rammeverk og en strategi for risiko- og sårbarhetsstyring som en integrert del av virksomhetens styringsprosess vil være essensiell for å kunne håndtere krise- og katastrofesituasjoner som kan true virksomhetens forretningsprosesser.
Hvorvidt en metode er mer hensiktsmessig fremfor en annen, vil ofte være svært situasjonsbetinget. Begrensninger i ulike ressurser som foreksempel personell, økonomi, tid og kompetanse vil være påvirkende for valg av tilnærming. Er det nødvendig med raske analyser, og situasjoner som krever strakstiltak kan kanskje en tilnærming til NSM-ROS2004 være mer hensiktsmessig. Tilmotsetning vil det kanskje være mer hensiktsmessig med en tyngre og mer omfattende metode i de tilfellene hvor systemer utsettes for store endringer. Samtidig bør det sannsynligvis også vurderes hvor stort risikobilde virksomheten må operere under. De fleste virksomheter står overfor en konstant usikkerhet og en stadig forandring i trussel- og risikobilde. En etablering av et helhetlig rammeverk for risiko- og sårbarhetsstyring med en gjennomarbeidet ROS-metode kan være mer hensiktsmessig om virksomheten må operere under et omfattende trussel- og risikobilde. En helhetlig risikostyring med både intern kontroll og mulighet for å avdekke uakseptabel risiko i form av måling av informasjonssikkerhet, kan trolig bidra til at virksomheten kan være bedre rustet til å takle uforutsette og katastrofelignende situasjoner. Videre kan også et helhetlig rammeverk og risikostyring bidra til effektiv rapportering og etterlevelse av både lover og regler.
For en bedrift eller virksomhet med få ressurser og et stramt økonomisk budsjett, kan det derimot være mer hensiktsmessig med mindre og mer effektiv ROS-metode som er tilpasset virksomhetens ressurser. For å oppnå kvalitet i analyseresultatet kan det være nødvendig å frigjøre ressurspersoner fra de vanlige arbeidsoppgavene for å kunne utføre ROS-analysen. Dette vil trolig også kunne gi analyseresultatet bedre pålitelighetsmessig verdi for ledelsen.

Forskningsspørsmål under «Generelt»

- Hvilke gevinster eller konsekvenser ligger det i å samlokalisere IKT-systemer?
- Hvilke sikkerhetsfaktorer blir påvirket og fremkommer det nye sårbarheter ved en reorganisering av IKT-infrastruktur?

8.3.4 Konklusjoner ved samlokalisering av IKT-systemer

Forretningsmessige behov er som oftest det behovet som utfordrer den teknologiske utviklingen. Ved å imøtekomme nye krav for å forenkle arbeidsprosesser. Det settes stadig større krav til teknologiske systemer som underbygger og effektiviserer arbeidsprosessene. Risiko og sårbarhet legger begrensninger på ulike konsepter som kan bidra til å etablere en mer effektiv virksomhet og organisasjon. Samtidig vil aspekter som sikkerhet og informasjonssikkerhet bli påvirket når informasjonssystemer utsettes for store endringer i omgivelsene. Krav til økt effektivitet i helsesektoren har medført til at større mengder tjenester og informasjon bør samlokaliseres for å underbygge effektivitetskravene i arbeidsprosessene. Som et resultat medfører dette større informasjonstilgjengelighet, nye kommunikasjonsformer og kommunikasjonskanaler, og ikke minst større angrepsflate for en angriper.

Fellestrekkene innen helsesektoren er at organisasjonene er desentralisert med mindre lokasjoner, samtidig er det tilrettelagt for sentraliserte IKT-løsninger. Tjenestespektret er bredt og varierende med både basistjenester som e-post, internett-tilgang osv, og anvendelser av felles systemer og tjenester. Virksomhetene er kontinuerlige avhengig av IKT-systemet for å fungere effektivt. Således er virksomhetene også avhengig av å ha en velfungerende og effektiv IKT-avdeling. Sentrale løsninger blir ofte etablert for å redusere kostnader og skape stordriftsfordeler. Forventningene til gevinstene kan beskrives ved økte tilgjengelige ressurser, økonomisk innsparing, mer innflytelse overfor leverandører og sentralisering av (spiss)kompetanse for å forsterke tiltak.

Organisasjonsmessig gir en regional IKT-enhet mulighet for å kunne splitte ansvarsområder og for bedre å kunne koordinere fysiske, logiske og organisatoriske sikkerhetstiltak. Splitting av ansvarsområder gjør det enklere å stille krav til avdelinger og til de ansvarlige. Videre vil en sentralisering av drift og support gi mindre ressursbruk, som kan gi større mulighet for gjenbruk av personell og fokus på viktige satsningsområder. Samtidig vil en endring til færre tekniske installasjoner og færre knutepunkter, gi et mindre komplekst system. Dette kan gi enklere konfigurasjon og feilsøking, bedre sikring og mulighet for å benytte de nye ressursene på overvåking.

Fordelene og gevinstene ved å samlokalisere systemer er mange og varierende fra organisasjon til organisasjon. Ofte kan konsekvensene vurderes opp mot gevinstene. Sannsynligvis vil det være hensiktsmessig å vurdere om gevinstene er større enn konsekvensene. Ved konsolidering og samlokalisering, vil grensene mellom ulike systemer og maskinvare som tidligere fungerte som barrierer mot angrep, fjernes og det dannes nye sårbarheter og ny risiko. Konsolidering av store og flere datasystemer representerer utfordringer for å bevare krav om tilstrekkelig sikkerhet. Et mindre antall knutepunkter i infrastruktur vil resultere i større sårbarhet ved knutepunktene. Samtidig vil store deler av virksomhetens informasjon ofte samles i ett og samme system, selv om det kan være nødvendig ut i fra et foretningsmessig perspektiv, får det konsekvenser for sårbarheten. Videre vil integrasjonen av systemer med inkompatible sikkerhetsmekanismer medføre lite samsvar

mellom komponenter og dårlige sikkerhetsløsninger. Ofte vil resultatet være en ytterligere sårbarhet.
Å samle informasjonen i en organisasjon i ett og samme system gir oftest systemene økt verdi for organisasjonen, men gjør samtidig systemet også mer attraktivt for angripere. Samtidig vil en større del av bedriften få økt avhengighet til ett og samme system. Økningen i avhengighet til systemet er også beskrevet av Nærings- og handelsdepartementet som en kritisk sårbarhet [73]. Større antall brukere resulterer i større mengde passord og brukernavn, og større antall forskjellige restriksjoner for brukere, leverandører og forvaltere. På denne måten vil en konsolidering medføre mindre kompleksitet enkelte steder, men også økt kompleksitet på andre områder.
En sentral faktor som gjerne blir glemt i risikovurdering ved et system, er innvolvering av den menneskelige faktor [86]. Mennesket vil alltid utgjøre en betydelig del av et system, enten som bruker eller som forvalter. Menneskets bevisste eller ubevisste handlinger utgjør en konstant risiko og sårbarhet som bør taes med i betraktning ved et system. Det kan ligge utfordring i både nysgjerrighet, lojalitet til virksomheten eller ren ondsinnethet. Dette er vesentlige faktorer som kan bli satt på prøve i ulike situasjoner, ofte med svært forskjellige konsekvenser. Uansett vil resultatet påvirke det totale sikkerhetsbildet til systemet.
En samlokalisering av IKT-systemer på regionalt nivå tilrettelegger for en mer effektiv helsesektor, samtidig medfører en endring en større sårbarhet. En reduksjon av sårbarhet og risiko skjer ikke av seg selv ved etablering av regional IKT-enhet eller en sentralisert IKT-løsning, men gir mulighet for større tilgjengelige ressurser, økt koordinering av tiltak, muligheten for splitte ansvarsområder og økt kompetanse i virksomheten. Økonomi er en drivkraft som ofte legger press på å gjennomføre en samlokalisering, men fordelene kan forsvinne i krav til redusert sårbarhet og evne til å håndtere større hendelser. Samtidig vil en reduksjon eller forflytting av overlappende kompetanse i seg selv utgjøre en sårbarhet.

9 Videre arbeid

I dette kapitlet diskuteres det videre arbeidet i oppgaven.

9.1 Evaluering av metodene

Denne rapporten har forsøkt å besvare spørsmålet hvilke resultater to metoder gir og hvilken objektivitet eller subjektivitet ligger i resultatene. En mer spesifikk videreføring av dette arbeidet vil være å evaluere i hvilken grad dette resultatet er i samsvar og reelt i lignende situasjoner, sektorer og virksomheter. En evaluering av metodene krever flere og mange runder med ROS-analyse, samt detaljert analyse hvorvidt resultatet som foreligger er preget av objektivitet eller subjektivitet. Dette er et omfattende og tidkrevende arbeid, og kan ikke omfattes i denne oppgaven. Derfor vil de erfaringer og resultater som er beskrevet i denne oppgaven, inngå som en større del av BAS5 og FFI sin evaluering av metoder og bruksområde. Det ville allikevel være interessant å avdekke om metodene resulterer i samme konklusjoner innen andre virksomheter i helsesektoren og andre sektorer. Hvordan gjøres vurderinger av risiko og sårbarhet med fokus på andre verdier? Er det forskjell på helseforetak i privat og offentlig sektor? Og er vurderingene av risiko og sårbarhet som ligger i resultatet basert på synspunkter til ledelsen, de ansatte, eller virksomhetens? Dette vil kunne være en kvalitetssikring og kunne delvis verifisere resultatet i denne oppgaven, samtidig også gi mulighet for å vurdere metodene med tanke på brukbarhet osv.

9.1.1 FTA og informasjonssikkerhet

Vår tilnærming til FTA, genererte flere spørsmål og forslag til videre arbeid og utvikling av metoden til bruk innen informasjonssikkerhet. En evaluering og ny gjennomgang ved konstruksjon av feiltrærne vil kanskje kunne bidra til å finne bedre og andre alternative løsninger for konstruksjon av feiltrærne. Det ville også vært interessant å se på hvilke resultater vår tilnærming ville gitt i et system som har høyere grad av automatisering, og et godt statistisk datasett tilgjengelig. Et videre arbeid vil også kunne være å konstruere feiltrær av forskjellige systemer, og vurdere hvilken betydning den strategiske plasseringen av komponentene har for systemet. Kan en implementert FTA-løsning med bruk av Birnbaums mål resultere i identifikasjon av svake komponenter/systemområder? Og hvilke resultater gir dette over en lengre periode? Et alternativ kan være en analyse og evaluering av hvordan den strategiske plasseringen av komponenter/ systemområder kan bidra til å senke feilratene og heve pålideligheten til et system. Videre ville det vært interessant med en evaluering av hvordan en kan konstruere feiltrær av systemer som har stor grad av menneskelig involvering. Å konstruere feiltrærne etter vår tilnærming er neppe det eneste og beste alternativet. Det finnes sannsynligvis andre og bedre løsninger som kan gi et mer pålitelig resultat.
En mer spesifikk videreføring av arbeidet vil være å teste ut i hvilken grad metoden FTA kan bidra til måling av informasjonssikkerhet og faktisk verifisere en virksomhets informasjonssikkerhet. Det ville være interessant å se på hvilke resultater en videreutviklet FTA-metode gir i bruk i en virksomhet over lengre tid. Kan metoden bidra til å identifise-

re og avdekke risikoområder, eller dårlige rutiner og praksis ved informasjonssikkerhet i en virksomhet? Samtidig vil det være interessant å avdekke hvorvidt metoden kan bidra til å avdekke hvor det er mest hensiktsmessig med implementering av tiltak, og hvordan iverksettelse av tiltak faktisk bidrar til å bedre sikkerheten/påliteligheten ved et system. En slik type måling kan kanskje gi analytikerne kvantitative beskrivelser på hvorvidt sikkerhetsarbeidet gir positive resultater.

9.1.2 Kost/nytte vurderinger

Et annet alternativ til videre arbeid ville være å avdekke om det er en mulig å benytte FTA i en tilnærming hvor evaluering av tiltak er basert på en kost-nytte vurdering. En kostnad er en essensiell del i en vurdering av alternative tiltak. De fleste sikringstiltak har en kostnad, og investeringskostnadene ved et tiltak må veies mot det potensielle tapet som et sikkerhetsbrudd kan medføre. Å kunne utføre rangering av tiltak på bakgrunn av kost-nytte vurderinger, er hensiktsmessig i å kunne presentere et fullstendig og godt resultat for ledelsen. Vi skisserer følgende noen tanker om hvordan det videre arbeid angående kost-nytte-vurderinger.

Gitt at vi kjenner strukturfunksjonen $h(x_1, x_2, \ldots, x_n)$ til et system og Birnbaums mål til hver enkelt komponent

$$\left(\frac{\partial h}{\partial x_1}, \frac{\partial h}{\partial x_2}, \ldots \frac{\partial h}{\partial x_n}\right).$$

Vi gjenkjenner gradient vektorfeltet til funksjonen h evaluert i punktet $(x_1, x_2, \ldots, x_n)$, som betegnes ved

$$\nabla h(x_1, x_2, \ldots, x_n).$$

Denne vektoren peker i den retningen hvor den deriverte av $h(x_1, x_2, \ldots, x_n)$ er maksimal. Den maksimale økningen av påliteligheten i systemet oppnås dermed ved å endre tilstanden i systemet i retningen $\nabla h(x_1, x_2, \ldots, x_n)$.
I et virkelig system er det selvfølgelig urealistisk å endre på alle komponentene i systemet. En tilnærming til dette problemet er presentert i avsnitt 6.9.6. Iterativ forbedring av den komponenten som til enhver tid har høyest Birnbaums mål, inntil tilfredsstillende systempålitelighet oppnås eller at budsjettet er oppbrukt. Det ville være av stor interesse å finne en algoritme som kan velge ut hvilke komponenter som skal endres og hvor mye disse skal endres, basert på Birnbaums mål og kostnaden knyttet til å endre hver enkelt komponent og å få testet denne ut på et virkelig system.

9.2 Konsekvenser ved samlokalisering av IKT-systemer

Denne rapporten bidrar i arbeidet med å etablere et fundament for videre arbeid med å samlokalisere IKT-systemer innen helsesektoren. Arbeidet må også sees i en større sammenheng, både ved evaluering av metoder og kunnskapsbidraget som oppgaven resulterer i. En videre forskning med utgangspunkt i resultatet, kan både være av fordypende og av utvidet karakter. En fordypende forskning kan innebære at kunnskapsbidraget gis en økt kvalitet i form av ytterligere teoretisk og empirisk underlag. Dette kan også være en kvalitetssikring av de resultatene denne oppgaven resulterer i, enten at de forandres og/eller styrkes, eller utprøves. Selv om arbeidet har gitt mange indikatorer på konsekvenser ved sentralisering i resultatet, er det mye arbeid som gjenstår og som må fullføres før resultatet kan beskrives som reelt. En forskning av utvidet karakter kunne innebære

at kunnskapsbidraget anvendes i en annen kontekst eller en annen sammenheng. Det ville vært interessant i det videre arbeid å kunne avdekke om resultatene er gjeldene for andre sektorer som for eksempel bank og finans.

Bibliografi

[1] Kumamoto, H. & Henley, E. J. 1996. *Probabilistic Risk Assessment and Management for engineers and scientists*. Number 0-7803-6017-6. IEEE Press.

[2] Schuff, D. & Louis, R. S. 2001. Centralization vs. decentralization of application software. *Commun. ACM*, 44(6), 88–94.

[3] Nasjonal sikkerhetsmyndighet, N. 2005. Veiledning i risiko- og sårbarhetsanalyse, NSM-ROS2004. http://www.nsm.stat.no/dokumenter/Veiledninger%20S2-2/ROS_2004_veiledning.pdf.

[4] Moberg, F. Security analysis of an information system using an attack tree-based methodology. Master's thesis, Chalmers University of Technology, 1999.

[5] Glück, E. & Berglihn, O. T. Web-løsninger som et alternativ, informasjonsutveksling i helsesektoren. Technical Report 22, Kompetansesenter for IT i helse- og sosialsektoren AS (KITH), http://www.kith.no/upload/1089/R05-03Info-utveksling-i-helsesektoren-v2.pdf, 2003.

[6] Gulbrandsen, R. 3 2005. Krise- og beredskapsplanlegging, beskyttelse mot avbrudd i kritiske forretningsprosesser. http://www.isaca.no/DataZ/DataZ%20nr.%201-2003.pdf. DataZ.

[7] Audestad, J. A. 2003. *E-bombs and E-granades*. Forelesnings kompendie ved Høgskolen i Gjøvik.

[8] Aksnes, B. & Vestad, A. Driftssikkerhet ved bruk av elektronisk pasientjournal. Technical report, Kompetansesenter for IT i helse- og sosialsektoren AS (KITH), http://www.kith.no/upload/1045/R07-02EPJ-Driftssikkerhet.pdf, 2002.

[9] Leedy, P. D. & Ormord, J. E. 2004. *Practical Research, planning and design. 8th Edition.* Pearson Merrill Prentice Hall.

[10] Aksnes, B., Vestad, A., & Grøtan, T. O. Risikoanalyse, metodegrunnlag og bakgrunnsinformasjon. Technical report, Kompetansesenter for IT i helse- og sosialsektoren AS (KITH), 2000.

[11] Keong, T. H. Risk analysis methodologies. http://home1.pacific.net.sg/ thk/risk.html http://home1.pacific.net.sg/ thk/biblio.html.

[12] Bergum, S. 06 2004. Informasjons- og kommunikasjonsteknologi (ikt) og innovasjoner i organisasjonsstrukturer, prosesser og nye organisasjonsformer. Østlandsforskning.

[13] Limoncelli, T. A. & Hogan, C. 2002. *The practice of system and network administration*. Boston, Addison-Wesley.

[14] Leavitt, H. J. 1965. Applied organizational change in industry : structural, technological, and humanistic approaches. Classic Readings in Organizational Behavior by J. Steven Ott. ISBN: 0-534-11073-8.

[15] HOD (Helse- og omsorgsdepartementet). Lov om helseregistre og behandling av helseopplysninger(helseregisterloven). http://www.lovdata.no/all/hl-20010518-024.html. (Lest Januar 2006) Lovdata.

[16] HOD (Helse- og omsorgsdepartementet). Lov om helseforetak m.m. (helseforetaksloven). http://www.lovdata.no/all/nl-20010615-093.html. (Lest Januar 2006) Lovdata.

[17] FAD (Fornyings- og administrasjonsdepartementet). Forskrift om behandling av personopplysninger (personopplysningsforskriften). http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20001215-1265.html. (Lest Januar 2006).

[18] HOD (Helse- og omsorgsdepartementet). Lov om pasientrettigheter (pasientrettighetsloven). http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20001221-1385.html. (Lest Januar 2006) Lovdata.

[19] HOD (Helse- og omsorgsdepartementet). Forskrift om pasientjournal. http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20001221-1385.html. (Lest Januar 2006) Lovdata.

[20] FAD (Fornyings- og administrasjonsdepartementet). Forskrift om elektronisk kommunikasjon med og i forvaltningen (eforvaltningsforskriften). http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20040625-0988.html. (Lest Januar 2006) Lovdata.

[21] JD (Justis- og politidepartementet). Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven). http://www.lovdata.no/all/hl-19670210-000.html. (Lest Januar 2006) Lovdata.

[22] Datatilsynet. Forskrift om pasientjournal. http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20001221-1385.html.

[23] Pfleeger, C. P. & Pfleeger, S. L. 2002. *Security in Computing*. Prentice Hall Professional Technical Reference.

[24] Bakås, T. H. God praksis for måling av informasjonssikkerhetsnivå. Master's thesis, Høgskolen I Gjøvik, 2005.

[25] 17799, N.-I. Information technology - Code of practice for information security management, ISO.

[26] Ween, M. Rammeverk for formulering av portable krav til informasjonssikkerhet. Master's thesis, HiG, 2004. (Lest Des. 2005).

[27] Sikkerhetsmyndighet, N. 2004. *Objekt- og informasjonssikkerhet: Metode for risiko- og sårbarhetsanalyse*, volume 2. Norges teknisk-naturvitenskapelige universitet.(NTNU)/Nasjonal Sikkerhetsmyndighet.

[28] Johan Gustav Bellika, Gunnar Hartvigsen, m.fl. Delrapport fra elviraprosjektet. nettbasert pasientinformasjonssystem, arkitektur og visualisering. Technical report, Nasjonalt Senter for Telemedisin NST, 2001.

[29] Idsø, E. S. & Øyvind Mejdell Jakobsen. 2000. *Objekt- og Informasjonssikkerhet, Metode for risiko og sårbarhetsanalyse.*, volume 1. Institutt for produksjonsteknikk og kvalitetsteknikk. Norges teknisk-naturvitenskapelige universitet.

[30] Avizienis, A., Laprie, J., & Randell, B. 2001. Fundamental Concepts of Dependability. http://www.cert.org/research/isw/isw2000/papers/56.pdf.

[31] Stølen, K. 2004. Sikkerhet, Tillit og Personvern: ser vi sammenhengen nå? http://www.sintef.no/static/td/arr/juni2004/presentasjoner/9.st%C3%B8len.pdf. SINTEF/UiO.

[32] Vestad, A. Krav til kommunikasjonssikkerhet for edi-løsninger. Technical report, KITH, http://www.kith.no/upload/1039/R04-02KravKommsikkEDI.pdf, 2002.

[33] Berglihn, O. T. & Alsaker, M. Delrapport paraplyprosjektet - informasjonssikkerhet ved pacs løsninger. Technical report, Kompetansesenter for IT i helse- og sosialsektoren AS (KITH), http://www.kith.no/upload/1093/R07-03Infosikkerhet-PACS.pdf, 2003. (Lest Nov. 2005).

[34] Gafurov, Helkala, & Svendsen, K. 2005. Security models for electronic medical record. *Telektronikk*, 5.

[35] Payne, S. C. September 2001. A guide to security metrics. SANS Security Essentials GSEC Practical Assignment Version 1.2e. http://www.sans.org/rr/whitepapers/auditing/55.php.

[36] Bass, T. & Robichaux, R. 2001. Defense-In-Depth Revisited: Qualitative Risk Analysis Methodology for Complex Network-Centric Operations. http://www.silkroad.com/papers/pdf/milcom2001-430.pdf.

[37] Aven, T. 2005. *Pålitelighets- og risikoanalyse*. Universitetsforlaget.

[38] Holm, O. Risk management of information systems in dynamic environments - A case study of the Norwegian Defence and the process of approving classified information systems. Master's thesis, Høgskolen i Gjøvik (HIG), 2004.

[39] Aven, T. A unified framework for risk and vulnerability analysis and management covering both safety and security. UiS, 2005.

[40] Kahneman, D. & Tversky, A. 1979. Prospect theory: An analysis of decision under risk. *Econometrica*, Vol. 47, pp. 263–292.

[41] Loomes, G. & Sugden, R. Supplemen 1987. Testing for regret and disappointment in choice under uncertainty. *Economic Journal*, 97(388a), 118–29. available at http://ideas.repec.org/a/ecj/econjl/v97y1987i388ap118-29.html.

[42] Neumann, J. V. & Morgenstern, O. 1944. *Theory of Games and Economic Behavior*. Princeton University Press.

[43] Jose J. Gonzalez. 2003. *From modeling to managing security, A system dynamics approach*. HøyskoleForlaget, Norwegian Academic Press.

[44] J.W. Cappelens Forlag AS. Cappelens lexicon. http://www.caplex.net/.

[45] P.J.Bugden. Why risk analysis. 4.

[46] Jenkins, B. D. 1998. Security risk analysis and management, risk analysis helps establish a good security posture; risk management keeps it that way. http://www.nr.no/ãbie/RA_by_Jenkins.pdf. Countermeasures, Inc.

[47] Sintef. Stiftelsen for industriell og teknisk forskning ved Norges tekniske høgskole (NTH) (Sintef). http://www.sintef.no/. (Last visited 25.02.2006).

[48] Johnsen, O.-A., Gulbrandsen, R., & m.fl, J. O. S. 2002. Metoder og verktøy for gjennomføring av risikoanalyser. American Society of Industrial Security (ASIS) Norway. http://www.asis.no/.

[49] Fridheim, H. 2005. Sårbarhet i kritisk infrastruktur - ikke minst ikt-systemer. http://www.ntnu.no/videre/konferanse/si2002/Tidligere%20konferanser/2005/Fridheim.pdf. Forsvarets Forskningsinstitutt (FFI).

[50] Hagen, J. M. & Nystuen, K. O. 1999. Beskyttelse av samfunnet med vekt på offentlig telekommunikasjon. Forsvarets Forskningskinstitutt (FFI).

[51] Rodal, S. K. 2001. Sårbarhet i kraftforsyningens drift og styringssystemer. *Forvarets Forskningsinstitutt,FFI RAPPORT, FFI/RAPPORT-2001/04278*, 28.

[52] Fridheim, H. 2002. Survivability of the modern society - Critical infrastrukture vulnerability. The Norwegian Defence Research Establishment (FFI). European Survivability Workshop, 26-28 February 2002, Köln-Wahn, Germany.

[53] Olsen, O. K. Adversary modelling. Master's thesis, Høgskolen i Gjøvik, NISlab, http://www.hig.no/imt/file.php?id=1055, 2004.

[54] Olsen, O. K. & Snekkenes, E. July 2004. A Framework for Adversary Models. Høgskolen i Gjøvik (HiG). Vedlegg i oppgaven.

[55] Fredriksen, R., Kristiansen, M., & mfl. 2000. The coras framework for a model-based risk management process. *Springer-Verlag GmbH*, Springer, 12.

[56] A.Moore, R.Ellison, & R.Linger. Mars 2001. Attack modeling for information security and survivability.

[57] Consulting, D. V. Persondata-utveksling i norge. Technical Report 0, Da Vinci Consulting, http://odin.dep.no/filarkiv/221100/Utveksling_av_persondata_–_da_Vinci_Consulting_AS.pdf, Mai 2004.

[58] Rapport fra forprosjekt, nasjonal strategi for elektronisk pasientjournal. http://www.shdir.no/vp/multimedia/archive/00004/Forprosjektrapport -h 4714a.doc. (Lest Januar 2006).

[59] Nasjonal IKT. April 2005. Overordnet IKT-strategi for de regionale helseforetakene, med forslag til felles satsningsområder og tiltak. http://www.helse-ost.no/showimage.asp?iEntityId=1743. (Lest Januar 2006).

[60] Vestad, A. & Alsaker, M. Sikker innføring av it-systemer. Technical report, Kompetansesenter for IT i helse- og sosialsektoren AS (KITH), http://kith.episerverhotell.net/upload/1283/RutineNyttIT-system.pdf, 2003. (Lest Nov. 2005).

[61] HOD (Helse- og omsorgsdepartementet). Lov om helsepersonell m.v. (helsepersonelloven). http://www.lovdata.no/all/hl-19990702-064.html. (Lest Januar 2006) Lovdata.

[62] JD (Justis- og politidepartementet). Lov om behandling av personopplysninger (personopplysningsloven). http://www.lovdata.no/all/hl-20000414-031.html. (Lest Januar 2006) Lovdata.

[63] Lima, B. Elektronisk pasientjournal og personvern i allmennlegetjenesten. Master's thesis, Avdeling for forvaltningsinformatikk (AFIN)/ Universitetet i Oslo (UiO), http://www.afin.uio.no/forskning/hovedfag/BeritLima_OK_DT.pdf, 2002. (Lest Nov. 2005).

[64] Sosial og Helse Direktoratet (SHDir). 2005. Norm for informasjonssikkerhet i helsesektoren. http://www.shdir.no/vp/multimedia/archive/00001/Norm_for_informasjons_1280a.doc. (Lest Januar 2006).

[65] Rausand, M. 1991. *Risikoanalyse: Veiledning til NS5814*. Tapir, SINTEF.

[66] Software, R. Fault Tree Analysis - FTA. http://www.fault-tree.com/.

[67] CORAS. The coras project. http://coras.sourceforge.net/.

[68] Fredriksen, R., Kristiansen, M., & mfl. Experiences from using model-based risk assessment to evaluate the security of a telemedicine application. http://heim.ifi.uio.no/ massl/publications/ticd02.pdf.

[69] N Stathiakis AND C.E. Chronaki AND m.fl. 2003. Risk assessment of a cardiology ehealth service in hygeianet. http://coras.sourceforge.net/.

[70] Booch, Jacobson, & Rumbaugh. 2006. *The Unified Modeling Language User Guide, Second Edition*. Number 0201571684. Addison Wesley Professional.

[71] ISACA. Control Objectives for Information and Related Technology (COBIT). http://www.isaca.org/cobit/.

[72] Kredittilsynet. Egenevalueringsskjema for foretakets IT-virksomhet(CobiT). http://www.kredittilsynet.no/wbch3.exe?ce=15428.

[73] Nærings- og handelsdepartementet. Oktober 2000. Samfunnets sårbarhet som følge av avhengighet til it. http://odin.dep.no/nhd/norsk/dok/andre_dok/rapporter/024101-220003/dok-bn.html.

[74] Helmer, G., Wong, J., Slagell, M., Honavar, V., Miller, L., & Lutz, R. 2001. A software fault tree approach to requirements analysis of an intrusion detection system. Iowa State University.

[75] Amoroso, E. 1994. *Fundamentals of Computer Security Technology*. Prentice Hall.

[76] Schneier, B. Desember 1999. Attack trees, modeling security threats. Dr. Dobb's Journal.

[77] Sutton, I. S. 1992. *Process Reliability and Risk Management*. Van Nostrand Reinhold.

[78] Andersen, E. S., Grude, K. V., & Haug, T. 1998. *Målrettet Prosjektstyring*. Number 8256260645. NKI PriceWaterHouseCoopers (PwC).

[79] Sikkerhetsmyndighet, N. 2003. Risikovurdering 2003: Sikre samfunnsviktige objekter og informasjon. http://www.nsm.stat.no/dokumenter/Risikovurdering/EndeligversjonUgradertRV03.pdf.

[80] Bundesamt für Sicherheit in der Informationstechnik. 2004. IT-Grundschutz Manual 2004: Threats Catalogue Force Majeure. http://www.bsi.bund.de/english/gshb/manual/download/threat-catalogue.pdf.

[81] Holen, A. T., Høyland, A., & Rausand, M. 1988. *Pålitelighetsanalyse*. Number 82-519-0568-0. Tapir.

[82] Alsaker, M. & Aksnes, B. 01.04 2004. Indikatorer for informasjons-sikkerhet. Kompetansesenter for IT i helse- og sosialsektoren, KITH. http://www.kith.no/upload/1177/R08-04IndikatorerInformasjonssikkerhet.pdf.

[83] Tone Hoddø Bakås. God praksis for måling av informasjonssikkerhetsnivå. Master's thesis, Høgskolen i Gjøvik, HiG, 2005.

[84] Swanson, M., Bartol, N., Sabato, J., Hash, J., & Graffo, L. Juli 2003. Security Metrics Guide for Information Technology Systems. National Institute of Standards and Technology, NIST Special Publication 800-55.

[85] The Standard of Good Practice for Information Security. Standard of good practice. http://www.isfsecuritystandard.com/index_ie.htm.

[86] Nasjonal Sikkerhetsmyndighet. 1 2006. Nasjonal sikkerhetsmyndighet, Temahefte 1/2006, Sårbarheter og trusler mot informasjonssystemer. http://www.nsm.stat.no/dokumenter/Risikovurdering/EndeligversjonRV06.pdf.

[87] Justisdepartementet. Ot.prp. nr. 92 (1998-99) Om lov om behandling av personopplysninger (personopplysningsloven). http://odin.dep.no/jd/norsk/dok/regpubl/otprp/012005-050050/. (Last visited 16.02.2006).

[88] KKD (Kultur- og kirkedepartementet). Lov om arkivering (arkiveringsloven). http://www.lovdata.no/all/hl-19921204-126.html. (Lest Januar 2006) Lovdata.

A Lovverk

Det eksisterer flere sentrale lover og forskrifter med fokus på sikkerhet og informasjonssikkerhet ved deling og overføring av persondata. Samtidig finnes det lover som gjelder for elektronisk behandling av persondata, eksempelvis Personopplysningsloven, Arkivloven og Forvaltningsloven, og de lovene som er rettet mer mot helse som virksomhets- og fagområdet, eksempelvis Helsepersonelloven, Pasientrettighetsloven og Helseregisterloven.

Lover som er aktuelle for helsesektoren er nevnes følgende, mens de lovene som omhandler oppgavens fokus beskrives nøyere.

Lover er identifisert i [64]:

- Arkivloven.
- Forskrift om kontrollkommisjonens virksomhet.
- Forskrift om pasientjournal
- Forvaltningsloven
- Helsepersonelloven
- Helseregisterloven
- Kommunehelsetjenesteloven
- Offentlighetsloven
- Pasientrettighetsloven
- Personopplysningsforskriften
- Personopplysningsloven
- Psykisk helsevernloven
- Smittevernloven
- Sosialtjenesteloven
- Spesialisthelsetjenesteloven
- Tannhelsetjenesteloven

Følgende beskrives det regelverket som berører oppgavens område:

A.1 Personopplysningsloven og forskrift til personopplysningsloven

Personopplysningsloven [62] og forskrift til personopplysningsloven [17] er to av de mest sentrale lovene og forskriftene som må etterleves ved behandling av personopplysninger. I personopplysningsloven § 13 pålegges den behandlingsansvarlige å sørge for tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger. Kravene til informasjonssikkerhet omfatter både administrative og edb-tekniske forhold i virksomheten. Dette omfatter å sørge for at tilstrekkelig faglig kompetanse er tilgjengelig

hos den behandlingsansvarlige. For å oppnå en tilfredsstillende informasjonssikkerhet står det beskrevet at man skal benytte «planlagte og systematiske tiltak». Dette begrepet innebærer at kjente teknikker og anerkjente standarder for kvalitetsstyring, internkontroll, og informasjonssikkerhet, skal legges til grunn ved sikkerhetsarbeidet. De tiltak som etableres, skal være både organisatoriske og tekniske. Sikkerhetstiltakene og selve informasjonssystemet skal dokumenteres. Dokumentasjonen skal omfatte beskrivelse av organisering, rutiner for bruk samt registrering av hendelser.

Beskrevet i Ot.prp. nr. 92 (1998-99) [87] under kapittelet «Kapittel II Alminnelige regler for behandling av personopplysninger», seksjon «Til § 13 Informasjonssikkerhet» i merknadene til personopplysningsloven § 13, «Sikkerhetstiltak må etableres etter en konkret vurdering av de personopplysninger som behandles i forhold til de trusler mot informasjonssikkerheten som er tilstede». Det er ikke mulig å på forhånd oppstille uttømmende krav til hvor høy sikkerheten skal være for ulike typer behandlinger. Loven angir derfor sikkerhetsstandarder i form av krav til konfidensialitet, integritet og tilgjengelighet. Og beskriver følgende begrunnelse «Hva som skal til for at en konkret personopplysningsbehandling oppfyller disse kravene, avhenger særlig av hvilke trusler personopplysningene er utsatt for. Betydelige trusler vil typisk kreve strenge sikkerhetstiltak før kravene til konfidensialitet, integritet og tilgjengelighet er oppfylt» [87]. Denne vurderingen skal utføres av den behandlingsansvarlige med utgangspunkt i et styringssystem for sikkerhet. Det er kravene til dette styringssystemet som beskrives i dette kapittelet i forskriften.

I forskriften til personopplysningsloven, heretter forkortet «pof» [17], er det spesielt kapittel 2 som omhandler «Informasjonssikkerhet». Her er følgende viktig «fordi som behander personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler der det for å hindre fare for tap av liv og helse, økonomisk tap eller tap av anseelse og personlig integritet er nødvendig å sikre konfidensialitet, tilgjengelighet og integritet for opplysningene».

Her benevnes de paragrafene som synes å være av relevant karakter i forhold til oppgavensbegrensninger og fokus.

Under pof § 2-4 «Risikovurdering» beskrives det at det skal føres oversikt over hva slags personopplysninger som behandles, virksomheten skal selv fastlegge kriterier for akseptabel risiko i forbindelse med den behandlingen av personopplysninger og den som er behandlingsansvarlig skal gjennomføre risikovurdering for å klarlegge sannsynligheten for og konsekvenser av et sikkerhetsbrudd. Videre skal resultatet av risikovurderingen dokumenteres.

Ved pof § 2-5 «Sikkerhetsrevisjon», bestemmelsen pålegger den behandlingsansvarlige jevnlig, å etterprøve sikkerhetsarbeidet for å verifisere at de sikkerhetstiltak som er besluttet etablert, faktisk er iverksatt og fungerer etter sin hensikt. Formålet er å vurdere ledelsens beslutninger opp mot virksomhetens behov for informasjonsteknologi og informasjonssikkerhet.

Ved pof § 2-8 «Personell» benevnes de som skal benytte seg av informasjonssystemet. Her pålegges den behandlingsansvarlige å begrense bruk av informasjonssystemet til det som er tjenstlig nødvendig (autorisasjon og autorisering). Som hovedregel vil all bruk av informasjonssystemet medføre risiko. Slik risiko reduseres til akseptabelt nivå ved hjelp

av sikkerhetstiltak.

Pof § 2-10 omhandler «Fysisk sikring», denne bestemmelsen pålegger den behandlingsansvarlige å benytte seg av sikkerhetsmekanismer for å hindre uautorisert adgang til utstyr benyttet for behandling av personopplysninger eller med betydning for informasjonssikkerheten. Eksempelvis skal tjener- og klientmaskiner, og utstyr benyttet som sikkerhetsbarrierer i virksomhetens datanett, fysisk sikres mot uautorisert adgang. Fysisk sikring kan gjennomføres ved tilsyn/vakt, låsing/skjerming av det enkelte utstyr eller låsing/skjerming av lokaler. Tilsyn/vakt etableres eksempelvis ved hjelp av resepsjonstjeneste og ledsagelse av uautorisert personell (besøkende). Låsing/skjerming av utstyr oppnås eksempelvis ved fysiske sikkerhetsmekanismer integrert i utstyret. For låsing/skjerming av lokaler er det som hovedregel tilstrekkelig å etablere normal bygningsmessig sikkerhet. Herunder er det også nødvendig å benevne at gjeldende regel må sees i sammenheng «I personopplysningsloven § 13 pålegges den behandlingsansvarlige å sørge for tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger».

Videre i «pof» nevnes de tre sentrale begrepene innenfor informasjonssikkerhet. § 2-11 «Sikring av konfidensialitet», bestemmelsen pålegger den behandlingsansvarlige å hindre uautorisert innsyn i personopplysninger. Personopplysninger som overføres elektronisk ved hjelp av overføringsmedium utenfor den behandlingsansvarliges fysiske kontroll, skal krypteres eller sikres på annen måte når konfidensialitet er nødvendig. For lagringsmedium som inneholder personopplysninger hvor konfidensialitet er nødvendig, skal behovet for sikring av konfidensialitet fremgå ved hjelp av merking eller på annen måte

§ 2-12 «Sikring av tilgjengelighet», pålegger den behandlingsansvarlige å sikre nødvendig innsyn i opplysninger slik at behandling av personopplysninger kan gjennomføres som bestemt. Det skal også sikres tilgang til informasjon om informasjonssystemet og om sikkerhetstiltak når dette er nødvendig for sikkerhetsarbeidet. Valg av hvilke opplysninger som det skal sikres tilgjengelighet for, og hvilke sikkerhetstiltak som må etableres, følger av resultatet av risikovurderingen. Sikkerhetstiltakene skal også sikre tilgang til annen informasjon med betydning for informasjonssikkerheten. Videre beskrives at det skal finnes en «alternativ behandling skal forberedes for de tilfeller informasjonssystemet er utilgjengelig for normal bruk».

§ 2-13 «Sikring av integritet», pålegger den behandlingsansvarlige å hindre utilsiktet endring av personopplysninger. Også informasjon om informasjonssystemet og om sikkerhetstiltak skal sikres mot uautorisert endring når dette er nødvendig for informasjonssikkerheten. Valg av hvilke opplysninger som det skal sikres integritet for, og hvilke sikkerhetstiltak som må etableres, følger av resultatet av risikovurderingen som er gjennomført. Videre nevner pof det at «det skal treffes tiltak mot ødeleggende programvare».

Samtidig nevner pof i tillegg «Sikkerhetstiltak» under § 2-14. Bestemmelsen understreker at sikkerhetstiltak skal etableres både med formål å hindre et sikkerhetsbrudd, og for å avdekke hendelser som kan forårsake sikkerhetsbrudd. Dette medfører at alle forsøk på uautorisert bruk av informasjonssystemet må registreres, dette kan sees i sammenheng med logging.

§ 2-15 «Sikkerhet hos andre virksomheter» I tillegg til ansvar for sikkerheten i egen avdeling eller organisasjon, må den behandlingsansvarlige også forsikre seg om at informasjonssikkerheten er tilfredsstillende hos de som er kommunikasjonspartnere og leve-

randører av tjenester. Bestemmelsen understreker at den behandlingsansvarlige kun kan overføre personopplysninger til kommunikasjonspartnere, eksempelvis databehandlere, som tilfredsstiller bestemmelsene i dette avsnittet. Formålet med bestemmelsen er blant annet å sikre et nødvendig sikkerhetsnivå i alle berørte parter.

I kapittel 3 i pof som omhandler «Internkontroll»3, beskrives bestemmelsene om internkontrollens formål og virkeområde tilsvarer personopplysningslovens bestemmelser om det samme. Hvor strenge krav som konkret stilles til internkontrollen, herunder dokumentasjonskrav og dermed hvor tyngende kravene blir, vil avhenge av hva slags personopplysningsbehandling som foregår.

A.2 Helseregisterloven

Helseregisterloven [15] bygger på EUs personverndirektiv:(95/46/EC)10. Helseregisterloven gjelder for behandling av helseopplysninger i helseforvaltningen og helsetjenesten, uavhengig av om det skjer i privat eller offentlig regi. Dette innebefatter også når formålet med behandlingen av opplysningene er administrasjon, styring, planlegging eller kvalitetssikring av helsetjenesten, og er ment å omfatte alle de oppgaver helseforvaltningen og helsetjenesten må utføre for å oppfylle virksomhetens formål, som ikke direkte er rettet mot den enkelte pasientbehandling. Loven gir enkeltindividet rettigheter, samtidig som behandlingsansvarlig pålegges plikter. Den gir hjemmel for opprettelsen av lokale, regionale og sentrale helseregistre, men legger også opp til et system med økt bruk av anonyme og avidentifiserte data som beslutningsgrunnlag og for kunnskapsoppbygging [26]. Helseregisterloven slår fast at det skal fremgå hvem som har registrert opplysninger i EPJ. Virksomheten som tar i bruk EPJ vil være databehandlingsansvarlig. Helseregisterloven gir også anledning til å opprette regionale, lokale eller sentrale helseregistre, enten gjennom forskrift eller med direkte hjemmel i loven. Helseregisterloven beskriver, i tillegg til kravet om tilfredsstillende informasjonssikkerhet, at det skal etableres nødvendige internkontrollsystemer og rutiner for å sikre at kravene overholdes. Noe som overlappes av pol og pof. Helseregisterloven og personopplysningsloven stiller like krav til informasjonssikkerhet, men Helseregisterloven tar det femte aspektet i tillegg til de 3 første nevnt under punktet «Sikkerhetsaspekter».

De viktigste punktene i Helseregisterloven [15] er:

§ 6. om «Behandlingsrettet helseregister», behandlingsrettede helseregistre kan føres elektronisk. Det skal fremgå av registeret hvem som har registrert opplysningene. Dette kan gjøres ved hjelp av elektronisk signatur eller tilsvarende sikker dokumentasjon. Regionale helseforetak og helseforetak, kommune og annen offentlig eller privat virksomhet som tar i bruk behandlingsrettede helseregistre, er databehandlingsansvarlig for opplysningene. Foretaket og kommunen kan delegere databehandlingsansvaret.

§ 7. «Regionale og lokale helseregistre», som beskriver at det ikke kan etableres andre regionale og lokale helseregistre med helseopplysninger enn det som følger av denne eller annen lov. Videre beskrives det i § 13 «Tilgang til helseopplysninger i den databehandlingsansvarliges og databehandlers institusjon», at bare den databehandlingsansvarlige, databehandlere og den som arbeider under den databehandlingsansvarliges eller databehandlers instruksjonsmyndighet, kan gis tilgang til helseopplysninger, dette vil i praksis si helsepersonell som har arbeid som er relatert til en pasient.

§ 13. om tilgang beskriver at bare den databehandlingsansvarlige, databehandlere og deres ansatte, kan gis tilgang til helseopplysninger. Tilgang kan bare gis i den grad dette

er nødvendig.

§ 14. tar for seg «Utlevering av helseopplysninger». Helseopplysninger kan utleveres eller overføres for sammenstilling som er tillatt etter § 12. Sammenstilte helseopplysninger kan, etter at navn og fødselsnummer er fjernet, utleveres eller overføres til en virksomhet som bestemt av departementet, når formålet er å avidentifisere eller å anonymisere opplysningene. Helseopplysninger kan dessuten utleveres eller overføres når utlevering eller overføring har hjemmel i eller i medhold av lov, og den som mottar opplysningene har adgang til å behandle dem etter personopplysningsloven.

I § 16. beskrives de tre sikkerhetsaspektene og i tillegg elementet kvalitet under tittelen «Sikring av konfidensialitet, integritet, kvalitet og tilgjengelighet». Den databehandlingsansvarlige og databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet, kvalitet og tilgjengelighet ved behandling av helseopplysninger. Det er sammenfallende med pol og pof sitt krav til informassjonssikkerhet (§13), unntatt begrepet kvalitet som er i tillegg.

§ 18. tar for seg «Databehandlers rådighet over helseopplysninger». En databehandler kan ikke behandle helseopplysninger på annen måte enn det som er skriftlig avtalt med den databehandlingsansvarlige.

Videre i § 27. beskrives det et forbud mot å lagre unødvendige helseopplysninger. Den databehandlingsansvarlige skal ikke lagre helseopplysninger lenger enn det som er nødvendig for å gjennomføre formålet med behandlingen av helseopplysningene. Hvis ikke skal helseopplysningene oppbevares i henhold til arkivloven eller annen lovgivning, skal de slettes.

A.3 Helsepersonellloven

Helsepersonelloven [61] omhandler helsepersonells plikter og ansvar i forbindelse med utøvelse av yrket. Sentralt her er brudd på taushetsplikten. Leger og annet helse relatert personell har et ansvar for å sikre at pasientopplysninger ikke kommer på avveie. Om sensitive opplysninger kommer på avveier ved elektronisk overføring, kan det være brudd på taushetsplikten. Riktig informasjonssikkerhet bidrar til å minske risikoen for brudd på taushetspliktreglene. Her overlappes Personopplysningsloven § 13 hvor det pålegges den behandlingsansvarlige å sørge for tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger. De viktigste punktene i helsepersonelloven er:

I § 21. «Hovedregel om taushetsplikt», hvor helsepersonell skal hindre at andre får adgang eller kjennskap til opplysninger om folks legems- eller sykdomsforhold eller andre personlige forhold som de får vite om i egenskap av å være helsepersonell, herunder konfidensialitet.

Selve plikten for helsepersonell til å dokumentere i journal fremgår av helsepersonellovens § 39, «Den som yter helsehjelp, skal nedtegne eller registrere opplysninger som nevnt i § 40 i en journal for den enkelte pasient. Plikten til å føre journal gjelder ikke for samarbeidende helsepersonell som gir hjelp etter instruksjon eller rettledning fra annet helsepersonell».

Videre er Helsepersonellovens § 45. om overføring og utlevering og tilgang til journal og journalopplysninger , hvor det beskrives «Med mindre pasienten motsetter seg det, skal helsepersonell som nevnt i § 39. gi journalen eller opplysninger i journalen til andre som yter helsehjelp etter denne lov, når dette er nødvendig for å kunne gi helsehjelp på

forsvarlig måte. Det skal fremgå av journalen at annet helsepersonell er gitt tilgang til journalen etter første punktum».

I § 46. om «Elektronisk pasientjournal» fastslåes det at «Pasientjournal kan føres elektronisk».

A.4 Pasientrettighetsloven

Pasientrettighetsloven [18] formål er å bidra til å sikre befolkningen lik tilgang på helsehjelp av god kvalitet ved å gi pasienter rettigheter overfor helsetjenesten. Lovens bestemmelser skal bidra til å fremme tillitsforholdet mellom pasient og helsetjeneste og ivareta respekten for den enkelte pasients liv, integritet og menneskeverd. Noen viktige punkter i forhold til oppgavens fokus i forhold til pasientrettighetsloven er:

§ 3-6. «Rett til vern mot spredning av opplysninger». Dette gjelder opplysninger om legems- og sykdomsforhold samt andre personlige opplysninger skal behandles i samsvar med gjeldende bestemmelser om taushetsplikt. Opplysningene skal behandles med varsomhet og respekt for integriteten til den opplysningene gjelder. Taushetsplikten faller bort i den utstrekning den som har krav på taushet, samtykker. Dersom helsepersonell utleverer opplysninger som er undergitt lovbestemt opplysningsplikt, skal den opplysningene gjelder, så langt forholdene tilsier det informeres om at opplysningene er gitt og hvilke opplysninger det dreier seg om.

§ 5-1 Rett til innsyn i journal Pasienten har rett til innsyn i journalen sin med bilag og har etter særskilt forespørsel rett til kopi. Pasienten har etter forespørsel rett til en enkel og kortfattet forklaring av faguttrykk eller lignende.

§ 5-3 Overføring og utlån av journal. Her har pasienten har rett til å motsette seg utlevering av journal eller opplysninger i journal. Opplysningene kan heller ikke utleveres dersom det er grunn til å tro at pasienten ville motsette seg det ved forespørsel.

A.5 Helseforetaksloven

Helseforetaksloven [16] er lovgrunnlaget for overføring av eierskap for sykehusene fra kommuner og fylkeskommuner til staten. Loven beskriver regionale helseforetak (RHF) og helseforetak (HF), og hvordan foretakene skal organiseres og ansvarsforhold.

Noen viktige punkter i loven er:

§ 1. Lovens og helseforetakenes formål. Et regionalt helseforetak skal etter eiers (Helsedepartementet) retningslinjer planlegge og organisere tjenesten og at det legges til rette for at de regionale helseforetakene skal organisere sine sykehus og andre helseinstitusjoner som helseforetak.

§ 2. Lovens virkeområde. Helseforetak er virksomhet som eies av regionalt helseforetak alene og som er opprettet i medhold av § 9. Helseforetak yter spesialisthelsetjenester, forskning, undervisning og andre tjenester som står i naturlig sammenheng med dette.

§ 9. Opprettelse av helseforetak. Utøvende virksomhet skal organiseres som helseforetak.

A.6 Journalforskriften

«Forskriften gir nærmere regler om helsepersonells dokumentasjonsplikt, herunder om innhold i pasientjournaler, føring, retting, sletting, oppbevaring, overføring, tilgang til og tilintetgjøring av journal, jf. helsepersonelloven kapittel 8» [22]. Journalforskriften skiller mellom journal og journalsystem. En journal er knyttet til den enkelte pasient og

dokumentasjonsplikten for helsepersonell. Oppretting av et journalsystem gjelder virksomhetene som yter helsehjelp. Journalforskriften behandler også elektroniske og papirbaserte journaler og journalsystemer under ett. Et pasientjournalsystem, papirbasert eller elektronisk, beskrives i forskriften som et system for føring og oppbevaring av pasientjournaler som skal kunne etterkomme gjeldende regelverk om innsyn, tilgang og utlevering, redigering, retting og sletting, sikring mot innsyn og forsvarlig oppbevaring. Gjeldene her er «Journalsystemet må organiseres slik at det er mulig å etterleve krav fastsatt i eller i medhold av lov, blant annet regler om innsyn i journal, jf. helsepersonelloven § 41 og pasientrettighetsloven § 5-1, tilgang til og utlevering av journal, jf. helsepersonelloven § 25 og § 45 samt pasientrettighetsloven § 5-3, og sikring mot innsyn fra uvedkommende, jf. helsepersonelloven kapittel 5, herunder forsvarlig oppbevaring, jf. helsepersonelloven § 21» [22].

A.7 Informasjonssikkerhet i helsesektoren

Helsesektoren utarbeider i disse dager en norm for informasjonssikkerhet i helsesektoren, på initiativ fra SHDir. Normen skal gi konkrete føringer for hvordan samsvar med regelverket skal oppnås. Formålet med utarbeidelsen av normen er å oppnå en tilfredsstillende informasjonssikkerhet i den enkelte virksomhet i helsesektoren samt en velfungerende, sikker elektronisk samhandling innen helsesektoren. Normen er også ment å være et hjelpemiddel i den enkelte virksomhets arbeid med informasjonssikkerhet. Det skal også nevnes at normen vil være juridisk bindende for de virksomheter som gjennom avtale med Norsk helsenett AS eller andre har forpliktet seg til å følge normen [64]. Dermed må dette også ansees som en del av lovverk.

A.8 Lov om arkivering (arkivloven)

Arkivloven [88] med forskrifter inneholder generelle bestemmelser om offentlige og private arkiv, med hjemmel for forskrift om offentlige arkiv. Forskriften er mer detaljert enn bestemmelsene i Arkivloven med hjemler for Riksarkivaren for ytterligere detaljering. Arkivloven har som formål «å sikre arkiver som har betydelig kulturell eller forskningsmessig verdi eller som inneholder rettslig eller viktig forvaltningsmessig dokumentasjon, slik at disse kan bli tatt vare på og gjort tilgjengelig for ettertiden». Bevaring og tilgjengeliggjøring for ettertiden er formålet med loven. Spesielt § 6. Arkivansvaret, «Offentlige organ plikter å ha arkiv, og disse skal være ordna og innrettet slik at dokumentene er trygge som informasjonsskilder for samtid og ettertid».

Lover:	**Integ.:**	**Konfid.:**	**Tilgj.:**	**Kvalit.:**	**Sporb.:**	**Ikke-forn.:**
Personoppl.loven	X	X	X		X	X
Forskr.til perso.loven	X	X	X	X	X	X
Helseregisterloven	X	X	X	X	X	
Helsepersonellloven	X	X		X		
Pasientrettighetsloven	X	X	X			
Helseforetaksloven		X				
Journalforskriften	X	X	X	X		X
Norm for Info.Sikk.	X	X	X	X		
Arkivloven	X	X	X			

Tabell 6: Oversikt over loververk.

Tabell 6 viser oversikt over hvilke lover som identifiserer begrepene integritet, konfidensialitet, tilgjengelighet, kvalitet, sporbarhet og ikke-fornekting.

B Appendix

Følgende beskrives den modelleringen som ble gjort av helseforetaket til første ROS-analyse.

Modell av systemet til første ROS-analyse
2.2.2006

IKT Infrastruktur

Innhold:

1 INNLEDNING 3

1.1 VIKTIGE SIKKERHETSASPEKTER 3
1.2 ROLLER FUNNET I LOVVERKET 4
1.3 VERDIFASTSETTING 4
1.4 DAGENS AGENDA 4

2 TEKNISKE BESKRIVELSER OG SKISSER 6

2.1 TEORI VED SAMLOKALISERING AV IKT-SYSTEMER. 6
2.2 NEDBRYTING AV SYSTEM. 7
2.3 TEKNISK OPPBYGNING OG STRUKTUR. 7
2.4 GROVSKISSE. 12

1 INNLEDNING

Følgende beskrives hva som er tenkt gjennomført i første ROS-møte. En modell og skisse av system er modellert og beskrevet, basert på materiale fra helseforetaket. Det beskrives også innledningsvis en kort og enkel teori for utgangspunkt til ROS-møtet.

1.1 Viktige sikkerhetsaspekter

Det skilles ofte mellom følgende hovedaspekter ved sikkerhet:

1. Konfidensialitet, beskyttelse mot innsyn fra uvedkommende/uautoriserte personer.
2. Tilgjengelighet, sikring av at tilstrekkelige og relevante opplysninger er tilstedet og kan nåes etter behov.
3. Integritet, beskyttelse mot utilsiktet eller uautorisert endring av data eller systemer. I dette inngår ofte også ”Ikke-benekting”, som beskrives som sikring av at den som har utført en handling, for eksempel. stilt en diagnose, foreskrevet behandling, lest/hentet ut informasjon, ikke kan nekte for dette i ettertid.
4. Kvalitet, sikring av kvalitet i informasjon som overføres, slik at informasjonen ikke fører til misvisende hos den som mottar informasjonen.

Det er flere årsaker til at sikkerhet kan bli kompromittert. Ofte beskrives det som en funksjon av både eksterne og interne forhold [ROS_2004_veiledning.pdf]. Kompromittering av informasjon og objekter i følge [Risikovurdering 2003, ”Sikre samfunnsviktige objekter og informasjon” NSM] skje på tre måter:

1. Trusselaktører – eksterne aktører som ved tilsiktede handlinger forsøker å skaffe seg innsyn i gradert informasjon, eller manipulere eller gjøre den utilgjengelig for de som er autorisert. Når det gjelder objekter vil en aktiv aktør ved tilsiktede handlinger forsøke å påvirke objekters funksjonalitet og ytelsesevne. En slik aktør vil alltid forsøke å finne sårbare punkter som kan utnyttes.
2. Egeneksponering – en virksomhet eller organisasjon gjør seg selv mer sårbar dersom sikringen ikke fungerer etter tilfredsstillende evne. Eksempelvis er mangelfullt sikkerhetsarbeid, dårlig oppfølging, manglende rutiner osv. som vil kunne medføre at gradert informasjon og graderte objekter blir eksponert for uautoriserte. Ofte vil dette bli resultatet dersom regelverket som regulerer sikkerhetstjenesten unngåes. Egeneksponeringen kan skje både gjennom tilsiktede og utilsiktede handlinger.
3. Utro tjenere/medarbeidere – virksomhetens egne ansatte kan utgjøre en risiko, og kan under visse omstendigheter tilsiktet og bevisste handlinger til at informasjon kompromitteres. Drivkreftene kan være egen vinning ved for eksempel økonomi eller komme som et resultat av press fra eksterne aktører.

Ved sikkerhetsarbeid er det et behov for å rette fokus mot alle forskjellige typer trusler for å oppnå en helhetlig tilnærming til sikkerhet. Et helhetlig sikkerhetsarbeid, vil ofte gjøre bedriften robust mot tilsiktede og utilsiktede handlinger [”Veiledning i risiko- og sårbarhetsanalyse Nasjonal sikkerhetsmyndighet april 2005”].

1.2 Roller funnet i lovverket

I lovverket identifiseres det fire roller, hvor av tre blir berørt i vårt tilfelle. Personopplysningsloven definerer og beskriver fire roller i forhold til behandling av personopplysninger:

1. Den *behandlingsansvarlige*; som har bestemmelsesretten over formålet med behandlingen av personopplysninger samt hvilke hjelpemidler som skal anvendes, se nedenfor.
2. En person(*daglig ansvarlig*) med det daglige ansvaret for behandlingen.
3. En *stedlig representant* for behandlingsansvarlige som er etablert utenfor EØS-området og som behandler personopplysninger i Norge (ikke aktuelt i vårt tilfelle).
4. *Databehandler*; er den som behandler personopplysninger på den behandlingsansvarliges vegne og i henhold til skriftlig avtale. Dette betegner virksomheter eller personer som er den behandlingsansvarliges oppdragstaker, jf. outsourcing.

(www.Datatilsynet.no)

1.3 Verdifastsetting

Et viktig og ofte svært vanskelig punkt er å kartlegge og beskrive virksomhetens verdier. [Risikovurdering 2003, ”Sikre samfunnsviktige objekter og informasjon” NSM] beskriver dette. Begrepet verdi benyttes for det objektet eller den informasjonen virksomheten må sikre konfidensialitet, tilgjengelighet eller integritet for. I [”ROS 2004 NSM”- Veiledning] beskrives det at det ”i en slik sammenheng kan det ofte være fornuftig å visualisere systemet ved hjelp av en eller flere representasjonsteknikker”. En verdi for en virksomhet blir ofte identifiseres ved å anslå et følgende tap eller skadepotensial for virksomheten, gjerne ved kostnader for gjenanskaffelse, indirekte kostnader, tap av renome’
osv. Det beskrives videre at ”Ved risiko og sårbarhetsanalyse gjøres dette ofte ved en kombinasjon av konsekvens- og sannsynlighetsvurdering. Konsekvensvurdering er en vurdering av hvilke følger en hendelse kan få for virksomhetens verdier. Vurdering av sannsynlighet for at en hendelse inntreffer har som mål å finne svar på spørsmålet om hyppighet/frekvens”[”NSM-2004”- Veiledning].
.

1.4 Dagens agenda

Følgende beskrives hva som er tenkt gjennomført i det første ROS-møtet.

Hva skal analyseres:

- It-infrastruktur nåværende system, med overliggende applikasjon (DIPS). Slik systemet er pr. dags dato.
- It-infrastruktur ved et fremtidig system med overliggende applikasjon DIPS. Slik systemet vil være ved en overgang til RHF.

Følgende gis det en kort beskrivelse av systemet/tjenesten, dets omgivelser og bruken av systemet:

- It-infrastruktur og EPJ-system, brukes av doktor/lege, sykepleiere, sekretærer osv.
- Behandler sensitiv informasjon med krav til integritet, kvalitet, konfidensialitet, tilgjengelighet. Følgende krav til informasjonen; ingen andre enn pasient, foreldre, spesialsykepleier og/eller spesialist/behandlende lege skal ha tilgang til dataene, hvor personen som skal ha tilgang er i en behandlingsrelasjon med en pasient.
- Kommunikasjon mellom server og bruker PC. Flere grader av autentisering og autorisasjon ved innlogging og bruk av utstyr, for alle brukere.
- Dataene ikke må endres/forvrenges ved overføring eller lagring.
- Tilgjengelighet er svært kritisk.
- Det benyttes PC ved behandling av EPJ-informasjon i en applikasjon, og server som mottar informasjon, og lagrer informasjonen på et lagringsmedium.

Følgende beskrives hva som er målsetting for dagens møte:

- Kort gjennomgang av systemet/tjenesten, dets omgivelser og bruken av det.
- Risikoanalyse og vurdering, strukturert gjennomgang basert på modell:
  - Trusselkartlegging (hva kan gå galt hvor, hvorfor og hvordan) – fokusere på de områdene som er viktigst, f.eks. at uvedkommende får tilgang til sensitive opplysninger, at de som *skal* ha tilgang ikke får det, etc.
  - Identifisering av trusler og uønskede hendelser. En uønsket hendelse inntreffer når informasjon og objekter blir kompromittert. Med kompromittering av informasjon menes her tap av konfidensialitet, kvalitet, integritet og tilgjengelighet.
  - Definere nivå for konsekvens og sannsynlighet, velge risikonivå, og definere hvilke kombinasjoner av konsekvens og sannsynlighet som gir hvilket risikonivå (for eksempel ved hjelp av en risikomatrise). Her vil det benyttes akseptkriteriet definert av helseforetaket.
  - Frekvens/sannsynlighetsanalyse (hvor sannsynlig er det at en trussel vil inntreffe, hvor lett er det å utløse trusselen, hvor ofte tror vi at trusselen vil inntreffe).
  - Diskusjon og beskrivelse av konsekvensene hvis truslene utløses.
  - Oppsummering av det totale risikonivået/risikobildet hvis tiden tillater det.

2 TEKNISKE BESKRIVELSER OG SKISSER

Følgende beskrives kort teori som er funnet vedrørende samlokalisering av IKT-systemer. Tanken med å beskrive detter her, er at teori ikke bestandig er sammenfallende med praksis og derfor kan avvike ved systemet, og ved overgang til et regionalt system.

2.1 Teori ved samlokalisering av IKT-systemer.

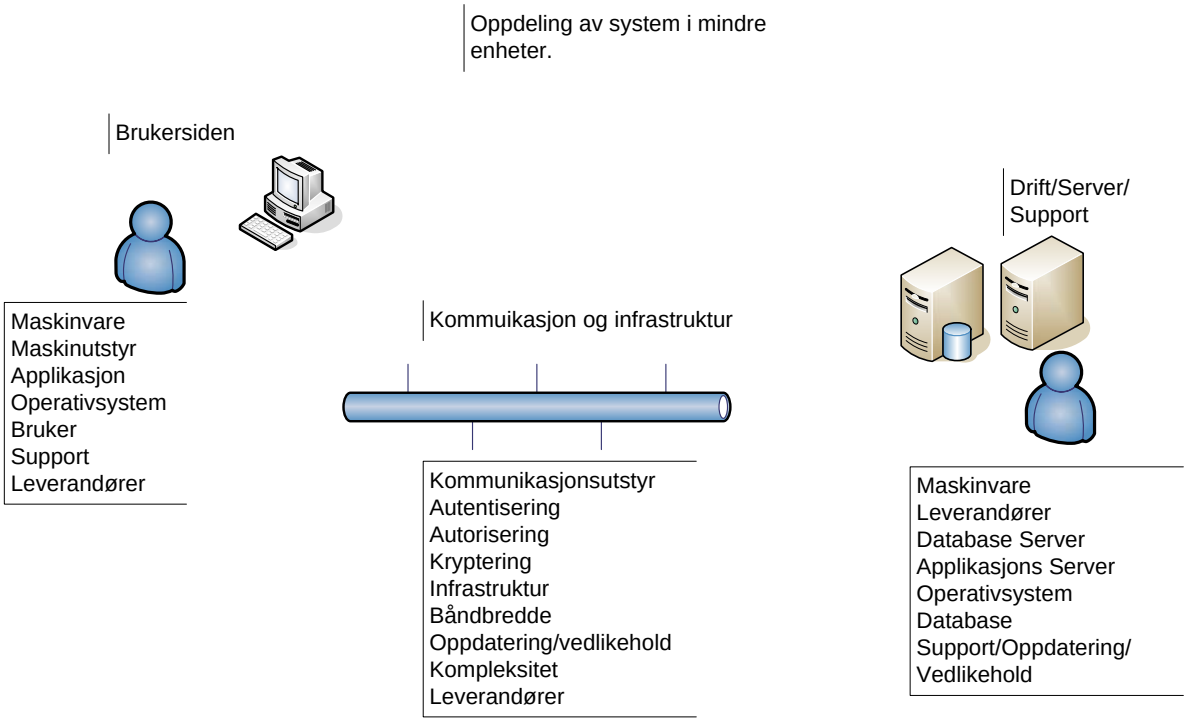
Positive erfaringer:

- Standardisering av en type programvare vil gjøre kompleksiteten av applikasjoner mindre. Infrastruktur vil også ha en positiv påvirkning med tanke på kompleksiteten. En samlokalisering av IKT og standardisering fra forskjellige behandlingsløp, dvs somatikk, psykiatri og rus er mulig vil forenkle administrativt arbeidet med selve systemet og helseforetaket.
- En enkel og velformet arkitektur som omfatter både fysisk og logisk inndeling, med et lite antall forskjellige leverandører er med på å redusere kompleksiteten i nettverket.
- Support og vedlikehold av en type programvare og systemer vil være enklere og langt mer effektivt enn ved flere forskjellige programvarer og leverandører.
- Det kan være en økonomisk gevinst ved å samlokalisere IKT-systemene, fordi det er behov for færre databaser, databaseservere og applikasjonsservere.
- Det kan i større grad benyttes ”tynn”-klienter, som vil redusere innkjøp av nytt datautstyr.
- Enklere reparasjon, vedlikehold, patching og oppdatering av software.
- Økt service til brukerne, ved større bredde kunnskap samlet på et sted.
- Virksomheten kan oppnå større effektivitet, noe som videre vil gi større økonomisk inntjening.
- Virksomheten kan oppnå en bedre og mer helhetlig pasientoppfølgning og få et bedre renome’.
-

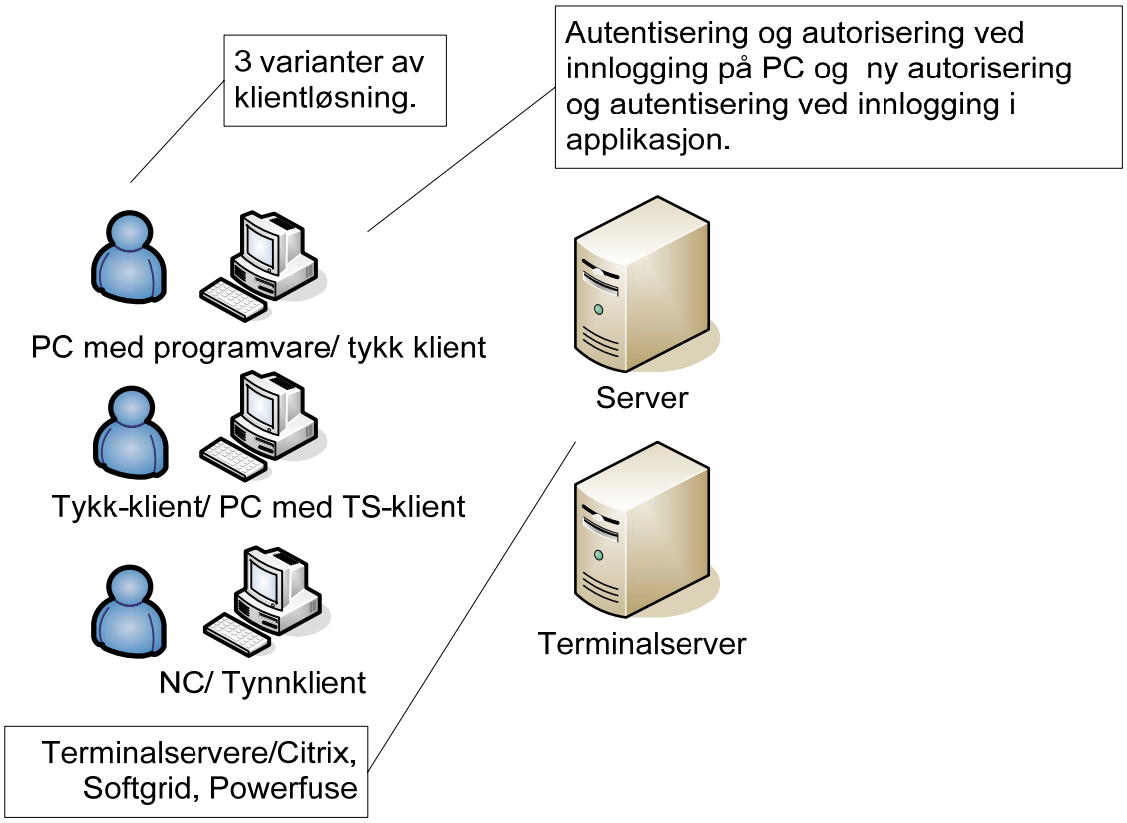
Negative erfaringer:

- Kritiske IKT-systemer medfører flere muligheter for å angripe IKT-systemene, både ved fysiske angrep, angrep gjennom nettverk (ved ikke behov for nærhet til angrepsmålet) og ved at informasjon om enkeltsårbarheter spres raskt.
- Sentralisert lagring av informasjon og avhengighet av sentrale servere, resultere i økt sårbarhet ved knutepunkter i infrastrukturen. Noe som vil påvirke den totale sårbarheten til systemet.
- Ved økt og større bredde i kunnskap samlet på et sted, er det mindre mulighet for å ha kompetanse og være tilgjengelig på lokasjonen hvor det er behov for ekspertisen.
- En sentralisering krever større båndbredde ved at dataen som transporteres fra en lokasjon til en annen vil være større.
- Det vil være større krav til pålitelighet(tilgjengelighet) og QoS til systemene.
- Det oppstår ofte en endring av organisasjonsstrukturen til et mer byråkratisk system. Fordi sentralisering ofte medfører et større behov for kontroll.
- Dataen som behandles er langt større, backup og sikring av data i ulike ledd vil være svært kritisk. Vedlikehold og oppfølging krever samhandling fra flere steder, noe som vil ta lengre tid og kreve flere ressurser.

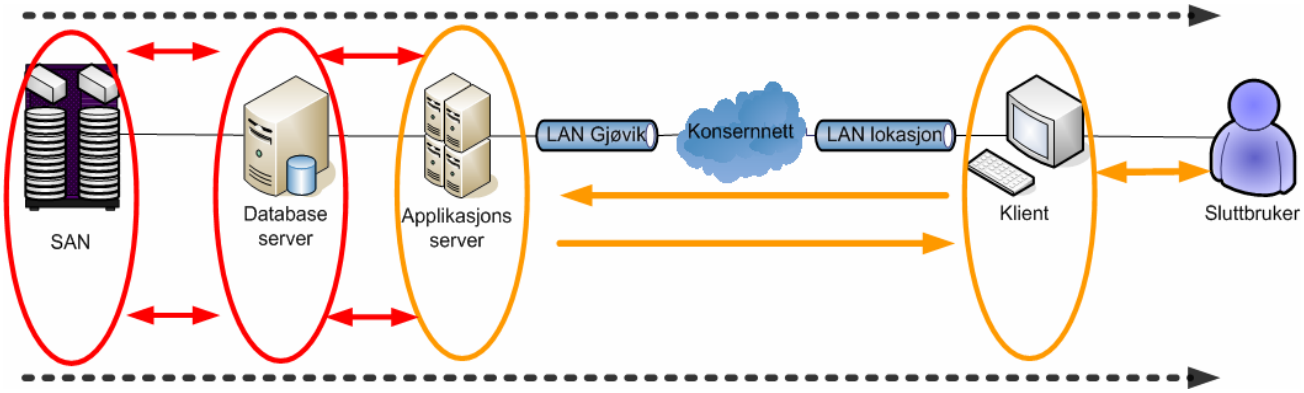
2.2 Nedbryting av system.

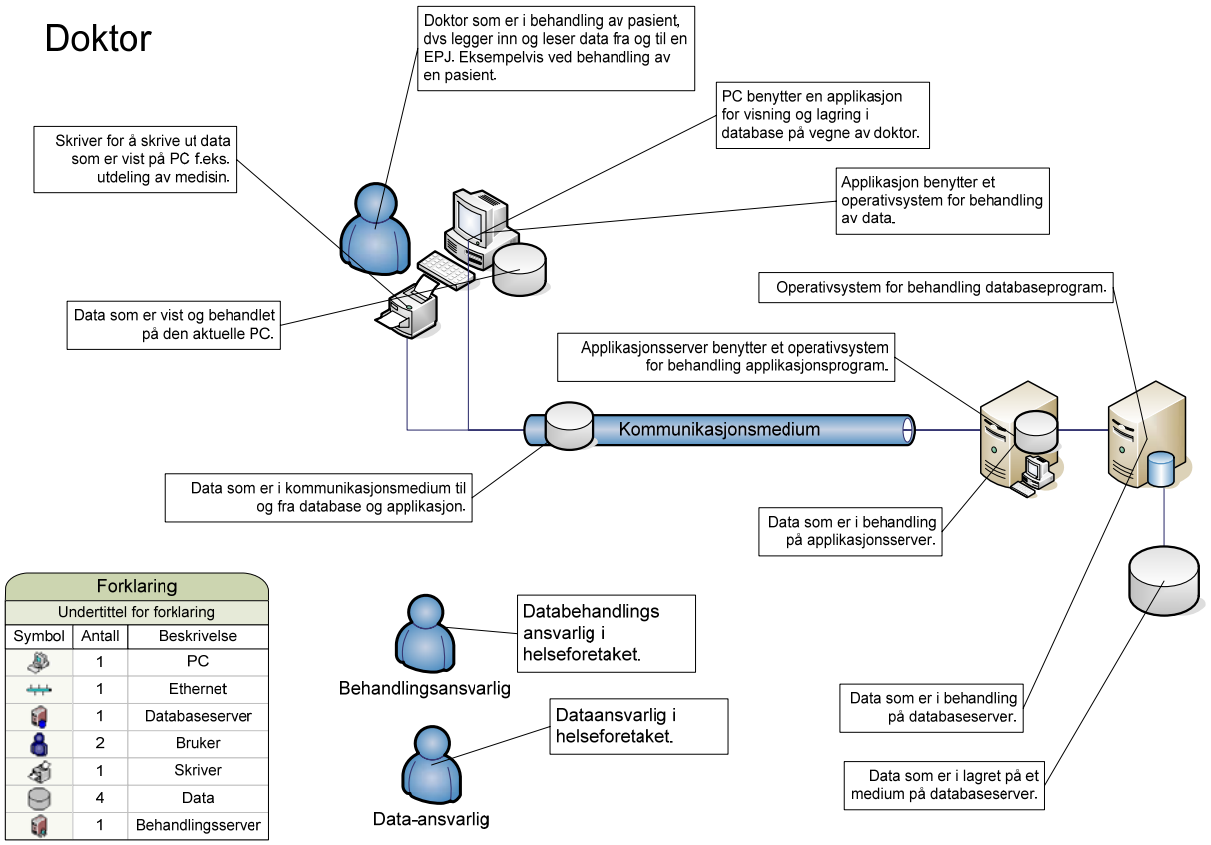


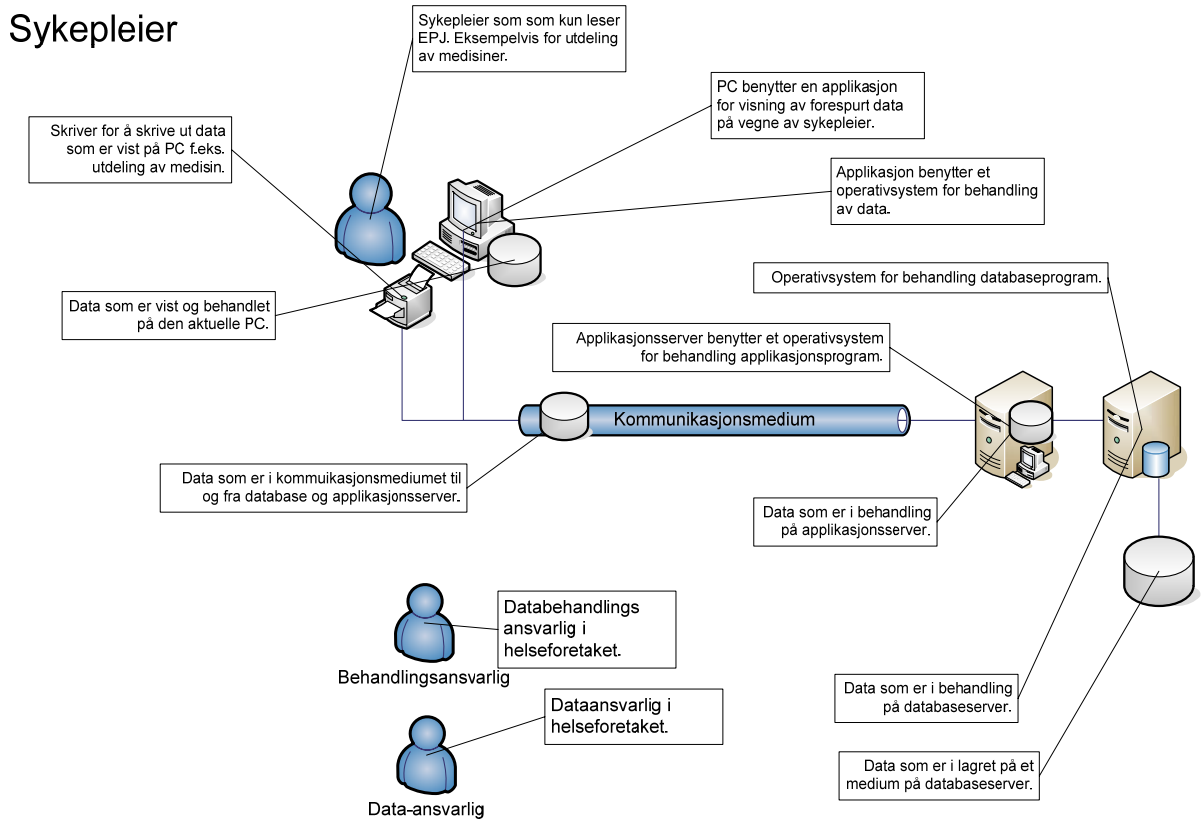
2.3 Teknisk oppbygning og struktur.

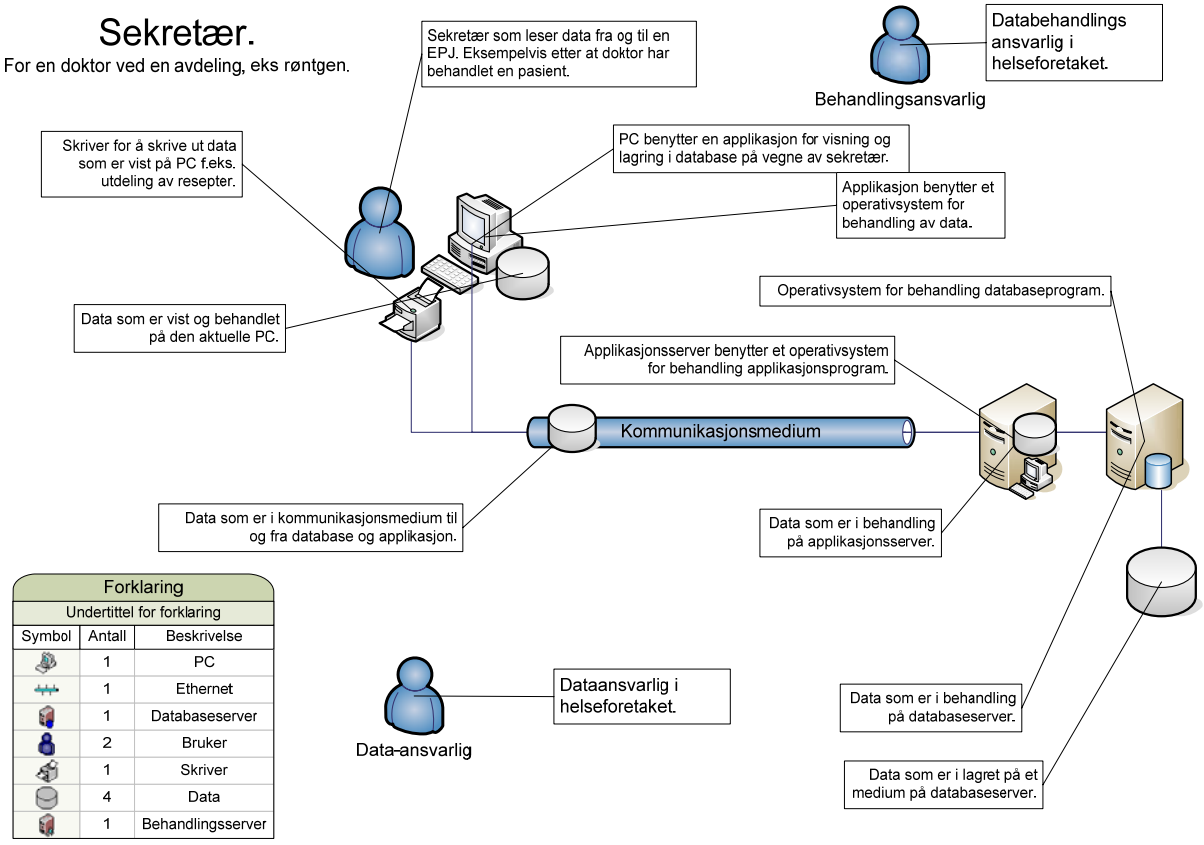


Skisse av kommunikasjon.

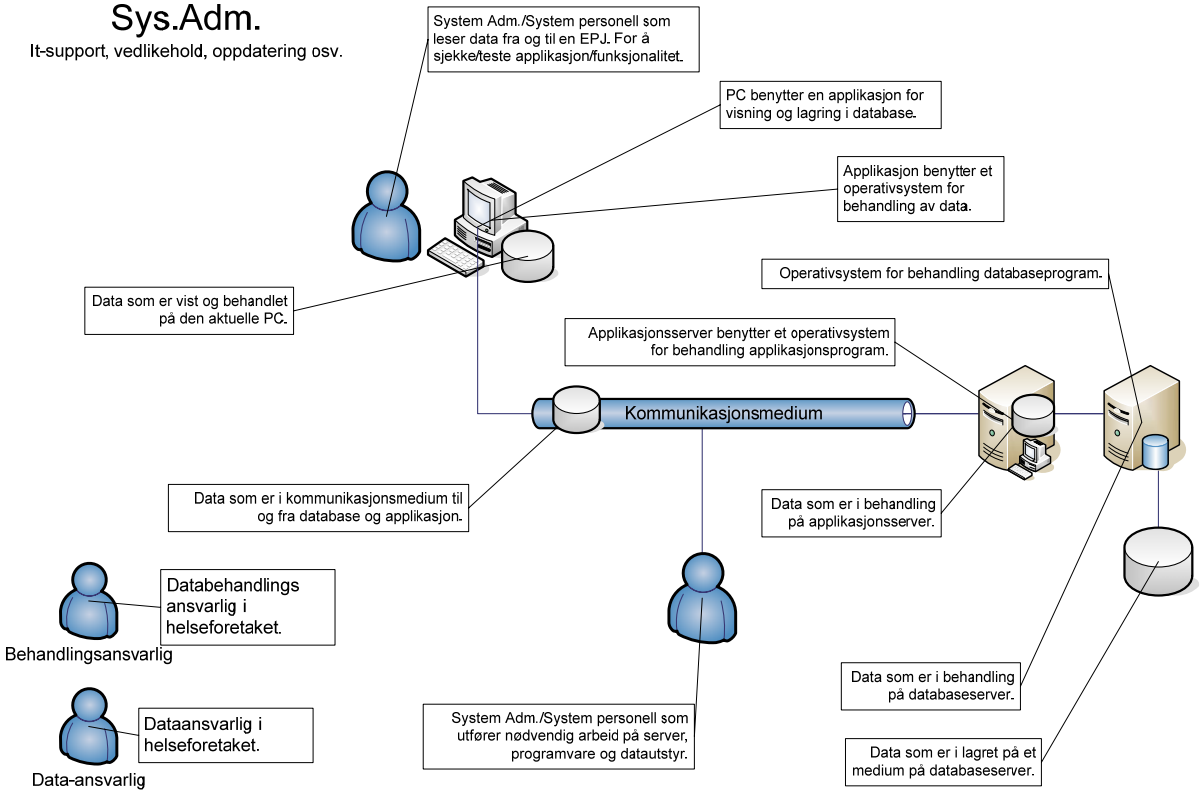


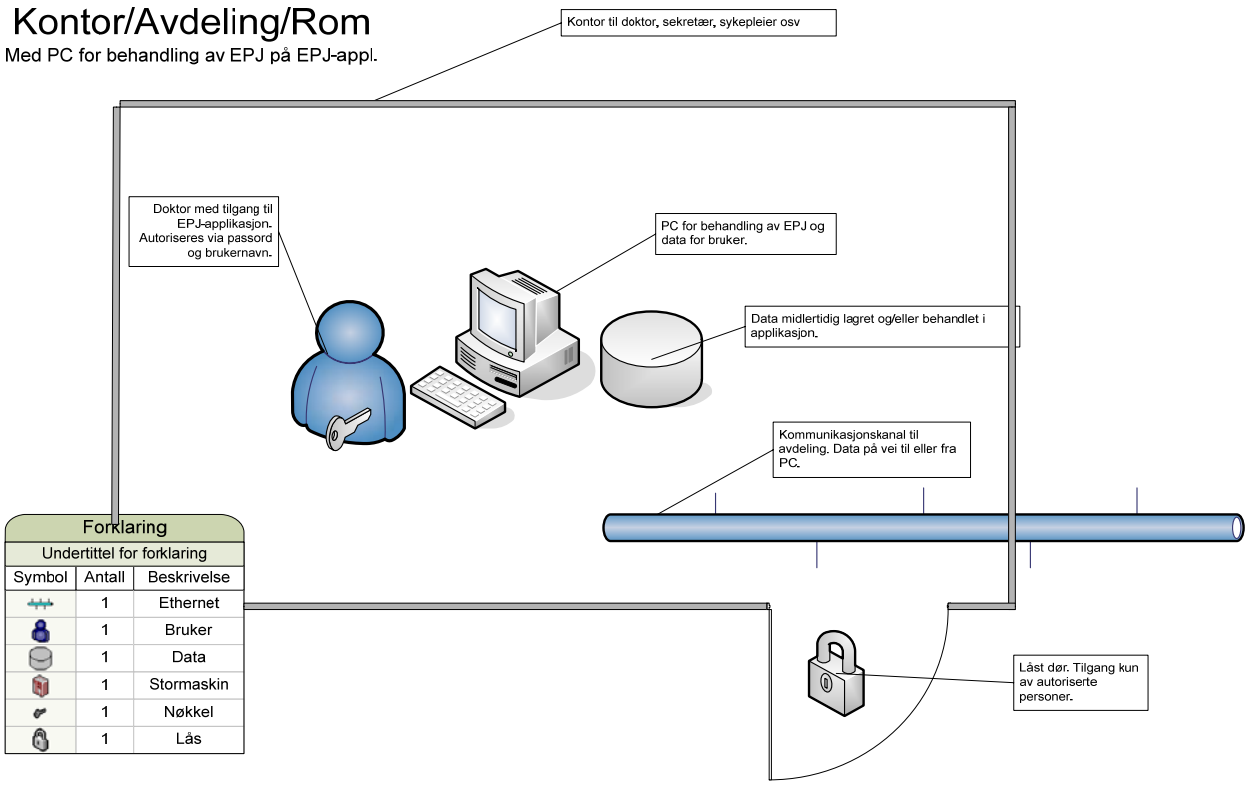


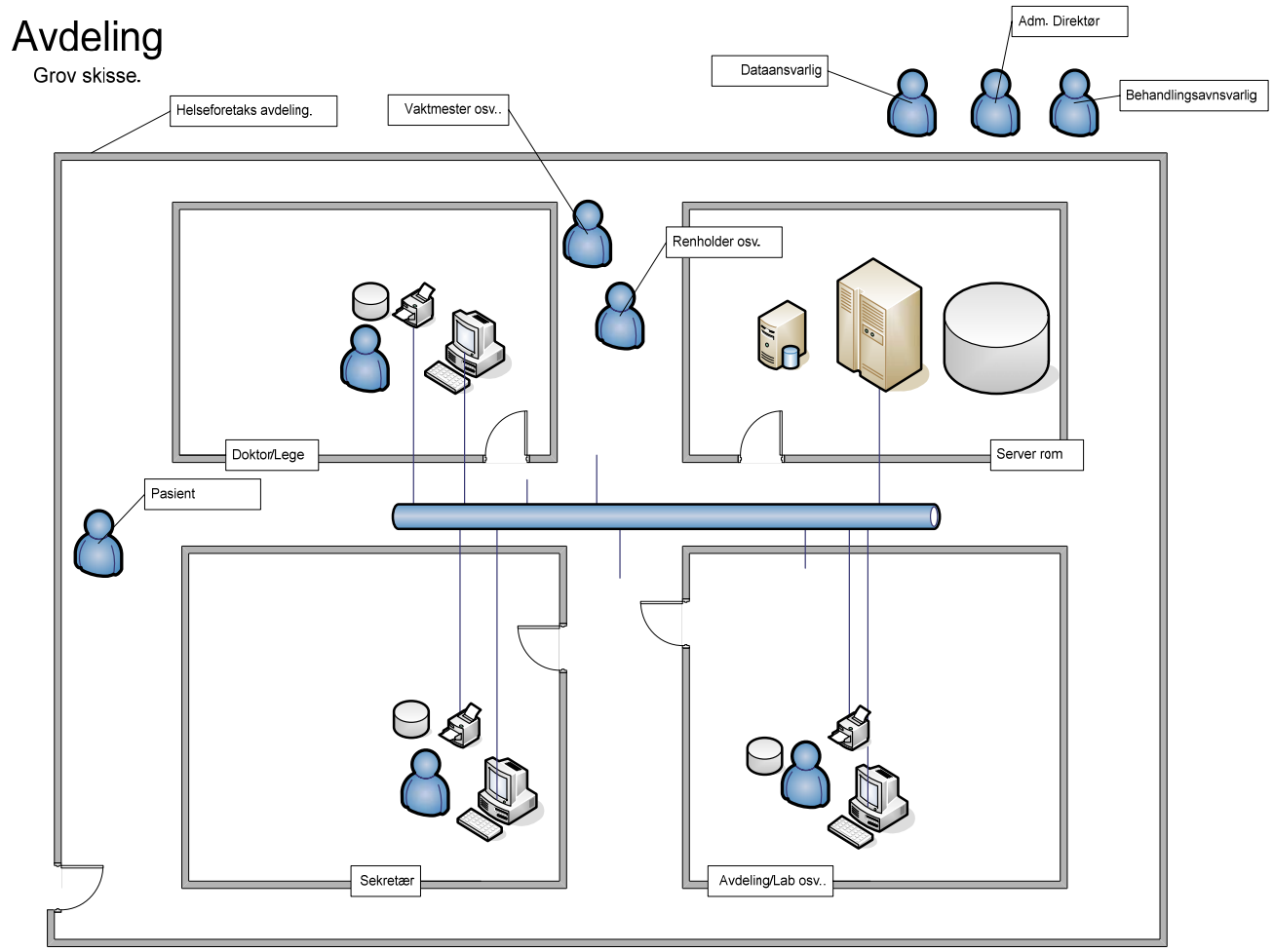


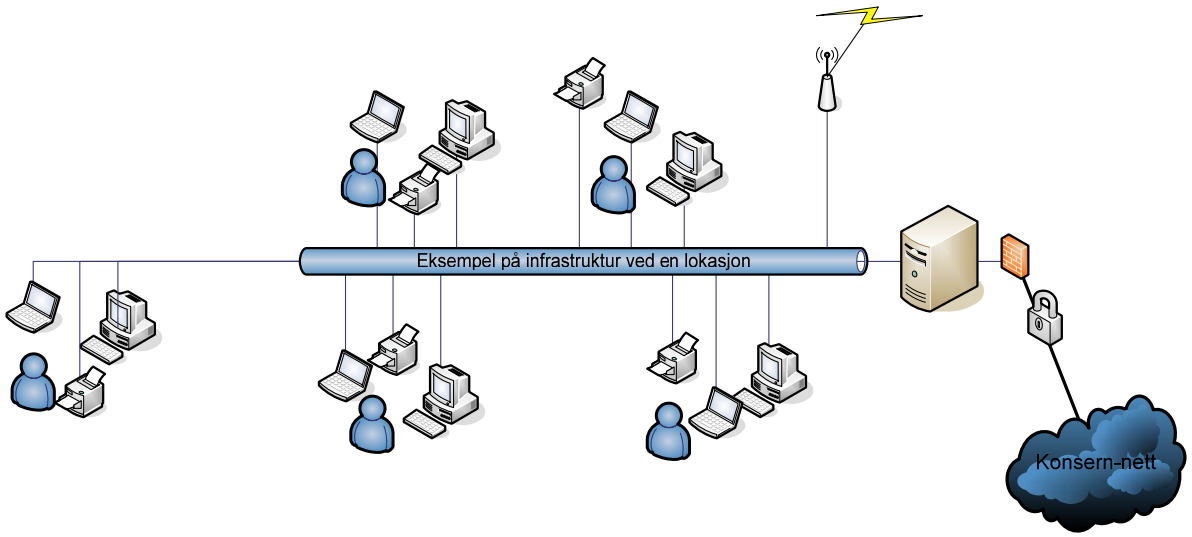


Forklaring		
Undertittel for forklaring		
Symbol	Antall	Beskrivelse
	1	PC
	1	Ethernet
	1	Databaseserver
	2	Bruker
	1	Skriver
	4	Data
	1	Behandlingsserver

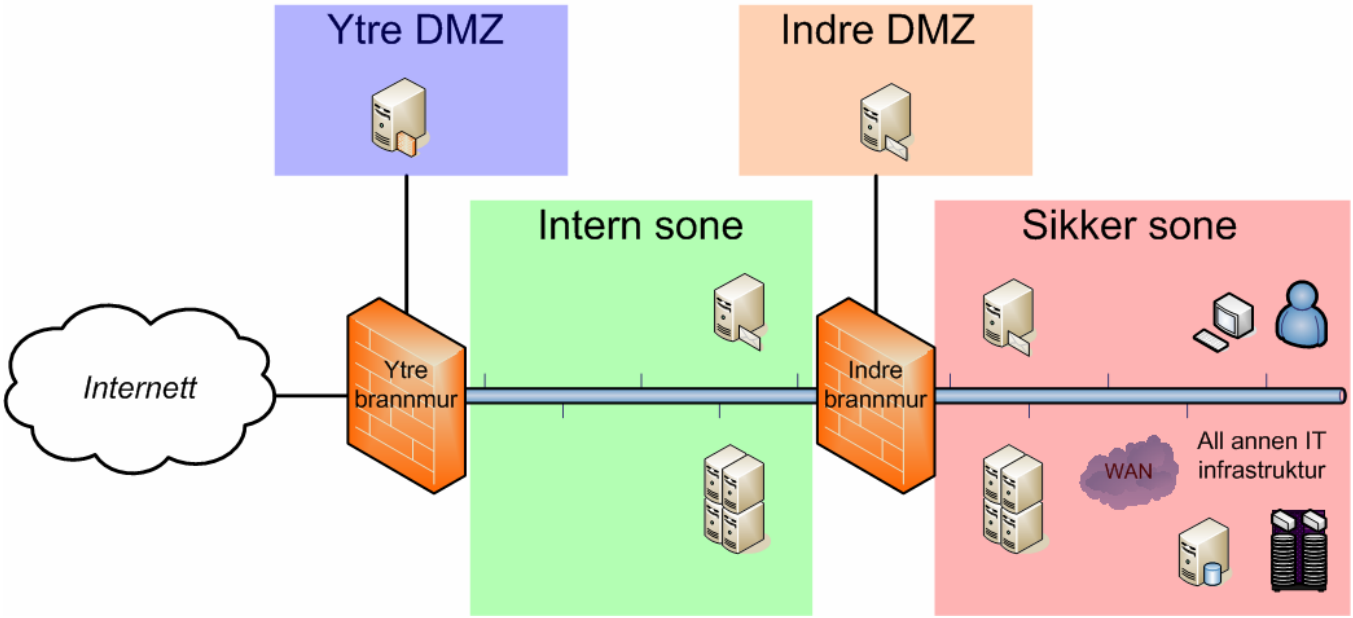

Sys.Adm.
It-support, vedlikehold, oppdatering osv.
System Adm./System personell som leser data fra og til en EPJ. For å sjekke/teste applikasjon/funksjonalitet.
PC benytter en applikasjon for visning og lagring i database.
Applikasjon benytter et operativsystem for behandling av data.
Data som er vist og behandlet på den aktuelle PC.
Operativsystem for behandling databaseprogram.
Applikasjonsserver benytter et operativsystem for behandling applikasjonsprogram.
Kommunikasjonsmedium
Data som er i kommunikasjonsmedium til og fra database og applikasjon.
Data som er i behandling på applikasjonsserver.
Databehandlings ansvarlig i helseforetaket.
Behandlingsansvarlig
Dataansvarlig i helseforetaket.
Data-ansvarlig
System Adm./System personell som utfører nødvendig arbeid på server, programvare og datautstyr.
Data som er i behandling på databaseserver.
Data som er i lagret på et medium på databaseserver.


Kontor/Avdeling/Rom
Med PC for behandling av EPJ på EPJ-appl.
Kontor til doktor, sekretær, sykepleier osv
Doktor med tilgang til EPJ-applikasjon. Autoriseres via passord og brukernavn.
PC for behandling av EPJ og data for bruker.
Data midlertidig lagret og/eller behandlet i applikasjon.
Kommunikasjonskanal til avdeling. Data på vei til eller fra PC.
Låst dør. Tilgang kun av autoriserte personer.
Forklaring
Undertittel for forklaring
Symbol | Antall | Beskrivelse
1 | Ethernet
1 | Bruker
1 | Data
1 | Stormaskin
1 | Nøkkel
1 | Lås

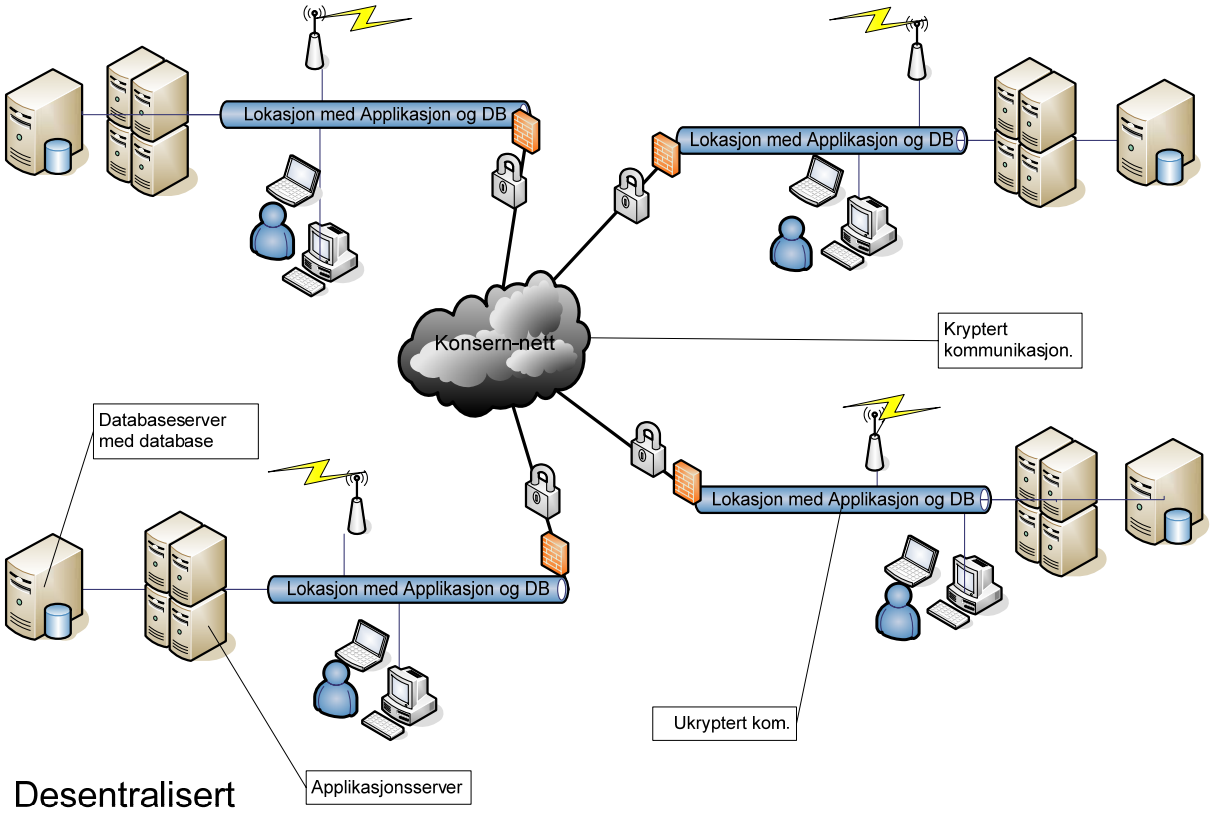

Avdeling
Grov skisse.
Helseforetaks avdeling.
Vaktmester osv..
Dataansvarlig
Adm. Direktør
Behandlingsavnsvarlig
Renholder osv.
Doktor/Lege
Server rom
Pasient
Sekretær
Avdeling/Lab osv..

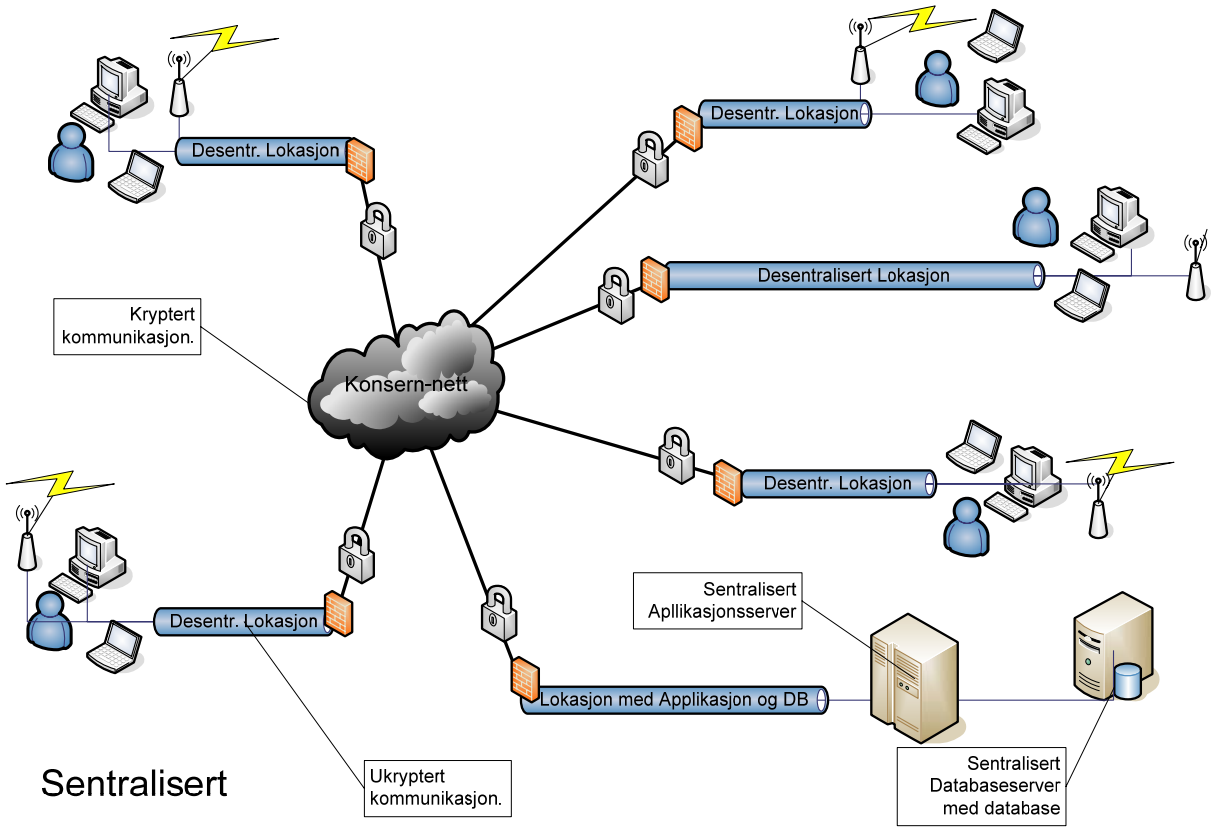

Eksempel på infrastruktur ved en lokasjon
Konsern-nett

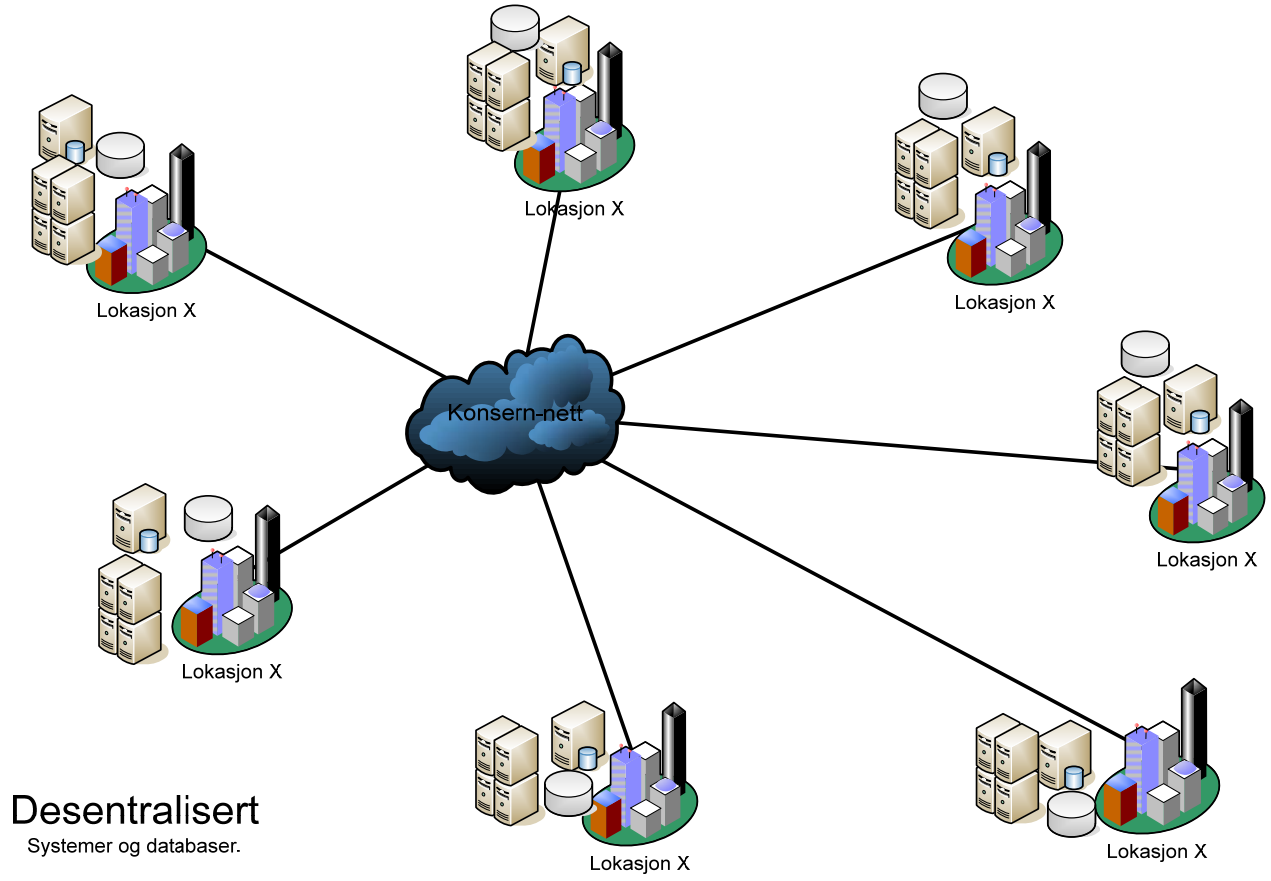
Lokasjon

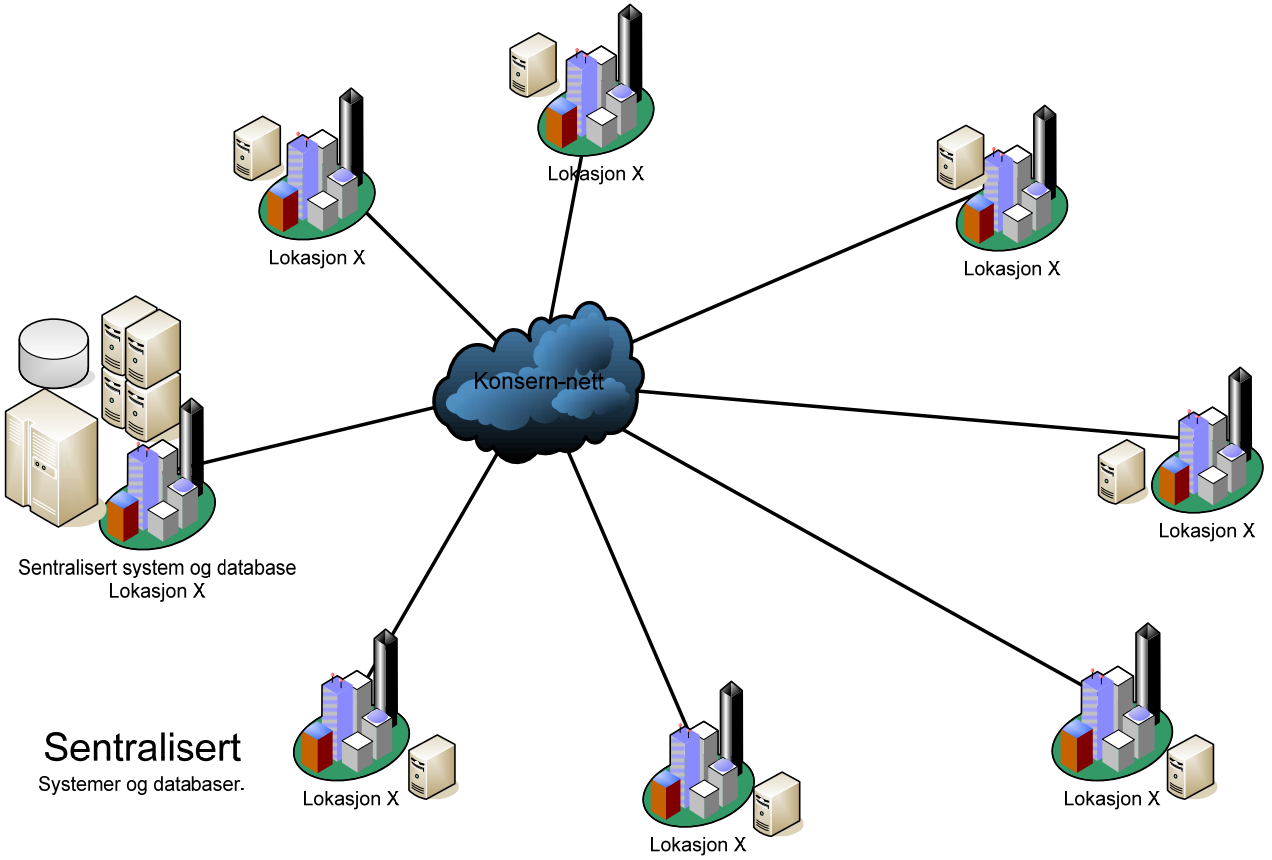


2.4 Grovskisse.




Desentr. Lokasjon
Desentr. Lokasjon
Desentralisert Lokasjon
Kryptert kommunikasjon.
Konsern-nett
Desentr. Lokasjon
Desentr. Lokasjon
Sentralisert Apllikasjonsserver
Lokasjon med Applikasjon og DB
Sentralisert
Ukryptert kommunikasjon.
Sentralisert Databaseserver med database


Lokasjon X
Lokasjon X
Lokasjon X
Konsern-nett
Lokasjon X
Lokasjon X
Lokasjon X
Lokasjon X
Desentralisert
Systemer og databaser.


Lokasjon X
Lokasjon X
Lokasjon X
Konsern-nett
Sentralisert system og database
Lokasjon X
Lokasjon X
Lokasjon X
Lokasjon X
Lokasjon X
Sentralisert
Systemer og databaser.

C Appendix

Akseptkriterier definert av helseforetaket.

1 AKSEPTANSEKRITERIER

På grunnlag av sikkerhetsmålene for informasjonssikkerhet, aksepteres ikke:

- manglende tilgjengelighet til informasjon og elektroniske tjenester
- at uvedkommende får innsyn i opplysninger
- at informasjon går tapt, eller endres uten at gjeldende bestemmelser er fulgt.

For å kunne ha et felles mål på vurdering av akseptable risiko for sannsynlighet og konsekvens, er det etablert følgende to matriser:

- 1.2 Vurdering av sannsynlighet – gir grunnlag for å angi hvilket nivå sannsynlighet for at uønsket hendelse inntreffer, ligger på.
- 1.3 Vurdering av konsekvens – gir grunnlag for å angi hvilket nivå konsekvens ved at uønsket hendelse inntreffer, ligger på.

Disse vil benyttes i risikovurderinger og gi et verktøy for å avklare hvilke trusler som medfører for stor sannsynlighet eller konsekvens, og hvor nye og endrede sikkerhetstiltak må etableres. Bruken vil suppleres med en beskrivelse for hver uønsket hendelse hvilke trusler som kan inntre og hvilke sikkerhetstiltak som skal gi akseptabel risiko for konsekvens og sannsynlighet.

1.1 FORKLARING PÅ MATRISENE

1. Matrise for vurdering og tallfesting av sannsynlighet, med følgende kolonner:
    a. Angivelse av konklusjon på vurdering angitt ved
        i. verdier fra 1 til 4
        ii. tekstlig beskrivelse av hva hver verdi gir av sannsynlighet
    b. Alternativ 1 – *Frekvens* – for vurdering av sannsynlighet. Denne baseres på erfaringsgrunnlag og vil i stor grad benyttes ifm vurdering av tilgjengelighet og eventuell sannsynlighet for tap.
    c. Alternativ 2 – *Letthetsvurdering* – for vurdering av sannsynlighet. Denne baseres på en kombinasjon av vurdering av:
        i. Hvilke motivering som skulle resultere i hendelsen
        ii. Hvilke ressurser som skal til for at hendelsen skal inntre
        iii. Vurdering av eksisterende tiltak

2. Matrise for vurdering og tallfesting av akseptabel risiko for konsekvens, med følgende kolonner:
    a. Angivelse av konklusjon på vurdering angitt ved
        i. verdier fra 1 til 4
        ii. tekstlig beskrivelse av hva hver verdi gir av konsekvens
    b. Beskrivelse av konsekvensen for de ulike aspekter som må vurderes. Dette omfatter vurdering av konsekvens:
        i. for helsehjelpen
        ii. i forholdet til pasienten
        iii. for helsevesenet
        iv. for helseforetaket/personellet
        v. for medarbeiderne.

Dette vil danne felles grunnlag for vurdering av sannsynlighet og konsekvens ved gjennomføring av risikovurderinger.

1.2 VURDERING AV SANNSYNLIGHET

Akseptabel Risiko – Sannsynlighet					
Vurdering:		**Frekvens**	**Letthet**		
			Motivering	**Ressurser**	**Eksisterende tiltak**
4	**Svært høy sannsynlighet**	Hendelsen inntreffer mange ganger årlig (ukentlig/månedlig)	Hendelsen kan forårsakes uaktsomt av autoriserte og uautoriserte medarbeidere, og av eksterne	Hendelsen kan forårsakes av autoriserte og uautoriserte medarbeidere, og av eksterne: - med normal kompetanse - uten at særskilt utstyr/ program må benyttes - uten kjennskap til sikkerhetstiltak	Sikkerhetstiltak er ikke etablert eller fungerer ikke etter hensikten
3	**Høy sannsynlighet**	Hendelsen inntreffer flere ganger årlig	Hendelsen kan forårsakes uaktsomt av autoriserte og uautoriserte medarbeidere Eksterne må opptre med forsett for å forårsake hendelsen	Hendelsen kan forårsakes av autoriserte og uautoriserte medarbeidere: - med normal kompetanse - uten at særskilt utstyr/program må benyttes - uten kjennskap til sikkerhetstiltak Eksterne må ha kjennskap til sikkerhetstiltak for å forårsake hendelsen	Sikkerhetstiltak fungerer ikke etter hensikten
2	**Moderat sannsynlighet**	Hendelsen inntreffer årlig eller sjeldnere	Autoriserte og uautoriserte medarbeidere må opptre med forsett for å forårsake hendelsen Eksterne må opptre med overlegg for å for å forårsake hendelsen	Hendelsen kan forårsakes av autoriserte medarbeidere: - med normal kompetanse - uten at særskilt utstyr/program må benyttes - uten kjennskap til sikkerhetstiltak Uautoriserte medarbeidere må ha kjennskap til sikkerhetstiltak for å forårsake hendelsen Eksterne må ha god kompetanse, ev. benytte særskilt utstyr/program og ha inngående kjennskap til sikkerhetstiltak for å forårsake hendelsen	Sikkerhetstiltak er etablert og fungerer delvis etter hensikten
1	**Lav sannsynlighet**	Hendelsen inntreffer 1 gang pr. 2 år eller sjeldnere	Autoriserte medarbeidere må opptre med forsett for å forårsake hendelsen Uautoriserte medarbeidere og eksterne må opptre med overlegg for å for å forårsake hendelsen	Hendelsen kan forårsakes av autoriserte medarbeidere: - med normal kompetanse - uten at særskilt utstyr/program må benyttes - kjennskap til sikkerhetstiltak Uautoriserte medarbeidere og eksterne må ha god kompetanse, ev. benytte særskilt utstyr/program og ha inngående kjennskap til sikkerhetstiltak for å forårsake hendelsen	Sikkerhetstiltak er etablert og fungerer etter hensikten

1.3 VURDERING AV KONSEKVENS

Akseptabel Risiko – Konsekvens							
FOKUS:		Helsehjelpen	Forholdet til pasienten		Helsevesenet	Helseforetaket/-personellet	Medarbeiderne
4	**Katastrofal konsekvens**	Hendelsen medfører uforsvarlig helsehjelp og manglende sikkerhet (for å unngå personskade) for pasienten	Hendelsen medfører manglende respekt for den enkeltes liv, integritet eller menneskeverd	Hendelsen medfører tap av liv, vedvarende helsetap, betydelig og uopprettelig økonomisk tap eller alvorlig tap av anseelse /integritet.			Hendelsen medfører tap av liv, vedvarende helsetap, betydelig og uopprettelig økonomisk tap eller alvorlig tap av anseelse/integritet.
3	**Stor konsekvens**	Hendelsen medfører helsehjelp med utilstrekkelig kvalitet	Hendelsen medfører manglende tillit mellom pasient og helsevesen/-personell	Hendelsen medfører helsetap, uopprettelig økonomisk tap eller alvorlig tap av anseelse/integritet.	Hendelsen medfører helsetjeneste med utilstrekkelig kvalitet	Hendelsen medfører fengselsstraff, inndragning av autorisasjon, lisens eller spesialistgodkjenning eller stengning av helseinstitusjon.	Hendelsen medfører helsetap, uopprettelig økonomisk tap eller alvorlig tap av anseelse/ integritet.
2	**Moderat konsekvens**	Hendelsen medfører helseopplysninger med utilstrekkelig kvalitet.	Hendelsen medfører at personlig integritet og privatlivets fred ikke ivaretas	Hendelsen medfører betydelig økonomisk tap som kan gjenopprettes eller tap av anseelse/integritet gjennom kompromittering av krenkende opplysninger	Hendelsen medfører helsehjelp med utilstrekkelig kvalitet	Hendelsen medfører bøtestraff, suspensjon av autorisasjon, lisens eller spesialistgodkjenning, erstatningsansvar eller tvangsmulkt	Hendelsen medfører betydelig økonomisk tap som kan gjenopprettes eller tap av anseelse/integritet gjennom kompromittering av krenkende opplysninger
1	**Liten konsekvens**			Hendelsen medfører økonomisk tap som kan gjenopprettes eller tap av anseelse gjennom kompromittering av følsomme opplysninger	Hendelsen medfører manglende informasjon / kunnskap om sykdomsforhold i befolkningen	Hendelsen medfører administrativ reaksjon, herunder advarsel fra helsetilsynet	Hendelsen medfører økonomisk tap som kan gjenopprettes eller tap av anseelse gjennom kompromittering av følsomme opplysninger

D Appendix

Følgende beskrives oversikt over kategorisering av feilkilder til andre ROS-analyse.

Begrep	**Brukerside:**	**Nettverk:**	**Server/Drift:**
Konfidensialitet:	Bruker får tilgang til andres EPJ i DIPS ved behandling av pasient.	Manglende kryptering på kommunikasjons-linjer ved kommunikasjon.	Uautorisert tilgang til datarom ved drift.
	Logisk tilgangs-kontroll mangler for innlogging til EPJ systemer, for brukere.	For små krypterings algoritmer for kryptering data ved kommunikasjon fra lokasjon til lokasjon.	Uautoriserte personer får tilgang til backup av pasient-data, ved forflytting av backup.
	Fysisk tilgangs-kontroll mangler for innlogging til EPJ systemer, for brukere.	Sniffing av passord og data ved kommunikasjon.	

Tabell 7: Illustrerer kategorisering av trusler og risiko innenfor konfidensialitet.

Begrep	**Brukerside:**	**Nettverk:**	**Server/Drift:**
Kvalitet:	Ikke tilstrekkelig båndbredde for kommunikasjon for transportering av data fra lokasjon til lokasjon.	Ustabile nettverk som medfører unødvendig mengde med kommunikasjon.	Overlastet kapasitet på server som medfører ventetid for brukere.

Tabell 8: Illustrerer kategorisering av trusler og risiko innenfor kvalitet.

Begrep	**Brukerside:**	**Nettverk:**	**Server/Drift:**
Integritet:	Infisering av ødeleggende programvare i applikasjon og operativsystem med eksternt lagringsmediet.	Ulike endringer ved data under transportering fra lokasjon til lokasjon i nettverket.	Tap av data ved overoppheting av datautstyr ved daglig drift.
	Doktorer, sykepleiere osv utfører uautorisert endring av andre pasienters data ved daglig drift.		Manglende oppdatering, vedlikehold og tetting av sikkerhetshull i operativsystem og databasesystem.
			Tap av pasientdata som er i behandling i en server ved strømbrudd på UPS og strøm.

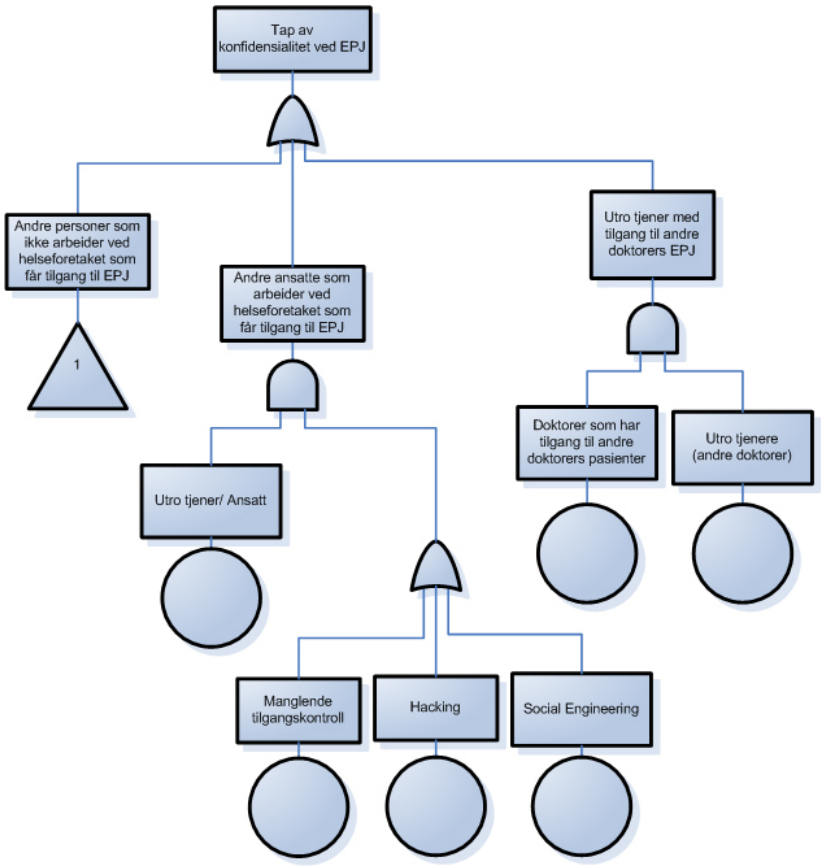
Tabell 9: Illustrerer kategorisering av trusler og risiko innenfor integrietet.

Begrep	**Brukerside:**	**Nettverk:**	**Server/Drift:**
Tilgjengelighet:	Manglende datautstyr på behandlingsrom/ kontor, for doktorer, sykepleiere og sekretærer ved behandling av pasienter.	Manglende eller tap av komponenter i kommunikasjonskanal ved nettverkskommunikasjon fra lokasjon til lokasjon.	Tap og frafall av servere som behandler EPJ, ved manglende redundans på servere.
	Manglende kompetanse ved bruk av datautstyr og programvare for behandling av pasient.	Manglende kartlegging av SPOF i nettverk.	DOS-angrep og hacking på servere som behandler pasientdata og som er i drift.
	Doktorer, sykepleiere osv får ikke logget inn på «bruker-PC» ved innlogging for behandling av pasient.	Manglende redundans i nettverket.	Tap av backupmedium som innholder pasientdata ved rutinemessig backup.
	Bruker får ikke logget inn på EPJ-applikasjon ved behandling av pasient.	Manglende DHCP server medfører ikke tildeling av ip-adresser.	Bruker mengden overstiger kapasitet til servere, som medfører tap av tilgjengelighet.
	Manglende ip-adresse på bruker-PC for behandling av pasienter.		

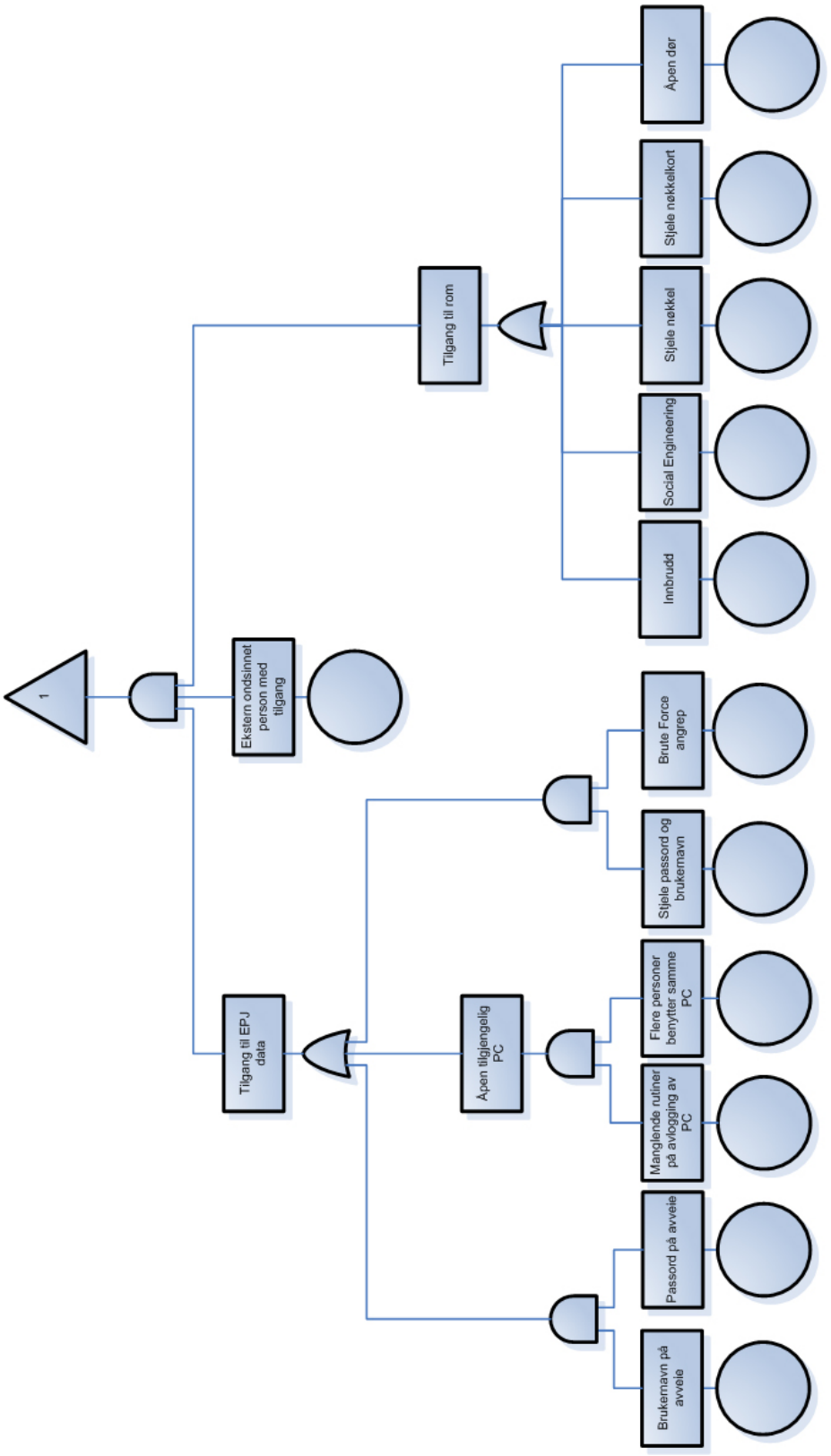
Tabell 10: Illustrerer kategorisering av trusler og risiko innenfor tilgjengelighet.

E Appendix

Et eksempel av et feiltre til andre ROS-analyse.



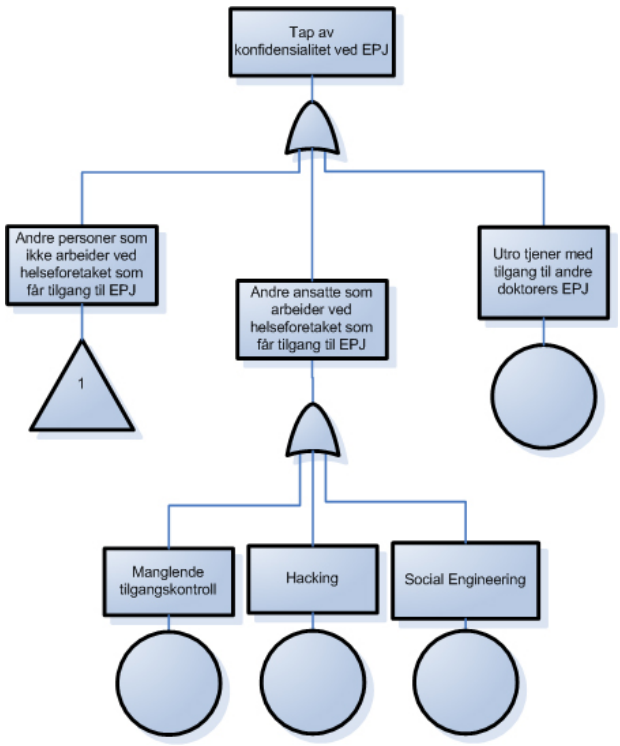
Figur 31: Skisse av feiltre.



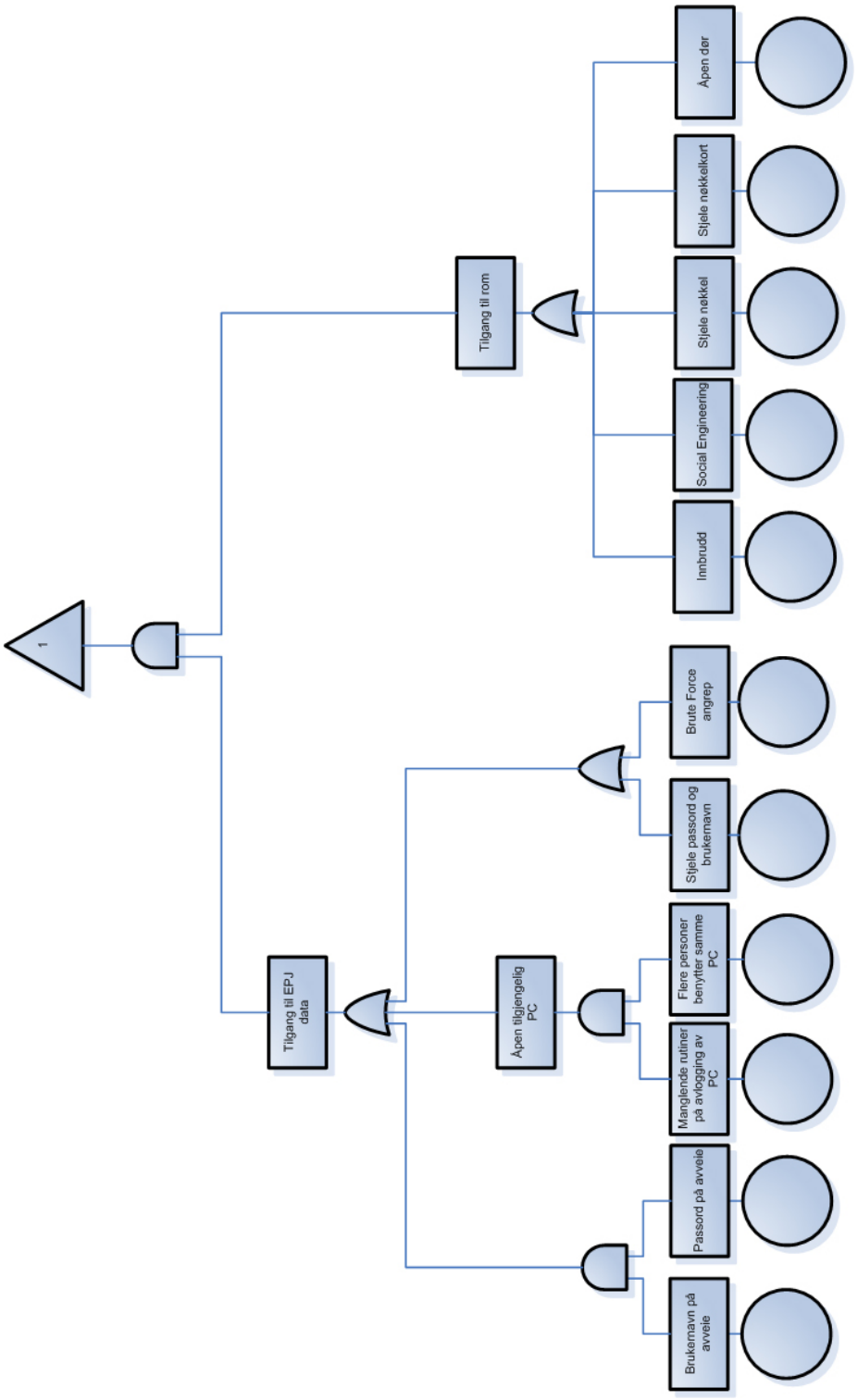
Figur 32: Skisse av feiltre.

F Appendix

Et eksempel på et revidert feiltre etter andre ROS-analyse.



Figur 33: Skisse av et revidert feiltre.



Figur 34: Skisse av revidert feiltre.

G Appendix

Rapport til SHDir.

Konsekvenser ved samlokalisering av IKT-systemer på RHF-nivå.

Innholdsfortegnelse

1 Innledning 3
1.1 Om prosjektet 3
1.2 Målsetting for prosjektet 3
1.2.1 Avgrensning 3

2 Beskrivelse av helseforetak og helsesektor 4
2.1 Innledning 4
2.2 Utvikling 4
2.3 Helsesektor 5
2.4 Helseforetak 5
2.5 Sikkerhet for helsesektor og annen sektor 6

3 Resultater fra studiet 7
3.1 Konsekvenser og gevinster ved samlokalisering 7
3.2 Oppsummering 9

4 Referanser 12

1 Innledning

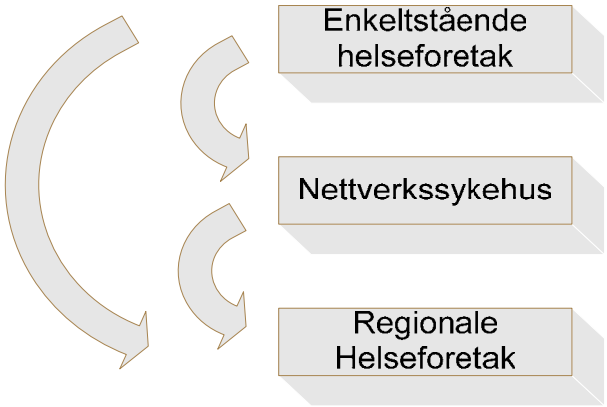
1.1 Om prosjektet

Denne rapporten er utarbeidet som en del av en Masteroppgave innenfor fagområdet informasjonssikkerhet ved Høgskolen i Gjøvik. Arbeidet er en del av SHDir sin strategi i arbeidet med å samlokalisere IKT-systemer på regionalt helseforetak nivå(RHF-nivå). Prosjektet har fått støtte ved råd og veiledning i risiko- og sårbarhetsanalysene av Håvard Fridheim ved FFI (Forsvarets Forsknings Institutt), samt støtte på faglige spørsmål ved Norges Tekniske og Naturvitenskapelige Universitet(NTNU) og Universitetet i Stavanger (UiS).

Rapporten beskriver resultater som fremkommer ved analyse og vurderinger som er gjort ved IKT-infrastruktur og tjenestelevering av EPJ-funksjonalitet(elektroniske pasient journal). Det er gjennomført casestudie av et helseforetak for å avdekke konsekvenser ved samlokalisering av IKT-systemer(informasjon og kommunikasjonsteknologi). Rapporten er forsøkt hevet på et overordnet nivå for å generalisere resultatet til å gjelde flere helseforetak.

1.2 Målsetting for prosjektet

Prosjektet har satt det som mål å påpeke og beskrive endringer og utfordringer ved å gå fra nåværende nettverkssykehus til det som blir sykehus på RHF-nivå. Vi ser for oss følgende skisse av mulige overganger, se figur 1. Helsesektoren har allerede gjennomført en overgang fra enkeltstående helseforetak, til nettverkssykehus. Dette beskrives som det systemet helsesektoren benytter i dag. Vi vil ta utgangspunkt i presentert figur nedenfor, og forsøke å avdekke hvorvidt en overgang til RHF representerer eller kan sammenlignes med en overgang fra ”enkeltstående helseforetak” til nettverkssykehus.



Figur 1 Skisse av overganger

1.2.1 Avgrensning

Det har fra prosjektets start vært et bevisst fokus på å kunne generalisere resultatet til å gjelde flere helseforetak. Det har blitt tatt et valg om å ikke være for detaljert, men fokusere på de større og overordnede trusler og risikoer som oppfattes som utfordrene ved en overgang. Prosjektet omfatter ikke detaljert beskrivelse av økonomiske begrensninger eller gevinster. Det er kun kort nevnt hvor det kan ligge utfordringer og gevinster. Prosjektet har vært gjennomført i våren 2006 med avgrensning til casestudie av et helseforetak. Det er mulig at det finnes enkelte momenter og løsninger ved andre helseforetak som ikke er berørt, men vi mener at resultatet gir en god oversikt over de større utfordringer og konsekvenser helsesektoren vil møte i en overgangsfase.

2 Beskrivelse av helseforetak og helsesektor

I dette kapitlet beskrives dagens utvikling, og hvordan dette påvirker helseforetak og helsesektor.

2.1 Innledning

I dagens samfunn er trygg og sikker forvaltning av sensitiv informasjon helt avgjørende for de fleste bedrifter og virksomheter. Mange bedrifter og virksomheter behandler og lagrer informasjon av høy sensitiv karakter, og det utvikles stadig nye og kraftigere verktøy for å innhente, behandle og utveksle informasjon. Forretningsmessige behov er som oftest det behovet som tvinger frem både samfunnsmessig og teknologisk utvikling. Ofte skjer dette i form av nye krav for å i møtekomme og underbygge arbeidsprosesser[10].
Dette fordrer en økende tendens til at moderne informasjonsteknologi tas i bruk på stadig nye områder. Risiko og sårbarhet er elementer som legger begrensninger på et konsept som kan bidra til å etablere en mer effektiv og rasjonell virksomhet eller organisasjon.

Krav til økt effektivitet i helsesektoren har medført at større mengde tjenester og informasjon bør samlokaliseres, for å underbygge nye krav i arbeidsprosessene. Dette medfører økt grad av informasjonstilgjengelighet, nye kommunikasjonsformer og kommunikasjonskanaler, og større angrepsflate for en angriper. Grensene mellom ulike systemer og maskinvare som tidligere fungerte som barrierer mot angrep, fjernes og det dannes ny sårbarhet og risiko for virksomheten. Konsolidering av store og flere datasystemer representerer nye og vanskelige utfordringer for å ivareta tilstrekkelige sikkerhet og informasjonssikkerhet. Store deler av virksomhetens informasjon samles ofte i ett og samme system. Selv om det kan være nødvendig ut i fra et forretningsmessig perspektiv, får det konsekvenser for sårbarhet og risiko.
Informasjonssikkerhet kan kort beskrives som å besvare kravene innenfor områdene konfidensialitet, integritet og tilgjengelighet. Det kan ofte beskrives som vanskelig å finne den rette balansen mellom områdene. Ofte fordi informasjonen eller objektet som skal sikres, har forskjellig krav til de forskjellige områdene. Dette kan eksemplifiseres ved å sikre for sterk grad av konfidensialitet til et objekt, kan medføre at tilgjengeligheten til objektet blir forsømt.

2.2 Utvikling

Dagens teknologi gir mulighet for effektivisering og fleksibilitet, men fordrer ofte en grad av sentraliserte løsninger for å gi gevinster[5]. Det kan derfor være nødvendig med en helhetlig tilnærming, og fokus på felles løsninger og felles arbeidsrutiner[6]. Bruk av informasjons og kommunikasjonsteknologi(IKT) som hjelpemidler gir mulighet for innsamling, bearbeiding, analysering, overføring, lagring og presentasjon av informasjon[6]. En økt tilnærming til IKT innen helsesektoren vil kunne gi virksomhetene mulighet til å kommunisere bedre og raskere, produsere bedre og raskere, samt transportere bedre og raskere. Samtidig vil den parallelle utviklingen av IKT og organisasjon gjensidig påvirke stadig flere oppgaver og områder, alt fra lagerstyring, produksjon, distribusjon og til markedsføring, og ikke minst kommunikasjon[6].

Oppbygning av organisasjonsstrukturen er grunnleggende og en svært påvirkende faktor for hvordan organisasjonen organiserer sin kommunikasjon med avdelinger og andre virksomheter[6]. IKT har ført til at organisasjoner og virksomheter kan knyttes sammen i felles kommunikasjonsplattformer relativt uavhengig av tid og rom, og på tvers av både avdelingsmessige, organisasjonsmessige og regionale grenser[6]. Tidligere var IKT mest benyttet for intern rasjonalisering. I dag benyttes IKT i større grad for å støtte mer ustrukturerte oppgaver, og i kommunikasjon med underavdelinger og samarbeidspartnere[6]. Dette medfører at større og flere faktorer i organisasjonen blir påvirket.

En av de mest kjente modellene som kan sees i sammenheng med effektivisering av organisasjonen, er Leavitts-diamant[7]. Leavitt hevdet at man ikke kunne se dimensjonene mennesker, system, teknologi, struktur og oppgaver, uavhengig av hverandre. Det beskrives at en endring i en av faktorene medfører et endringsbehov i de andre som også må oppfylles dersom endringen skal være i samsvar med intensjonen.

2.3 Helsesektor

Krav til økonomisk innsparing og økt effektivitet er sentrale begreper for å beskrive dagens samfunnsutvikling innen bedrifter, virksomheter og organisasjoner. De siste årene har vi sett en tendens til økt konvergens av parallelle løp innen informasjons- og kommunikasjonsteknologi[5]. Sentralisering og samlokalisering av ulike systemer og applikasjoner er elementer som er bidrar til en slik konvergens. Sentralisering av IKT-systemer er ofte et resultat av ønske om økt effektivitet.

For eksempel har etableringen av regionale helseforetak (RHF) og sammenslåing av sykehus til større helseforetak, medført at it-funksjoner som lagring og behandling av pasientdata kan samlokaliseres. Samtidig er det innen helsesektoren, som følge av den moderne pasientbehandlingen, et økende behov for å utveksle sensitiv og konfidensiell informasjon om pasienter[11]. Fortløpende tilgang til pasientdata og programvare er en absolutt nødvendig forutsetning for korrekt og effektiv behandling av pasientene. For å oppfylle kravene som stilles, er det behov for sikkerhetsmekanismer som sikrer tilgjengelighet, sikker overføring og lagring av opplysningene. Dette under etterlevelse av et omfattende regelverk.

Dagens system innen helsesektoren kan karakteriseres som tungvint og vanskelig. En overgang til sentraliserte IKT-løsninger og papirløse systemer, innebærer en økt sårbarhet for en, eller flere trusler. Men en endring vil også kunne redusere sårbarhet og risiko på enkeltområder, og samtidig kunne gi mulighet for en betydelig effektivisering for virksomhetene.

2.4 Helseforetak

Helseforetakene har et stort antall forskjellige applikasjoner og systemer, både separate systemer og integrerte systemer. Samtidig har institusjonene og avdelingene en stor variasjon i størrelse og kompetanse. Systemene og lokasjonene er spredt over et stort geografisk område, med varierende tilknytningshastighet. Fundamentalt og kritisk for virksomheten, er kommunikasjonen og tjenesteleveransen til brukeren. Kommunikasjonsløsningene er delt inn i to hoveddeler, lokal kommunikasjon (LAN) som vanligvis er intern-kommunikasjon i en bygning eller en lokasjon, mens ekstern kommunikasjon (WAN - Wide Area Network) er kommunikasjonen mellom lokasjoner. Sikker og stabil kommunikasjon blir derfor en sentral del i infrastrukturen, og for leveranse av tjenesten til brukeren. Leveransen blir aldri bedre enn den kapasitet og tilgjengelighet som kommunikasjonsløsningen kan tilby. Helseforetakets nettverk er bygget rundt 2 deler, kjernenett og distribusjonsnett. Kjernenettet inngår foretakets større lokasjoner, og feil på et samband skal ikke medføre brudd på kommunikasjonstjenesten. Dette betyr at det bestandig eksisterer en eller flere reserveveier tilgjengelig. Kapasiteten er bredbånd med fibertilknytninger på 100 Mbps hastighet for aksess til hovedlokasjonene. Dette er samme hastighet som en bruker har til sin egen PC på kontoret, altså innenfor samme byggning. Distribusjonsnettet er tilknytningen til kjernenettet ved virksomhetens hovedlokasjoner. Enheter tilknyttet distribusjonsnettet har ikke full redundans (det vil si feil at på samband kan medføre avbrudd i tjenesteleveransen til den aktuelle lokasjonen, og de brukere som er tilknyttet via denne kommunikasjonskanalen). Hastigheten for distribusjonsnettene er også betydelig mindre enn hastigheten i kjernenettet. Tatt sikkerhetsaspektet i betraktning, er det innenfor Helsesektoren vanlig å støte på såkalte fler-sonemodeller. Dette innebærer at IKT-nettverket skal ha flere tekniske barrierer mot eksterne nettverk, rutiner og prosedyrer for å

besvare krav til sikkerhet og for å sikre at virksomheten etterlever krav til informasjonssikkerhet.

2.5 Sikkerhet for helsesektor og annen sektor

Krav til sikkerhet finnes i de enkelte virksomheters egne kravspesifikasjoner, sikkerhetspolicyer og gjennom myndighetenes krav i lovverk. Lovverket krever ikke fullstendig spesifikke tiltak implementert, men gir føringer og setter krav for hvordan virksomheten kan oppnå tilfredsstillende sikkerhet og informasjonssikkerhet.

For en alminnelig bedrift vil det sannsynligvis ikke være nødvendig med så strenge krav til sikring av informasjon som det helsesektoren har. Alminnelige bedrifter har ofte krav om å etterleve personopplysningsloven og forskriften til personopplysningsloven. Et helseforetak har derimot et mer omfattende lovverk å forholde seg til. Det stilles forskjellige kriterier avhengig av fagområde, og til hva som er akseptabel risiko ved behandling av sensitive opplysninger. Det vil være svært kritisk om det skulle oppstå et brudd på konfidensialitet, tilgjengelighet, kvalitet, integritet og sporbarhet ved et helseforetak. Feilmedisinering og feildiagnostisering er mulige følger av brudd. Bedrifter og virksomheter i andre sektorer kan akseptere at systemer og informasjon ikke er tilgjengelig i en kortere periode. Og som oftest vil et slikt tap kun medføre tap av økonomisk fortjeneste eller markedsanseelse. Helsesektoren kan derimot ikke akseptere slike tilfeller, fordi det finnes en risiko for å kunne sette liv og helse i fare.

3 Resultater fra studiet

Et prosjekt som omfatter å etablere sentraliserte løsninger på RHF-nivå, representerer store endringer som involverer og påvirker vesentlige deler av organisasjonen, både organisasjonsmessig og teknologisk. I dette kapitlet diskuteres konsekvenser og gevinster ved samlokalisering av IKT-systemer.

3.1 Konsekvenser og gevinster ved samlokalisering

Som beskrevet, settes det stadig større krav til teknologiske systemer som underbygger og effektiviserer arbeidsprosessene. Risiko og sårbarhet legger begrensninger på ulike konsepter som kan bidra til å etablere en ytterligere effektiv virksomhet[5]. Aspekter som sikkerhet og informasjonssikkerhet vil påvirkes når informasjonssystemer utsettes for store endringer i omgivelsene. Krav til økt effektivitet i helsesektoren har medført til at større mengder tjenester og informasjon bør samlokaliseres for å underbygge effektivitetskravene i arbeidsprosessene. Som et resultat medfører dette større informasjonstilgjengelighet, og nye kommunikasjonsformer og kommunikasjonskanaler.

Generelt er det innen helsesektoren primært to forhold som skaper en spesiell og kompleks IKT-infrastruktur. Det første aspektet er antallet brukere og de varierte bruksbehovene. Det andre aspektet er antallet forskjellige applikasjoner og applikasjonskompleksitet. Det sist nevnte aspektet er av betydelig karakter. Det anbefales i fremtiden et økt fokus på standardisering av applikasjoner. Det ligger trolig en langsiktig gevinst for virksomhetene i å ha et fokus på standardisering av applikasjoner i tiden fremover for å løse eventuelle overganger. En standardisering av applikasjoner vil kunne gi bedre muligheter for integrering av forskjellige applikasjoner og systemer. Ved å utnytte standardiseringskonseptet vil det være langt enklere å kunne sentralisere IKT-systemer, og samtidig tilby stabile IKT-tjenester til hele organisasjonen innenfor en akseptabel ressursbruk.
Fellestrekkene innen helsesektoren er at organisasjonene er desentraliserte, samtidig er det tilrettelagt for sentraliserte løsninger i infrastrukturen. Tjenestespektret er bredt og varierende med både basistjenester som e-post, internett-tilgang, og anvendelse av felles systemer og tjenester. Virksomhetene er kontinuerlige avhengig av et stabilt og velfungerende IKT-system for å kunne utføre nødvendige og pålagte arbeidsoppgaver. Således er virksomhetene også avhengig av å ha en velfungerende og effektiv IKT-avdeling. Sentrale løsninger blir ofte etablert for å redusere kostnader og skape stordriftsfordeler. Forventningene til gevinstene kan beskrives ved økte tilgjengelige ressurser, økonomiske fordeler, mer innflytelse overfor leverandører og sentralisering av (spiss)kompetanse som gir mulighet for å forsterke iverksettelse av tiltak.

Organisasjonsmessig gir en regional IKT-enhet mulighet for å kunne splitte ansvarsområder og for bedre å kunne koordinere fysiske, logiske og organisatoriske sikkerhetstiltak[12]. Splitting av ansvarsområder gjør det enklere å stille krav til avdelinger og de ansvarlige. Samtidig vil sentralisering av drift og support frigi ressurser som kan overføres til andre satsningsområder, og som kan bidra til å forsterke iverksettelse av tiltak. Fra et teknisk synspunkt, vil en sentralisering gi færre tekniske installasjoner, og færre knutepunkter i infrastrukturen[13]. Dette betyr et mindre komplekst system som kan gi enklere konfigurasjon og feilsøking, bedre sikring og mulighet for effektiv overvåking.

Fra et medisinskfaglig synspunkt vil pasientbehandlingen kunne bedres og effektiviseres dersom all informasjon gjøres tilgjengelig til riktig tid der pasienten behandles. Forsvarlig og korrekt pasientbehandling avhenger av at alle nødvendige opplysninger om pasienten foreligger for behandlende lege, og ofte er de mest sensitive opplysningene av størst betydning. På den andre siden skal en respektere pasientens rettmessige krav. Det kreves, av hensyn til personvernet og for forsvarlig pasientbehandling, at opplysningene ikke gjøres tilgjengelig for utenforstående parter eller personer, slik at de kan endres/forvrenges under overføringen mellom de involverte parter. Dette reiser både tekniske og juridiske utfordringer

når det gjelder å finne frem til hensiktsmessige løsninger for å kunne yte pasientene optimal behandling innenfor rammen av lovverket.

En av de større sårbarhetene som helsesektoren i fremtiden vil stå overfor, kan være overgangen til EPJ med kun digital lagring. Dette vil sannsynligvis kunne medføre økt sårbarhet ved en sentralisert løsning. Manglende redundans og sikkerhet i løsningene kan gi tap av større mengde informasjon. Et mer eller mindre papirløst sykehus medfører at sykehuset blir mer avhengig av en mer robust teknologi. Krav til 100 % oppetid til alle systemer og komponenter som er i kommunikasjonskanalen mellom bruker og database er ansett som helt nødvendig. En katastrofe lignede situasjon vil sannsynligvis gi konsekvenser for pasienters liv og helse, påvirke de ansattes arbeidssituasjon og helseforetakets omdømme. Ved studert helseforetak beskrives det at det kan oppstå situasjoner som er kritisk for pasientens liv og helse etter mellom 48 t – 5 dager hvis tilgjengelighet til ønsket materiale ikke er tilstede[2]. Det beskrives også at for de øvrige forholdene er det vanskelig å si noe eksakt om hvor lang tid det kan ta før avbruddet vil gi alvorlige konsekvenser[2]. Feil og mangler/bortfall av elementer i kjeden fra bruker til database, vil gi ringvirkninger og ha konsekvenser av ulikt omfang. Feil og mangler på knutepunkter og sentrale elementer/deler i infrastrukturen vil kunne ramme et større og mer omfattende antall brukere. Resultatet vil ofte være av svært kritisk og katastrofal karakter.

En sentral faktor som ofte blir glemt i vurderinger av systemer, er påvirkning og involvering av den menneskelige faktor. Mennesket vil alltid utgjøre en vesentlig del av et system, både som bruker og som forvalter[10]. Menneskets bevisste eller ubevisste handlinger er en sårbarhet og risiko som bør taes i betraktning ved et system[10]. Utfordring ligger både i lojalitet til virksomheten, nysgjerrighet eller ondsinnethet. Dette er betydelige faktorer som kan bli satt på prøve i mange ulike situasjoner, med svært forskjellige konsekvenser. Resultatet vil påvirke det totale sikkerhetsbildet ved systemet.

En annen risiko og utfordring er integrasjon av systemer med inkompatible sikkerhetsmekanismer som kan medføre fragmenterte og dårlige sikkerhetsløsninger. Resultatet vil være en ytterligere sårbarhet. Helseforetakene og systemene er godt sikret mot ytre trusler som ondartet programvare og uønsket tilgang til programmer og data. Men virus som får tilgang fra innsiden kan spres i nettet og i ”verste fall” sette deler av infrastruktur ut av spill. Problemer, svakheter eller feil med program- og maskinvare kan i seg selv medføre stor risiko, noe som ofte resulterer i tap av systemdata og/eller brukerdata. Applikasjons- og programvarekonflikter, kan vise seg å være langt mer sannsynlig enn virusangrep. Det er også et overraskende resultat i studiet, at helsesektoren har et langt større fokus på teknisk sikkerhet og sikkerhetsløsninger framfor organisatorisk sikkerhet. Økt organisatorisk sikkerhet ved bevisstgjøring og holdningskapende arbeid, kan heve den totale sikkerheten.

Det er identifisert at det i dagens system eksisterer feil i tilgangskontroll til EPJ-systemer[3]. Det beskrives i lovverket at kun den lege/doktor som er i en behandlingsrelasjon til en pasient skal ha tilgang til den pasienten som vedkommende behandler. Dagens tilgangskontroll gir en lege/doktor tilgang til andre legers/doktorers pasienter. I dag er tilgang til pasientjournal styrt ut i fra hvilken organisasjonsmessig plassering brukeren har. Det er ikke mulig å gi tilgang ut i fra andre kriterier, for eksempel hvorvidt brukeren faktisk er i en behandlingsrelasjon med pasienten. Leger har for eksempel tilgang til journalnotater fra egen institusjon og egen divisjon som standard. Dette betyr at den komplette elektroniske journalen ikke er tilgjengelig for behandlende personell. Store deler av administrasjonen og kontorpersonalet har derimot i dag tilgang til den hele og komplette journalen.

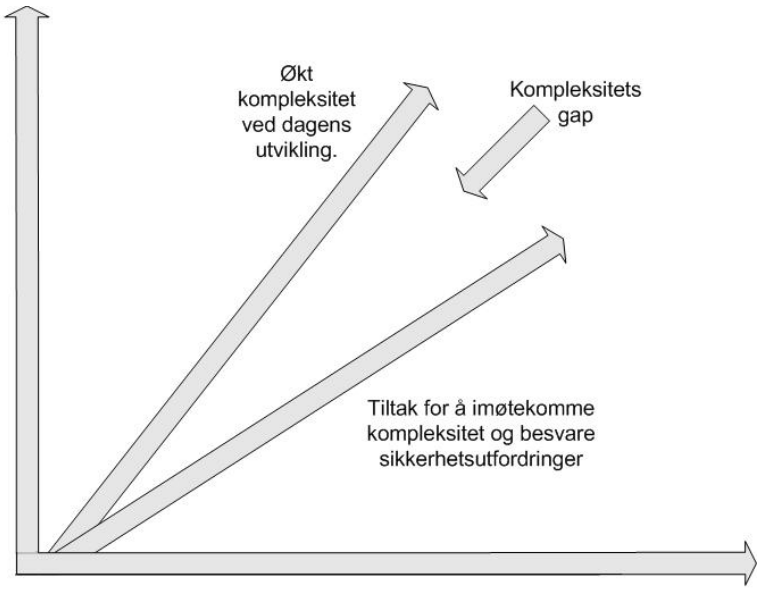
Videre bør det i fremtiden ikke forekomme en blanding av ny og gammel infrastruktur, eller større blanding av flere forskjellige komponentleverandører. Dette kan medføre utilgjengelighet, systemfeil, vanskeligheter med feilsøking og dårlig skalerte løsninger. Det bør derfor settes krav til oppdatering av det utstyr som beskrives som kritisk eller gammelt/utdatert. Samtidig bør det ved endring av IKT-infrastruktur være tilstrekkelige økonomiske midler tilgjengelig for å kunne utforme en ”korrekt og riktig” IKT-infrastruktur.

Opprustning og innkjøp av nytt utstyr må sannsynligvis påberegnes for å kunne tilfredsstille de krav som stilles ved tilgjengelighet, integritet, kvalitet og konfidensialitet. Dagens systemstruktur tilfredsstiller sannsynligvis ikke moderne og gode nok løsninger/utstyr på alle berørte områder i kjeden, men mesteparten av dagens IKT-infrastruktur kan beskrives som langt på vei god nok til å kunne benyttes i en overgang. Det utstyret som utgjør en risiko og sårbarhet, bør derfor byttes ut med nytt og oppdatert utstyr. Samtidig er det nødvendig å utarbeide gode beredskapsplaner og rutiner for å sikre ivaretakelse av virksomhetens vitale prosesser. Dette er grunnleggende for raskt å kunne begrense omfanget av katastrofer. De fleste virksomheter anvender i dag moderne informasjonsteknologi på en slik måte at det ikke er mulig å fungere uten tilgjengelige IKT-systemer[9]. Det er nødvendig å gjennomføre planlegging av strategier for uventede avbrudd i forretningsprosessene, samt å beskytte kritiske forretningsprosesser mot konsekvenser ved feil og uhell. For effektivt å kunne mestre alvorlige driftsavbrudd og katastrofesituasjoner, vil kvaliteten på en gjennomarbeidet og øvet beredskapsplan være helt avgjørende[9]. Når det gjelder drift, vedlikehold og arbeidsprosesser vil det være nødvendig å sam-koordinere og samkjøre disse oppgavene for alle berørte helseforetak som benytter eksempelvis samme servere osv. Samtidig er "Single-point-of-failure"(SPOF) en feilkilde og sårbarhet som må kartlegges og fjernes ved en overgang til et sentralisert system. Det er nødvendig med full redundans i alle elementer, ledd og systemer som behandler informasjon av sensitiv karakter. SPOF er betegnet som en sårbarhet i dagens IKT-infrastruktur, men vil sannsynligvis være mer bekymringsfull ved å inntreffe i en sentralisert IKT-infrastruktur.

3.2 Oppsummering

Fordelene og gevinstene ved å samlokalisere systemer er mange og varierende fra organisasjon til organisasjon. Ofte kan konsekvensene vurderes opp mot gevinstene. Sannsynligvis vil det være hensiktsmessig å vurdere om gevinstene er større enn konsekvensene. Ved konsolidering og samlokalisering, vil grensene mellom ulike systemer og maskinvare som tidligere fungerte som barrierer mot angrep, fjernes og det dannes nye sårbarheter og ny risiko[10]. Konsolidering av store og flere datasystemer representerer utfordringer for å bevare krav om tilstrekkelig sikkerhet[10]. En sentralisering vil sannsynligvis gi et mindre antall knutepunkter i IKT-infrastruktur. Dette vil medføre større sårbarhet ved knutepunktene. Samtidig vil store deler av virksomhetens informasjon ofte samles i ett og samme system. Selv om det kan være nødvendig ut i fra et forretningsmessig perspektiv, får det konsekvenser for sårbarheten. Videre vil integrasjonen av systemer med inkompatible sikkerhetsmekanismer medføre lite samsvar mellom komponenter og dårlige sikkerhetsløsninger. Ofte vil resultatet medføre en ytterligere sårbarhet. Krav til økt effektivitet i helsesektoren har medført at større mengde tjenester og informasjon bør samlokaliseres for å underbygge nye krav i arbeidsprosessene. Som en følge resulterer dette i større grad av informasjonstilgjengelighet, og nye kommunikasjonsformer og kommunikasjonskanaler. Store deler av virksomhetens kritiske informasjon samles i ett og samme system. Selv om det kan være nødvendig ut i fra et forretningsmessig perspektiv, får det konsekvenser for sårbarheten. Å samle informasjonen i ett og samme system gir som oftest systemene økt verdi for virksomheten og organisasjonen, men gjør samtidig systemet mer attraktivt for angripere. En side som også bør vurderes, er at en større del av bedriften vil få økt avhengighet til ett og samme system. En krise eller katastrofelignende situasjon vil sannsynligvis medføre at en større del av virksomheten blir påvirket av hendelsen. Samtidig vil en større informasjonstilgjengelighet medføre et større antall brukere og større mengde passord og brukernavn. Dette krever også et større antall forskjellige restriksjoner for brukere, leverandører og forvaltere. På denne måten vil en konsolidering medføre mindre kompleksitet enkelte steder, men også ytterligere kompleksitet på andre områder. Samlokalisering av IKT-systemer på RHF-nivå, vil trolig tilrettelegge for en ytterligere effektiv helsesektor. Samtidig vil det medføre en større sårbarhet og risiko. En reduksjon av sårbarhet og risiko skjer ikke av seg selv ved etablering av IKT-enhet på regionalt nivå, men åpner for muligheten ved større tilgjengelige ressurser, økt kompetanse, økt koordinering av

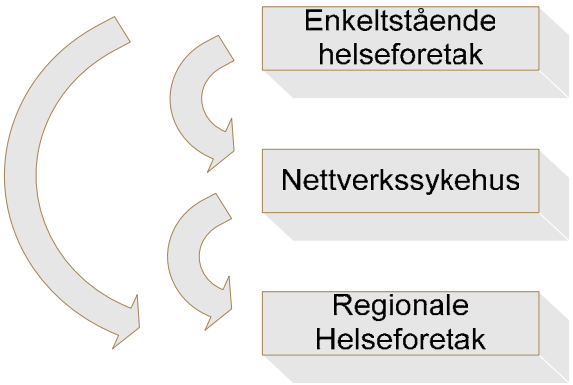
tiltak, og muligheten for splitte ansvarsområder. Økonomi er, som nevnt, ofte den drivkraften som legger press på å gjennomføre en samlokalisering. Men fordelene kan lett forsvinne i krav til redusert sårbarhet og evne til å håndtere større hendelser.



Figur 2 Skisse av kompleksitetsgap. Hentet fra Audestad[5]

Nærings og handelsedepartementet beskriver at ”Utviklingstrekkene har samlet sett både negativ og positiv innvirkning på sårbarheten i IKT-systemene. Trenden vurderes å gå mot at systemene blir relativt driftssikre og robuste mot enkelthendelser. Det vil si hendelser som en driftsansvarlige "forventer" kan/vil skje. For flere hendelser som inntreffer samtidig, synes det derimot å gå mot økt sårbarhet”[14]. Denne sårbarheten blir høyere dersom utfordringene i tillegg kommer fra villede trusseltyper, ofte der mennesker eller organisasjoner har intensjon om å gjøre skade. Parallelt med økningen i kvalitet og effektivitet som anvendelse av IKT medfører, utvikles det en økende avhengighet til systemene.

Slik vi ser det, vil en overgang til et sentralisert system på RHF-nivå, være en oppskalering av dagens nettverkssykehus. Det er stor sannsynlighet for at helsesektoren vil møte de samme utfordringene som de møtte ved overgang fra enkeltstående helseforetak til nettverkssykehus. Sett i forhold til dagens utvikling, har kanskje dagens overgang til sentralisert løsning to fordeler. Den ene er at utviklingen som har skjedd de siste årene har medført et større fokus på sikkerhet. Den andre er å benytte den lærdom og erfaringer som ble gjort ved forrige endring.



Figur 3 Skisse som viser mulige overganger.

Det finnes utallige teknologiske hjelpemidler som kan benyttes for å besvare og imøtekomme spørsmålet om tilstrekkelig sikkerhet og informasjonssikkerhet. Dette er allerede i tatt i bruk i

helsesektoren, slik at muligheten for å besvare og imøtekomme både teknologisk utvikling og samfunnsmessig utvikling er tilstede.

Ved en overgang til et sentralisert system vil IKT-avdelingens rolle i helseforetaket få en betydelig større rolle, og det vil stilles større krav til tjenestene som IKT-avdelingen leverer, både ved kvalitet, servicegrad og tilgjengelighet. IKT-infrastruktur og tekniske løsninger må opprustes slik at tjenester ikke faller bort, selv om det oppstår feil på komponenter som inngår i "kjeden". En overgang til sentraliserte løsninger krever at man, i større grad, vil bli avhengig av de elektroniske løsningene, og det vil kreve en profesjonell driftsrutine som drives etter forretningsmessige prinsipper[2]. Kontrakter og retningslinjer som ITIL (IT-Infrastructure Library) og SLA (Service Level Agreement), vil sannsynligvis bli mer sentralt i organisasjonen, både for tilfredsstillelse av egen drift og andres eksterne samarbeidspartneres drift[2]. Helseforetakene og IKT-avdelingene vil sannsynligvis ha behov for økonomiske midler i form av investeringer i nytt utstyr, kompetanseheving og større ressurser, slik at de kan gjennomføre nødvendige tiltak for å imøtekomme kravene til den nye driftssituasjon.

Slik systemet benyttes i dag, er det beskrevet og karakterisert som tungvint. Slik at en sentralisering av IKT-systemene sannsynligvis vil komme før eller siden. Det bør tas forbehold om at en sentralisering av systemene vil medføre større sårbarhet og risiko for helsesektoren. Utfordringer ved økonomi, risiko, og sårbarhet bør vurderes opp mot gevinstene av samlokalisering. En sentralisering av systemene kan gi både muligheter for økonomisk innsparing, bedre kompetanse og bedre ressursbruk i virksomheten. Men den økonomiske fordelen kan lett forsvinne i krav til redusert sårbarhet og evne til å håndtere større risiko og hendelser. Velger en å se bort fra både de økonomiske utfordringene, kan det fortsatt være hensiktsmessig å gjennomføre en sentralisering. Resultatet av en sentralisert løsning kan bli et langt mer rasjonelt helseforetak, en ytterligere effektiv pasientbehandling og bedre pasientoppfølging.

En eventuell overgang vil sannsynligvis prege flere og mange forskjellige sider ved helseforetakene. Samtidig vil en overgang vil sannsynligvis prege den videre organisasjonsutviklingen innen helsesektoren. Neste steg i arbeidet vil sannsynligvis være å utarbeide en strategi for videre utvikling mot sentraliserte løsninger på RHF-nivå. Det vil sannsynligvis være nødvendig med en detaljert oversikt og detaljert analyse av både tekniske, organisatoriske og økonomiske utfordringer helseforetakene står overfor. En slik strategi kan sannsynligvis inngå som en del av helsesektorens videre organisasjonsutvikling og arbeid mot et papirløst sykehus. Det bør også utarbeides en ytterligere teknisk detaljvurdering av risiko og sårbarhet. Et slikt arbeid bør ha fokus på hvilke løsninger som gir minst sårbarhet og risiko. Risiko og sårbarhetsvurderingene bør så settes opp mot mulige gevinster.

4 Referanser

[1] ”Vurdering av risiko og sårbarhet ved drift av elektronisk pasientjournal”, Helse Øst.

[2] ”Sluttrapport EPJ SI-forprosjekt”, Sykehuset Innlandet.

[3] ”Security models for electronic medical record”. Gafurov,Kalstad Svendsen og Helkala. Telektronikk 2005.

[4] “Centralization vs. decentralization of application software”, Schuff, D. & Louis, R. S. 2001.. *Commun. ACM*, 44(6), 88–94.

[5] Audestad, J. A. 2003. *E-bombs and E-granades*. Forelesnings kompendie ved HiG.

[6] Svein Bergum, s. 2004. Informasjons- og kommunikasjonsteknologi (ikt) og innovasjoner i organisasjonsstrukturer, prosesser og nye organisasjonsformer. *Østlands Forsknings notat* nr 06/2004, 38.

[7] Leavitt, H. J. 1965. Applied organizational change in industry : structural, technological, and humanistic approaches. Classic Readings in Organizational Behavior by J. Steven Ott. ISBN: 0-534-11073-8.

[8] IKT, N. 2005. Overordnet ikt-strategi for de regionale helseforetakene, med forslag til felles satsningsområder og tiltak. http://www.helse-sor.no/_innhold/styremoter/dokumenter/vedlegg%20sak%2050-2005%20revidert%20strategiplan%20-%20versjon%202.pdf

[9] Guldbrandsen, R. 20. Mars 2003. Krise- og beredskapsplanlegging, beskyttelse mot avbrudd i kritiske forretningsprosesser. DataZ- ISACA. ISACA.

[10] ”Sårbarheter og trusler mot informasjonssystemer”, NSM-Temahefte 1/2006, Nasjonal sikkerhetsmyndighet

[11] ”Informasjonsutveksling i helsesektoren, Web-løsninger som et alternativ” KITH Rapport 05/03

[12] ”Infrastruktur og sårbarhet”, Kim Johnny Mathisen. Helse Vest IKT.

[13] “Survivability of the modern society – Deregulation of services vs. critical infrastructure vulnerability”. Håvard Fridheim, Forsvarets Forskingsinstitutt (FFI).

[14] Nærings- og handelsdepartementet: Samfunnets sårbarhet som følge av avhengighet til IT, Oktober 2000. http://odin.dep.no/nhd/norsk/dok/andre_dok/rapporter/024101-220003/dok-bn.html