Petter Almklov, Stian Antonsen og Jørn Fenstad

IKT, nye grensesnitt og nye sårbarheter?

Hvordan nye teknologier og organisasjons-former påvirker robusthet og beredskaps-evne for IKT-hendelser ved et sykehus.

Studio Apertura, NTNU Samfunnsforskning AS

NTNU
Samfunnsforskning AS

Avdeling: Studio Apertura

Postadresse: 7491 Trondheim
Besøksadresse: Dragvoll Allé 38B

Telefon: 73 59 63 00
Telefaks: 73 59 62 24
E-post: kontakt@samfunn.ntnu.no
Web.: www.samforsk.no

Foretaksnr. NO 986 243 836 MVA

RAPPORT

TITTEL

IKT, nye grensesnitt og nye sårbarheter?

Hvordan nye teknologier og organisasjonsformer påvirker robusthet og beredskapsevne for IKT-hendelser ved et sykehus

FORFATTERE

Petter G. Almklov, Stian Antonsen og Jørn Fenstad

OPPDRAGSGIVER

Norges forskningsråd

RAPPORT	GRADERING	OPPDRAGSGIVERS REF.	
2010	Åpen	Critical infrastructures, public sector reorganization and societal safety	
ISBN		PROSJEKTNR.	ANTALL SIDER
978-82-7570-222-5		1452	27
DATO		PROSJEKTLEDER	KVALITETSSIKRET
September 2010		Petter G. Almklov	Trond Kongsvik

SAMMENDRAG

Denne rapporten tar for seg hvordan nye organisasjonsmodeller i IKT-organiseringen påvirker robustheten og beredskapsevnen til et sykehus. Prosjektet tar spesifikt for seg organiseringen rundt driftingen av IKT-infrastrukturen ved St. Olavs Hospital og ser på sårbarheter og styrker ved denne fra et organisatorisk sikkerhetsperspektiv. Et utfyllende sammendrag finnes på side ix.

STIKKORD

Sykehus, IKT, Bestiller/utfører-modell, Samfunnssikkherhet, Sikkerhet Robusthet, Kritisk infrastruktur, Beredskap. IKT-infrastruktur

Forord

Denne rapporten beskriver funnene fra siste delstudie av prosjektet Critical Infrastructures Public Sector Reorganization and Societal Safety (CISS). Dette prosjektet er finansiert av Forskningsrådets Program for Samfunnssikkerhet og Risiko (SAMRISK). Prosjektet som helhet studerer de sikkerhetsmessige konsekvensene av restrukturering av organisasjoner som ivaretar samfunnskritiske infrastrukturer som elektrisitetsforsyning, vannforsyning og telekommunikasjon. Denne rapporten er 3. delrapport i dette prosjektet og omhandler IKT-infrastruktur. Siden IKT-infrastruktur er så utbredt og mangfoldig har vi fokusert spesifikt på IKT-infrastrukturen på et sykehus.

Delstudien er utført av Studio Apertura ved NTNU Samfunnsforskning AS. En av prosjektdeltakerne, Stian Antonsen, skiftet arbeidsgiver i løpet av prosjektperioden, men har fortsatt i prosjektet, som dermed har fått hans nye arbeidsgiver SINTEF Teknologi og Samfunn som partner.

Prosjektet fikk finansiering fra forskningsrådet fra 3. kvartal 2007. Vi gjennomførte en generell litteraturstudie[1] samt en spesifikk en rettet mot elkraft-sektoren i slutten av 2007 og gjennomførte en empirisk studie av kraftsektoren (nettselskaper) i første kvartal 2008 (Almklov et al. 2008). Høst 2008 begynte vi på en spesifikk litteraturstudie av konsekvensene av nye organisasjonsformer for sikkerheten i vannforsyningen og deretter gjorde vi empiriske studier av organisasjonene som står for vannforsyningen i Trondheim og Bergen kommune (Almklov, 2010) Den foreliggende rapporten er noe mindre i omfang og basert på et mindre datamateriale enn de to foregående. Den kan leses som en selvstendig rapport, men siden vi begynner å nærme oss avslutningen av prosjektet, vil en del av diskusjonen være fokusert rundt komparasjon med de andre bransjene, og overgripende funn. En komparativ sluttrapport der funnene fra alle delrapportene inkluderes og analytiske hovedtrekk fra prosjektet diskuteres vil foreligge i slutten av 2010.

Vi er stor takk skyldig til Håkon Gammelsæter (Beredskapssjef) og Trond Grimstad (IKT-sjef) ved St. Olavs Hospital. De har kommet med gode innspill til tema og vært gode tilretteleggere for intervjuer og tilgang. Takk også til ansatte og ledere ved St. Olav, Hemit og EDB som har bidratt med litt av sin tid til å snakke med oss.

Trondheim, september 2010
NTNU Samfunnsforskning AS, Studio Apertura

Petter Almklov, Stian Antonsen og Jørn Fenstad

[1] Se Antonsen et al (2010) og rapportene Almklov et al (2008; 2010).

Innhold

Sammendrag

Denne rapporten er en studie av hvordan nye organisasjonsmodeller inspirert av New Public Management influerer på påliteligheten og robustheten til IKT-systemene til et sykehus. Et spesielt fokus har vært rettet mot potensial for storhendelser og beredskapen mot disse. Rapporten er siste casestudie i prosjektet *Critical infrastructures, public sector reorganization and societal safety*, som har studert hvilke effekter nye organisasjonsformer i infrastruktursektorene kan ha på samfunnets sårbarhet. Studien er utført innenfor forskningsrådets SAMRISK-program. Informasjons og kommunikasjonsteknologi blir stadig viktigere på moderne sykehus et eventuelt utfall har et stort skadepotensial. Studien baserer seg på intervjuer med IKT-personell i Hemit, samt utvalgte nøkkelinformanter og brukere ved St Olavs Hospital. Disse er supplert med dokumentstudier. Undersøkelsen er utforskende og søker å konseptualisere og forstå endringer i sårbarhetsbildet som følge av nye organisasjonsformer. Den er sånn sett ikke noen revisjon av dagens systemer, eller en evaluering av hvordan sikkerhetsnivået totalt sett har utviklet seg. Funnene i denne rapporten er både bidrag til den overgripende rapporten for prosjektet om virkningen av NPM på infrastrukturene. Den innholder i tillegg en del spesifikke observasjoner som først og fremst har relevans for IKT på sykehus og St. Olav spesifikt.

Rapporten går gjennom særtrekk ved IKT sammenlignet med andre infrastrukturer og beskriver hvordan IKT i økende grad har blitt kritisk for den daglige driften i helsesektoren. Det er dessuten en type teknologi som innebærer tette koblinger (noe som medfører at man kan få dominoeffekter) og den er relativt ”åpen”, i den forstand at man er avhengig av komponenter, programvare og tjenester fra eksterne parter for å opprettholde driften av systemet. Sikkerheten hviler dermed ikke bare på driftsleverandørens eget arbeid, men også på dens evne til å håndtere risikoen som eksterne parter utgjør, og dessuten ressursen de utgjør i beredskapssammenheng. Den økende kritikaliteten av IKT på sykehuset bør medføre at IKT i større grad blir et tema i beredskapsarbeidet. To tentative anbefalinger i så måte er at man i større grad kjører øvelser som inkluderer både klinikk og IKT-avdeling, og dessuten at det arbeides med å opprettholde kommunikasjonsløsninger som kan fungere uavhengig av IKT-infrastrukturen i beredskapssituasjoner.

Driften av IKT-systemene ved St. Olav baserer seg på ITIL-rammeverket, og er dermed sterkt strukturert. Et viktig punkt med en så pass strukturert samhandlingsmåte som ITIL-rammeverket utgjør, er at informasjonsflyten er svært formell og sentrert rundt et elektronisk saksbehandlingssystem. Hemits førstelinje utgjør på mange måter ”inngangsporten” til dette systemet og er den viktigste grenseflaten mellom klinikkene og IKT-driften i det daglige. Dette systemet fremstår som velfungerende, og verdien av at denne kanalen rendyrkes er sannsynligvis stor. Det kan

også fra et robusthetsperspektiv være nyttig å arbeide med flere parallelle og mer uformelle kommunikasjonsveier og å ha en løpende refleksivitet i forhold til hva som kan falle utenfor i eller være problematisk med systemet.

Som bidrag til hovedprosjektets problemstilling om hvorvidt nye organisasjonsmodeller påvirker sikkerheten, representerer dette caset en organisasjonsmåte som er tungt basert på en forretningslignende organisering, og mange av de positive trekkene vi har observert her illustrerer fordelene med denne. Rigide rapporteringsrutiner, og lojalitet til disse, sørger for svært god historikk. Standardiserte arbeidsprosesser og teknologi, åpenhet i systemet og kobling til fagmiljøer med spesialister gjør at organisasjonen kan trekke inn kompetanse utenfra i løsningen av problemer. Samtidig er det en forutsetning at driftsmiljøet har evne til å sette seg inn i lokale utfordringer som klinikkene vil ha ved et sammenbrudd i IKT-infrastrukturen, hvis organisasjonsmåten skal fungere i forhold til sikkerhet. Kommunikasjon rundt hva konsekvensen et bortfall av IKT-tjenestene kan bety for det kliniske miljøet og risikoen for tap av liv, må også fungere over grensesnittene i organisasjonen. Organisasjonsmodellen, med lange kjeder av leverandører, forutsetter derfor god oversikt over kritiske komponenter og oppgaver som eksterne er ansvarlige for, og samtidig kontroll på de sårbarheter disse kan introdusere for sykehuset. For å løse problemer må en også ha kontroll på de beredskapsressurser som eksterne partnere har tilgjengelig, og være sensitive på endringer i disse ressursene (nedbemanning og forretningsmessige endringer som kan endre leverandørers muligheter til å bistå i beredskapen).

I beredskapssituasjoner utfordres ofte eksisterende kommunikasjons- og koordinerinsstrukturer, og man tvinges ofte til å komme fort opp med nye løsninger. Dette forutsetter at de ulike aktørene i en beredskapssituasjon kjenner hverandres kompetanse og perspektiver og at de har en løpende uformell dialog om sikkerhet. Siden IKT har hatt en sterkt økende betydning for sykehusdriften, og dermed også dens robusthet, vil et integrert beredskapsarbeid og realistiske øvelser der samhandling mellom aktuelle klinikker og IKT-personell i IKT-relaterte beredskapssituasjoner inngår, være nyttig.

1. Innledning

Denne rapporten tar for seg IKT-infrastruktur[2] på et sykehus og ser på hvordan driften av den organiseres. Den er en del av et større prosjekt som ser på konsekvensene som nye organisasjonsmodeller har på sårbarhetsbildet til kritiske infrastrukturer. IKT er en allestedsnærværende infrastruktur i samfunnet, og den er mangfoldig og relativt uhåndgripelig for en empirisk studie av et så pass begrenset omfang som vår. Derfor har vi snevret dette casestudiet inn til å handle om den kritiske infrastrukturen til St Olavs Hospital. Dette valget er grunnet i flere hensyn. Helsesektoren er en sårbar tjeneste der konsekvenssiden av IKT-brudd er åpenbar. St. Olav har også hatt hendelser som har antydet noe av skadepotensialet ved slike brudd og hvilken sårbarhet et moderne sykehus har overfor dem. På bakgrunn av dette har caset en høy egenverdi i den grad vi kan gi innspill til St. Olav og andre helseorganisasjoner om potensielt sårbare punkter når det gjelder IKT-drift og beredskap. I tillegg til dette har man i helsesektoren i større grad en monopolsituasjon, ved at systemene er "lukkede" og at det bare er én tjenesteleverandør for de enkelte driftstjenester[3], noe som gjør caset noe enklere enn om man skulle se på samfunnets sårbarhet i forholdet til IKT-problemer generelt. Selv om caset ikke er representativt for IKT generelt, vil vi som de følgende sidene skal vise kunne trekke konklusjoner både hva angår teknologien og organisasjonsformene i denne infrastrukturen opp mot de andre casene våre og dermed levere den siste brikken i puslespillet inn mot hovedrapporten.

Det vi spesifikt skal se nærmere på er hvordan driften av IKT-systemene på St Olav er håndtert gjennom et system som både innbefatter en Bestiller-Utfører-Modell (som innebærer forretningsrelasjoner internt i helseforetaket) og eksterne tjenesteleverandører, herunder en sentral driftleverandør og flere underleverandører. Denne måten å organisere offentlig sektor på kan ses som en del av det som gjerne kalles "New Public Management" (NPM), som er en betegnelse på en relativt ny og stadig mer omseggripende måte å organisere offentlig sektor på. At det er sammenhenger mellom organisatoriske forhold og sikkerhet er et anerkjent faktum i sikkerhetsforskningen, så i så måte kan man ved disse endringene forvente endringer knyttet til robustheten til IKT-systemet. Slike endringer vil ikke skje i et vakuum, og det er ikke vårt formål å diskutere hvilken organisasjonsmodell som er best, eller å "måle"

[2] Bemerk at vi i denne rapporten referer til IKT-systemene som infrastruktur for samhandling og kommunikasjon til støtte for sykehusets funksjoner. Vår bruk av ordet "infrastruktur" må altså ikke forstås i den mer begrensede betydningen som ligger i en mer teknisk forståelse av IKT-infrastruktur, der infrastruktur refererer til avgrensede deler av et IKT-system.

[3] Det er en arbeidsdeling mellom Hemit og EDB, men de er begge monopolister innefor sitt område.

endringer i risikonivået som følge av organisasjonsendringer. Selv om sikkerheten og robusthetsnivået samlet sett kan være i bedring, er det alltid grunn til å følge opp endringer i risikobildet. Har man fått nye styrker og nye svakheter?

Det overgripende forskningsspørsmålet for denne rapporten er: Hvilke endringer i risikobildet kan identifiseres som følge av nye organisasjonsprinsipper i IKT-driften ved St. Olavs Hospital?

Rapportens struktur

Vi vil i kapittel 2 presentere bakgrunnen for denne studien og de problemstillingene vi tar for oss. Studien vil knyttes an mot sikkerhetsteoretiske problemstillinger og vår tidligere forskning (se Almklov et al., 2008, 2010). Kapittel 3 gir en kort innføring i organisasjonen vi har studert, med spesiell oppmerksomhet på tidligere hendelser knyttet til IKT-systemene. I kapittel 4 beskriver vi metodikken og datagrunnlaget for den foreliggende undersøkelsen. I kapittel 5 presenterer og analyserer vi funnene fra studien som fra ulike vinkler svarer på det overordnede forskningsspørsmålet. I kapittel 6 konkluderer vi og trekker fram de viktigste konsekvensene. Vi diskuterer også kort hvordan dette caset skiller seg fra de andre infrastrukturene som er studert i prosjektet og kommenterer hvilke lærdommer St. Olavs Hospital og andre helseorganisasjoner kan ta av studien.

2. Bakgrunn og teori: Samfunnssikkerhet, kritisk infrastruktur og organisasjonsendringer

Denne rapporten er en del av prosjektet Critical infrastructures, public sector reorganization and societal safety (CISS). Prosjektet springer ut fra et sett med forutsetninger:

- Et moderne samfunns sikkerhet er avhengig av at kritiske infrastrukturer er svært pålitelige. Dette har blant annet blitt slått fast av Willoch-utvalget og Infrastrukturutvalget. (NOU 2000:24; NOU 2006:6)

- Deregulering og NPM-inspirerte endringer medfører grunnleggende endringer i organisasjonsform i flere infrastruktursektorene.

- De fleste skoler innenfor sikkerhetsforskningen anerkjenner i dag en tett sammenheng mellom organisatoriske forhold og sikkerhet (e.g. Perrow

1984; La Porte og Consolini 1991; Roberts et al. 1993). En kan derfor forvente en endring av sårbarhetsbildet.

- Flere sikkerhetsforskere (de Brunije 2006;de Brujine og van Eeten 2007; Schulman og Roe, 2007)[4] har gitt uttrykk for at de endringene en deregulering normalt innebærer introduserer bærer med seg potensielle sårbarheter. Disse kan svært grovt grupperes på følgende måte.

    - Målkonflikter: Ved en privatisering eller privat-lignende organisering, vil man kunne oppleve at effektivitet går på bekostning av redundans og sikkerhet. Dette er en klassisk kritikk av NPM som ofte også er et tema i politisk debatt.

    - Fragmenteringseffekter: Tidligere integrerte organisasjoner deles opp i flere enheter og man får forretningsgrensesnitt mellom organisasjoner som opererer tett koblede systemer. Disse oppdelingene kan gi utfordringer med kommunikasjon og koordinering.

Disse punktene har vi tatt for oss i to tidligere publiserte rapporter (Almklov et al. 2008, 2010). Det er viktig å understreke at når vi i et prosjekt som dette er opptatt av nye sårbarheter, så kan de samme endringene også har positive sider når det gjelder sikkerhet. Sikkerhetsforskeres er opptatt av hva som kan gå galt, og vårt prosjekt springer ut av bekymringene som lanseres av sentrale forskere internasjonalt i titler som stiller spørsmål ved om New Public management er å anse som "a recipe for disaster" (Hood og Jackson, 1992) og om deregulerte kritiske infrastrukturer er "systems that should have failed" (de Bruijne og van Eeten, 2007).

Det er flere organisatoriske forhold som har stor betydning for beredskap, som klare ansvarsforhold og kommandolinjer. En organisatorisk egenskap med betydning for beredskap som kan utfordres av de organisasjonsformene man normalt knytter til NPM er graden av redundans, både personell- og kompetansemessig, at man har ekstra folk å sette inn og gjerne at man har ansatte med overlappende kompetanseområder. I beredskapssituasjoner faller ofte faste strukturer bort og en utfordring blir da å organisere seg mer dynamisk ved gjensidig tilpasning. Evnen til å skifte koordineringsmodus fra i det ene øyeblikk å lene seg på standardisering og formelle strukturer, til i det neste øyeblikk å koordinere innsatser mer uformelt og dynamisk er en nøkkelegenskap i mange kritiske situasjoner.

For å gripe tak i disse problemstillingene designet vi CISS som en komparativ studie hvor vi sammenligner tre infrastrukturer. Vi valgte også å studere problemstillingene på et intraorganisatorisk nivå. Det vil si at vi ikke har sett så mye på politiske, juri-

[4] For en oversikt over litteraturen se Antonsen et al (2010).

diske, statsvitenskaplige og reguleringstekniske problemstillinger. Disse er meget relevante i seg selv, og bør absolutt følges opp av de som har sin kjernekompetanse innenfor de feltene.[5] Vårt prosjekt er i større grad fokusert de intraorganisatoriske konsekvensene av nye organisasjonsformer og hva dette har å si for sikkerheten.

CISS tok i første case for seg dereguleringen av den norske el-nett bransjen, og så på hvordan bruk av bestiller-utfører-modell (BUM) og outsourcing i driften av strømnettet endret på sikkerhetsrelevante organisatoriske forhold. Vi gjorde intervjurunder på alle nivåer i to nettselskaper. Selv om vi gjorde observasjoner i denne studien som bekreftet hovedprinsippene i de "teoretiske" bekymringene som er diskutert over, var hovedinntrykket at driften fra dag til dag ikke var svekket. Grovt oppsummert så vi en formalisering av arbeidsprosessen i drift, og av relasjonene mellom de som arbeidet hos bestiller og utfører. Dette innebærer en sikkerhetsmessig styrking på noen områder, men også distinkte svakheter. Vi så også tegn på at effektiviseringen som endringene innebar har ført til svært slanke organisasjoner, noe som kan gi spesielle utfordringer i forbindelse med hendelser som er svært personellkrevende. I studien av vannforsyning så vi på bestiller-utfører modell i to kommuner. Der var ikke slike målkonflikter noe aktuelt problem, noe som bl.a. henger sammen med at bransjen er selvkostfinansiert. Dette caset demonstrerte også tydelig hvordan NPM medfører endrede grensesnitt og koordineringsmekanismer, og det gjorde oss spesielt oppmerksomme på en del interessante og potensielt uheldige effekter som kan inntre i overgangsfasen mellom modeller.

3. Om caset: Drift av IKT-infrastruktur på St. Olavs Hospital

IKT organiseringen ved St. Olavs Hospital pr i dag

I dette avsnittet vil vi gi en overordnet beskrivelse av organiseringen av IKT-driften ved St. Olav. Vi vil utdype de mest relevante punktene i forbindelse med observasjoner og analyse.

IKT-avdelingen på St. Olavs Hospital består av to personer, IKT-sjef og hans nestkommanderende. Den er en rendyrket bestillerenhet som selv ikke har utførende funksjoner. Den sentrale utføreren i systemet er Hemit, et foretak som er eid av Helse Midt-Norge, helseforetaket som også eier St. Olavs Hospital. St. Olav bestiller driftstjenester fra Hemit i en forretningsrelasjon, der det er det er kontraktsfestede spesifikasjoner på leveransene og tjenestekvalitet og hvor tjenestene er prissatt. Selv

[5] En modell for en slik tilnærming finnes hos Rasmussen (1997)

om de altså har samme eiere og at både bestiller og utfører er offentlige foretak, er relasjonen mellom dem designet for å ligne den mellom to private aktører. En annen sentral aktør for IKT-infrastrukturen på St. Olav er EDB Business Partner ASA[6], som har en rammeavtale for drift av IKT-nettverket. Dette er et stort privat selskap med flere underselskaper og totalt 6000 ansatte. Både Hemit og EDB støtter seg også i flere sammenhenger på sine egne underleverandører. Dette er alt fra internasjonale giganter som Cisco og HP til mindre norske leverandører. Ved at Hemit har ansvar for nettilgangen på medisinteknisk utstyr har også personell med ansvar for det medisintekniske utstyret på St. Olav organisatorisk grensesnitt mot IKT-miljøene på sykehuset.[7] Også andre avdelinger under Driftsservice ved sykehuset har fått nye grensesnitt mot IKT-miljøet, gjennom at systemer de har ansvar for er koblet opp mot IKT-infrastrukturen. Dette gjelder blant annet rørpost, heisanlegg og adgangssystemer.

Driften av IKT-systemet på St. Olav er bygget opp etter ITIL-rammeverket.[8] Dette er en globalt dominerende standard[9] for drift av IKT-systemer. Den har sitt utspring i et sett av "beste praksis"-dokumentasjon for drift av IKT-systemer. I disse ligger det tydelige føringer på arbeidsprosessen og organiseringen av driftsenheten. ITIL er et organiserende system som gjennomsyrer både Hemit og EDBs arbeid. I og med at dette er en verdensomspennende standard, betyr dette også at arbeidsprosessene er standardiserte strukturelt sett og at mye av kompetansen er knyttet opp mot at man er ITIL-sertifisert for de ulike oppgaver og ansvarsområder.

Et særlig relevant punkt i ITIL i denne sammenhengen er prinsippet om at det skal være ett kontaktpunkt for all brukerstøtte. For St Olavs del betyr det at alle IKT-relaterte henvendelser (*incidents*) rettes til Hemits førstelinjetjeneste. Alle saker (som kommer pr telefon eller elektroniske meldinger) registreres og kategoriseres etter en fast mal. De som førstelinjen ikke løser selv blir så fordelt videre (i det elektroniske saksbehandlingssystemet) i Hemits kjede, til andrelinje til spesialister på de ulike delsystemer. Man har altså en standardisert arbeidsprosess der enkle saker blir løst langt fremme i kjeden, mens mer kompliserte saker, *problems*, blir håndtert av spesialister. I denne organiseringen inngår også endringsprosesser som egen arbeidsflyt. Saker som angår EDBs ansvarsområde blir på tilsvarende vis meldt inn til Hemits førstelinje og oversendt EDB elektronisk derfra. Kontaktflaten som førstelinjen utgjør er essensiell i den daglige relasjonen mellom den kliniske delen av St. Olav og IKT-miljøene. Det at Hemit i prinsippet er en ekstern organisasjon og at den benytter ITIL-standarden, har medført en sterk strukturering av den daglige

[6] Omtales i det følgende som EDB.
[7] Vi intervjuet ikke noen fra disse miljøene for denne rapporten.
[8] For en beskrivelse av ITIL se for eksempel Rudd (2004). Wikipedia har også en utmerket artikkel om temaet: http://en.wikipedia.org/wiki/ITIL
[9] ITIL er ikke i seg selv en standard, men danner grunnlaget for ISO-sertifisering.

samhandlingen mellom brukerne på St Olav og IKT-driftsmiljøet. Endringer og oppgraderinger av IKT-systemene går gjennom en ITIL-spesifisert *change*-prosess. Et sentralt formål med denne er å strukturere og kvalitetssikre endringsprosessene, både internt i IKT-systemene og også opp mot brukerne. Til det siste formålet er *Change advisory board* en sentral institusjon. I dette utvalget er sykehuset representert og det har ansvar for å godkjenne foreslåtte endringer. Selv om *change* prosessen først og fremst foregår internt i IKT-miljøene, innebærer den også rutiner for kontakt mellom sykehuset og IKT-miljøene, og diskusjoner hvor sikkerhet og robusthet ved endringene er en viktig del.

St. Olavs Hospital har de siste årene gjennomgått store endringer i forbindelse med overgangen til nye sykehusbygg og en ny driftsmodell. Det store hovedbygget har gradvis blitt forlatt ettersom nye avdelinger har blitt etablert med egne nybygg. Dette utbyggingsprosjektet er dypt innvevd i denne rapportens tematikk, fordi prosjektorganisasjonen som står bak det nye sykehuset også har hatt en tydelig IKT-profil og valgt løsninger som helt klart har betydning for drift, pålitelighet og beredskap.

Tidligere hendelser

St. Olavs Hospital har de siste årene opplevd to alvorlige hendelser knyttet til bortfall av kritiske IKT-tjenester, henholdsvis i 2006 og 2009.

I juni 2006 falt IKT-nettverket bort i den delen av området som da var benevnt som ”nytt sykehus”. Dette omfatter laboratoriesenteret, kvinne-/barnsenteret, nevrosenteret og pasienthotellet. Det ble slått katastrofealarm ettersom alle nettverksbaserte funksjoner i nytt sykehus var ute av funksjon. Dette innebar bortfall av kritiske systemer som telefoni, e-post, utskriftsmuligheter, journalsystemer, bildediagnostikk og laboratoriesystemer. Nødnummeret 113 virket eksternt, men ikke for anrop fra avdelingene som hadde flyttet til det nye sykehuset. Kommunikasjonen ble ført over på manuelle (kurértjenester) og alternative (personlige mobiltelefoner) kanaler, samt melding over høyttalere tilknyttet brannvarslingsanlegget. Bortfallet varte fra kl. 18:30 den 19. juni til kl. 22:00 den 20. juni. Det ble meldt om seks forhold med potensielt alvorlige konsekvenser for pasienter. Disse var blant annet knyttet til manglende kontakt med vakthavende leger, bortfall av kommunikasjon med laboratorieenhet, porttelefoner ute av funksjon, samt manglende tilgang på arkivsystemer i blodbanken. I tillegg ble det rapportert om en rekke tilfeller med utsatte operasjoner, samt forsinkelser og forskyvninger i diagnostikk- og behandlingslister. Bortfallet ble utløst av en feil i programvaren i nettverkskomponenter levert av en internasjonal produsent.

I september 2009 skjedde det nok en hendelse som medførte at IKT-nettverket var utilgjengelig, denne gang i en drøy time. Det var problemer tilknyttet IP-telefoni i om lag 6 timer. Det ble, så vidt vi har fått opplyst, ikke rapportert om noen hendelser med potensielt alvorlig konsekvenser for pasienter. Nettverket fungerte i prinsippet, men på grunn av en feil tilknyttet printservere ble nettverket overbelastet med svært høy datatrafikk. Feilen ble utløst av en programvareoppdatering utført av personell fra Canon.

Disse hendelsene illustrerer den økte kritikaliteten IKT-infrastrukturer har fått i moderne sykehus. Denne økningen i kritikaliteten innebærer at St. Olavs Hospital, på linje med andre større sykehus, blir mer sårbar for interne beredskapshendelser. Det er også viktig å merke seg at eksterne parter (Canon og Cisco) hadde betydning som utløsende faktor, og at eksterne eksperter også bidro med ressurser og kompetanse i problemløsningen.

4. Metode

Vi gjorde totalt 11 intervjuer med 16 informanter. Informantene ble valgt for å kunne belyse grensesnittene mellom kliniske miljøer ved St. Olav og driftsavdelingene ved Hemit og EDB.[10] I tillegg til at vi har snakket med folk som arbeider i klinikk (sykepleiere/leger) og personell som arbeider med IKT-drift til daglig, har vi snakket med nøkkelpersonell med viktige roller eller særlig kompetanse. Et så lite og så bredt sammensatt utvalg kan ikke være representativt, og informantene er valgt på basis av hvorvidt vi tror de kan gi oss innsikt i og ulike perspektiver på problemstillingen. Undersøkelsen er dermed å betrakte som utforskende, mer enn noe som kan levere representative eller kvantifiserbare funn. På den andre siden er intervjuer som dette en velegnet måte å samle inn og systematisere ekspertbetraktninger fra informantene noe som har en stor egenverdi i seg selv om de behandles kritisk.

Denne typen undersøkelser er velegnet til å identifisere *mulige* sårbarheter. Om man ønsker mer robust beslutningsunderlag, for eksempel til å iverksette endringer, anbefales det en undersøkelse som er mer målrettet tematisk og bredere i informantsammensetningen.

Vi har gjort semi-strukturerte forskningsintervjuer med en varighet på en time. Temaer har naturlig nok variert etter informantens oppgaver, kompetanse og interesser. De viktigste punktene er oppsummert i Tabell 1.

[10] Dessverre fikk vi bare gjort ett intervju hos EDB. Vi fikk dermed ikke adgang til erfaringer og refleksjoner blant det driftspersonellet som er dedikert til driften på St.Olav.

Tabell 1 Temaer i intervjuguiden.

Hovedpunktene i intervjuguiden	
Om intervjuerne og forsknings-prosjektet	Bakgrunnen for intervjuene, litt om konfidensialitet etc
Om informanten	Stilling Bakgrunn Arbeidsoppgaver Relasjoner, hvem han/hun er i kontakt med til daglig
Diskusjon om grensesnitt	Avhengig av informantens ståsted snakker vi om grensesnitt mellom ulike aktører: Hemit, EDB, Klinikk, Beredskap, Driftservice, underleverandører IKT. Vi spør om hvordan kommunikasjon og koordinering foregår mellom enhetene i normal drift og beredskapssituasjoner.
IKT utvikling	Vi spør informantene om hva som har skjedd de siste årene innenfor teknologisk og organisatorisk utvikling innenfor IKT.
IKT og beredskap	Erfaring med hendelser -Spesielt de større hendelsene i 2006 og 2009. -Andre beredskapshendelser knyttet til IKT. Beredskap mot IKT hendelser -Organisering -Øvelser -Sårbarhet (hva opplever informanten er mest sårbart) IKT i andre typer hendelser

Ved siden av å spørre om informantens arbeidsdag generelt har vi særlig sett på relasjoner og grensesnitt (avhengig av ståsted) mellom Hemit, EDB, og klinikker og andre relevante avdelinger ved St. Olavs Hospital (drift, IKT, beredskap). Vi har diskutert de siste års utvikling med tanke på IKT med alle informanter, og vi har tatt opp IKT-hendelsene i 2006 og 2009 med alle som har kjennskap til disse. Vi har dessuten spurt om beredskapsproblematikk, om de øver, hvilke backupfunksjoner de har og så videre. Vi har gjengitt enkelte sitater i teksten, der vi mener at intervjuobjektenes utsagn illustrerer analysen vår.

Et annet element i vår analyse er gjennomgang av sentrale dokumenter. Vi har fått tilgang til ulike hendelsesrapporter, konsulentrapporter, planer og organisasjonsdo-

kumenter. Særlig viktige for vår analyse er beredskapsplanen for St. Olavs Hospital og dokumentasjonen fra hendelsene i 2006 og 2009.

5. Funn og Analyse

I dette kapittelet oppsummeres funnene fra intervjuer og dokumentstudier. De organisatoriske og tekniske særtrekkene ved IKT systemene og organiseringen av driften av disse ved St. Olav diskuteres løpende opp mot sikkerhets og beredskapshensyn. De fleste organisasjonsmåter har i seg potensielle svakheter som bør følges opp med tanke på å ivareta sikkerhet og beredskap. En slik gjennomgang er ikke fokusert på å gi en "rettferdig" og uttømmende analyse av systemene. I så fall måtte momenter som økonomi, effektivitet, brukervennlighet og lignende tas med i et helhetlig bilde samme med sikkerhets- og robusthetshensyn. I stedet fokuseres det her, relativt uavhengig av slike betraktninger, på å identifisere og diskutere reelle og potensielle svakheter i dagens situasjon.

Sykehusets avhengighet av IKT introduserer nye sårbarheter

Om vi hadde sett på helsesektoren for 10-15 år siden ville et IKT-bortfall hatt en relativt liten betydning sammenlignet med i dag. Telefoner var selvsagt viktige da som nå, men sykehuset var i mindre grad avhengige av datanettet. Noen systemer og funksjoner ville nok blitt rammet av et databortfall, men sammenlignet med dagens situasjon var IKT da ikke en spesielt kritisk infrastruktur i helsesektoren. Det har i denne perioden vært en sterk utvikling i retning av at kritikaliteten til IKT øker i helsesektoren. Dette gjelder i stor grad det nye St. Olavs Hospital som ligger i forkant i en del nye løsninger. Denne utviklingen ble beskrevet slik av en av de vi intervjuet:

> *"Altså IKT, på generelt grunnlag så er IKT mye tettere innvevd i kjernevirksomheten, altså diagnostikk behandling og til dels pleie av pasienter. Du har systemer som i mye større grad innvirker direkte på pasientdiagnostikk og behandling. Det er klart det tilfører en annen form for sårbarhet og et annet risikobilde enn det vi hadde før."*

Noe av den økte kritikaliteten skyldes at IKT er tettere innvevd i de kliniske arbeidet. Spesielt viktig i så måte er at pasientjournalene nå er elektroniske og at for eksempel prøvesvar og bilder formidles elektronisk. I tillegg er svært mange driftstekniske støttefunksjoner i det nye sykehuset nå knyttet opp mot IKT-nettet, roboter

som transporterer varer, matbestilling, heiser, dører, porttelefoner og adgangssystemer. IKT-infrastrukturene er også blitt tettere koblet i seg selv, for eksempel i det at telefoner og meldingssystemer er databaserte og dermed sårbare for feil som rammer IKT-nettverket.

Særegenheter ved IKT som infrastruktur

I dette avsnittet kommenterer vi noen kjennetegn og utviklingstrekk for IKT som infrastruktur som har betydning for dens robusthet og hvordan ulike organisasjonsmodeller fungerer.

En kritisk infrastruktur kjennetegnes ved at dens bortfall får store samfunnsmessige konsekvenser. Flere viktige infrastrukturer er også det man kan kalle naturlige monopoler. Det vil si at kostnadene av å opprette et konkurrerende system er så store at de i praksis stenger ute andre aktører. Den typiske illustrasjonen på dette er å se for seg etableringen av et konkurrerende strømnett eller en konkurrerende vannforsyning, noe som i de fleste tilfeller er helt urealistisk. Det at infrastrukturer er monopoler, forsterker ofte deres kritikalitet. For noen tiår siden var telefon og elektronisk kommunikasjon også preget av slike monopoltilstander, men den teknologiske utviklingen har medført en økende multiplisitet i IKT-sektoren, og det er flere overlappende kanaler som kan dekke mange av de samme behovene. Det er et stort antall parallelle og konkurrerende kanaler, slik at de mest kritiske informasjonsbehovene kan dekkes for de fleste brukere. Et sykehus har til en viss grad den samme muligheten til å operere i flere kanaler, men har samtidig et større behov for informasjonskontroll og lukking av systemene, spesielt på grunn av datasikkerhet. Dette medfører i en større grad at muligheten til å bruke flere infrastrukturer begrenses og at mye informasjon må holdes innen en kjerneinfrastruktur. I prosjektet "Nytt Sykehus" har det også blitt gjort flere valg som har rendyrket IKT-infrastrukturen i det nye St. Olavs Hospital rundt én kjerne, fra en hovedleverandør.[11] Sånn sett er det en viss rimelighet i å se IKT-infrastrukturen på et sykehus som sammenlignbart med de naturlige monopolene. Det er likevel klare kjennetegn ved teknologien som skiller seg klart fra de mer klassiske infrastrukturene.

Nesten uansett hvor mye man lukker systemene, vil IKT-infrastrukturer ha koblinger utad. Det betyr at det er vanskelig å avgrense dem mot at ytre endringer og handlinger kan påvirke dem. De to beredskapshendelsene beskrevet i kapittel 3 kan bidra til å illustrere dette. I 2006 så man hvordan en liten tidligere ukjent programvarefeil i en server levert fra et anerkjent multinasjonalt selskap interagerte med andre syste-

[11] Selv om man har infrastruktur fra en leverandør, betyr ikke dette at systemet ikke er redundant. Det er bygget inn flere nivåer med redundans og multiplisitet i systemet i seg selv med ekstraservere og backup-systemer og så videre.

mer på sykehuset og bidro til å utløse et kaskaderende sammenbrudd. Hendelser kan altså utløses av forhold langt utenfor driftsorganisasjonens rekkevidde. Samtidig er det en positiv side ved dette som man har sett ved beredskapshendelsene. De fleste feil i IKT er programvarerelaterte og kan håndteres uten fysisk tilstedeværelse. Dette kombinert med en utbredt standardisering av komponenter og prosesser (for eksempel ITIL se side 5) gjør at man ved hendelser, fort kan involvere eksterne ressurser i problemløsningen. I sikkerhetsforskningen er "tette koblinger", et svært viktig tema (se Perrow, 1984). Tette koblinger bærer i seg et potensial for uoversiktelige og kaskaderende hendelser der en lokal feil kan ha uforutsette konsekvenser over store distanser. IKT er både en infrastruktur som i seg selv er svært tett koblet, og som også formidler koblinger mellom andre systemer. Det å ha oversikt over mulige sammenhenger er derfor en stor utfordring (ibid.).

Det er en åpenhet i teknologien som medfører at mye av risikoen for feil (og potensialet for feilløsning) ligger utenfor driftsorganisasjonen. Strukturen i både maskinvare og programvare medfører at en organisasjon ikke kan gjøre alt selv, men at den vil være avhengig av en rekke underleverandører. Dette er også nøkkelpersonell på sykehuset klar over:

> *"[…] ikke sant du har begrenset mulighet til å påvirke organiseringen fra Hemit og utover da. Disse underleverandørfirmaene de kjøpes og selges og omsettes og kompetansen den flyter litt frem og tilbake og den har vi ikke kontroll på. Det tror jeg vi må innse."*

Dermed vil også risikohåndtering og beredskapsarbeid handle om å ha oversikt over leveransene av kritiske komponenter og oppgaver. Debatten om tjenesteutsetting og om man skal holde alt innomhus for å ha kontroll har i IKTs tilfelle blitt utdatert, og det det handler om i en sikkerhets- og beredskapssammenheng er hvordan bestilleren skal sørge for å ha den nødvendige kontrollen over sine leverandører.

Et annet kjennetegn ved IKT er at *bruken* av leveransen ikke er uproblematisk. Brukerfeil er en potensiell årsak til feil og problemer i seg selv. I tillegg utgjør de også et problem for de som skal drive feildiagnostikk, siden de ofte må avklare om det er feil med systemet eller brukeren som gjør noe galt.[12]

IKT-systemene kjennetegnes også ved en høy utskiftningstakt på komponenter (spesielt sammenlignet med andre infrastrukturer) og en høy grad av standardisering av tekniske komponenter. Dette betyr at personell som arbeider med infrastrukturen ikke nødvendigvis trenger stor erfaring med de tekniske systemene på St. Olav spe-

[12] I motsetning vil en som jobber med vannforsyning kunne være rimelig trygg på at det er noe galt med vannforsyningen, hvis en bruker ringer inn og sier at det ikke er vann i krana.

sifikt, men at de i mange tilfeller kommer langt med en generell IKT-kompetanse. Mens man i andre infrastrukturbransjer ser store kompetansemessige fordeler ved å ha erfaring med og kjenne gamle komponenter og deres særegenheter, gjør den raske teknologiske utskiftningstakten at det er like viktig å være orienter mot framtiden som mot den tekniske driftshistorikken. Det som likevel skiller seg ut som et spesielt krevende kompetansebehov hos IKT-leverandørene, er det å forstå og kunne håndtere de spesifikke behovene som helsesektoren har:

> *"Det er det som er utfordringen. Det er vel det som er vanskelig å lære seg. Å vite hvor kritisk er et medisinsk system. Hva er konsekvensen hvis det her ikke fungerer."*

> *"Det kan være hvordan de ordlegger seg når de har problemer ute på huset. Noe så enkelt som å sikre at det faktisk er det problemet som brukeren melder til meg. Altså, at jeg forstår det. […] Og kanskje også forståelsen av hvor alvorlig ting kan være. Og så høres det helt banalt ut for, egentlig IT-teknisk sett. Det kan være noe så enkelt som en mal som ikke virker. […] Hvorfor haster det så galt? Men da lammer du dem så ille."*

De medisinske/helsemessige konsekvensene av feil og brudd trenger ikke være proporsjonal med størrelsen på problemet rent IKT-teknisk, og kunnskapen om dette og rutinene for å forholde seg til det, er en distinkt utfordring for IKT-leverandørene på et sykehus. Systemene forholder seg også til tungt forankrede arbeidsmåter i de medisinskfaglige miljøene som ikke er lette å endre på.

Outsourcing, kontroll og koordinering

IKT-systemer er ikke så avgrensede og lokalt forankret som for eksempel vannforsynings-infrastrukturer som vi har sett på tidligere. Der er det i stor grad mulig å gjøre det meste av arbeidet med egne folk, og kun kjøpet utstyr eksternt. Det vi derimot ser her er at det er nærmest umulig å se for seg en IKT-infrastruktur av St Olavs størrelse og kompleksitet som ikke i stor grad må støtte seg på innleide ressurser i form av personell og kapasiteter. En ting er at mye av driften leveres av EDB, men både de og Hemit er også avhengige av flere underleverandører som bidrar med sine spesialkapasiteter. Disse kan være store multinasjonale selskaper som Cisco, Canon, HP og Immatis, men også mindre lokale selskaper.

Dette gjør at leverandørkjedene innenfor IKT-sektoren fort kan bli lange og uoversiktlige. På St. Olav har man vært bevisst på viktigheten av at leverandørene forstår kritikaliteten i de tjenestene de leverer. I de tilfellene hvor leverandørene setter ut deler av arbeidet til underleverandører er det imidlertid mer uklart hvordan kritikali-

teten i leveransen formidles videre til disse. Siden det ikke har blitt gjort intervjuer hos underleverandører, gir ikke kartleggingen som er gjort i dette prosjektet grunnlag for å trekke noen slutninger rundt dette, men det har heller ikke framstått som et tema som blir systematisk oppfulgt. Som nevnt er sykehuset imidlertid bevisst dette forholdet, og en vi intervjuet uttrykte bekymringen på denne måten:

> *"[…] altså du kan fortelle det [at følgene av brudd kan være dramatiske] til folk. Men hva det faktisk betyr altså, overfor et kuvøsebarn eller en person som ligger på operasjonsstua eller som er avhengig av å ha et røntgenbilde eller annen bildediagnostikk opp på skjermen for å gjøre en guidet undersøkelse, angiografisk av hjernen eller hjertet ikke sant, altså hvis det der går i svart, midt under en sånn en, så er det jo en kjempekrise. Det vil med en gang kunne påvirke liv eller død eller kritiske tap av helse for enkeltpasienter. Og det å få en bevissthet om det, som følger kontraktsprosessen og endringsprosessen ute hos leverandører og underleverandører. Det er tøft å få til det altså."*

Det at flere leverandører (og underleverandører) blir involvert i driften av tjenester og infrastruktur skaper et økt behov for koordinering mellom de ulike leverandørene. Dette gjelder i første rekke EDB og Hemit, hvor det har vært eksempler på at koordineringen dem i mellom skaper problemer for tjenestene til St. Olav. For eksempel har man ved ett tilfelle opplevd at håndteringen av en driftsforstyrrelse ble mer komplisert enn nødvendig fordi Hemit ikke hadde fått med seg nødvendige tilganger etter at de overtok et system fra EDB. Resultatet ble at Hemit-ansatte ble avhengige av EDB-personell for tilgang til systemet under håndteringen av hendelsen. Slik sett gjør tjenesteutsetting og organisatorisk fragmentering at de som drifter systemet blir mer avhengig av prosesser som ligger utenfor organisasjonens grenser, og som en dermed har begrenset kontroll over og innsyn i. På dette området kan imidlertid ITIL-standarder fungere som mekanisme for koordinering og kontroll gjennom å gi rutiner for kommunikasjon, beredskap og hendelseshåndtering.

For å opprettholde kontroll over kritiske tjenester har en på St. Olav valgt å ikke tjenesteutsette brukernære tjenester. Dette gjelder for eksempel elektronisk pasientjournal, pasientadministrasjon og laboratoriedata. Disse tjenestene driftes av Hemit. Imidlertid illustrerer særlig hendelsen fra 2009 at de tette koblingene mellom systemene gjør at skillet mellom brukernære og brukerperifere tjenester blir noe kunstig. Når systemene henger så tett sammen og er avhengige av mye av den samme infrastrukturen, vil hendelser i brukerperifere tjenester kunne påvirke mer sentrale tjenester.

Selv om mye av det de gjør er normal drift av IT-systemer, ligger Hemits spesialitet nettopp i kompetanse på helse. Ved den sterkt standardiserte organisasjonsformen og den potensielle utbyttbarheten som ligger i en markedsbasert organisasjonsform, er Hemits posisjon som en intern-ekstern leverandør i stor grad forklart og legitimert ved deres langsiktige relasjon med St. Olav. I våre studier av andre bransjer har vi også sett at det er deler av arbeidet som er vanskelig å tjenesteutsette, fordi at det har en historie som har gitt langsiktig kompetanseutvikling (Almklov et al., 2008, 2010). I de andre bransjene har dette handlet om den ikke dokumenterte erfaringen som kommer fra å drifte et gammelt og heterogent teknisk system over tid. Det kan synes som at det er en parallell her, men at denne relasjonen handler om det å ha erfaring med et sykehus og dets særtrekk og utfordringer. Det er noe motsetningsfylt i at St Olavs Hospital benytter en intern IKT-leverandør på de brukernære systemer, samtidig som man i stor grad rendyrker det forretningsmessige og formelle i denne relasjonen. Vi tror at denne nærheten er viktig for sikkerheten og at man arbeider for at de ansatte der skal kjenne de spesielle sårbarhetene de ulike avdelingene på et sykehus har og de kravene som ligger i IKT-bruk på et sykehus. En generell kompetanse som dette kan trolig være en ekstra ressurs i ekstreme beredskapssituasjoner, der man kan bli tvunget til å improvisere. I slike situasjoner er kompetanse også utover eget fagfelt essensielt.[13] Selv om organisasjonen rendyrker en forretningsmessig og formell relasjon, har ikke ansatte i Hemit som vi snakket med en opplevelse at det ville vært enkelt å skifte dem ut som leverandør. De mener også at det ville vært svært utfordrende for Hemit å skulle ta over andre helseforetaks IKT-infrastruktur. Dette begrunner de i at systemet, og da spesielt koblingene opp mot sykehuset, ikke er så standardisert at ikke erfaring med dem vil være en stor fordel.

Kommunikasjon mellom brukere og IKT-miljøer

I det følgende vil vi trekke frem noen kjennetegn ved kommunikasjonen mellom de kliniske miljøene på St. Olavs Hospital og IKT-miljøene ved Hemit og EDB. Vi har lagt særlig vekt på kommunikasjon som dreier seg om IKT-systemene på sykehuset. Det er ikke lagt vekt på å beskrive intern kommunikasjon i den enkelte avdeling, men kommunikasjon mellom de kliniske miljøene og IKT-miljøene, og mellom IKT-miljøet på sykehuset og eksterne leverandører.

Måten kommunikasjon rundt IKT foregår på sykehuset, er karakterisert av en strukturert form. Dette innebærer bruk av samarbeidsteknologi i forhold til ekstern kontakt med brukere og leverandører, og kategorisering og oversetting av denne kom-

[13] Mens driften av IKT systemet stort sett vil kunne sies å ha standardisering som primær koordineringsmekanisme, vil en beredskapssituasjon i større grad kreve gjensidig tilpasning mellom ulike aktører Mintzberg (1983).

munikasjonen til informasjonspakker som kan sendes videre i en elektronisk dokumentflyt. Den strukturerte måten å kommunisere på støttes opp av en prosessorientert arbeidsmåte beskrevet i ITIL[14]. Hemit er sentral i all kommunikasjon rundt IKT-systemene siden de har rollen som 1. linje for alle henvendelser både fra brukere og fra eksterne leverandører. Feil og problemer fra brukere kategoriseres med hensyn på et sett av standardkategorier som alvorlighetsgrad, antall rammede brukere, feiltype, system og så videre. Sakene løses enten direkte hos førstelinjen eller de utløser så en strukturert saksbehandlingsprosess avhengig av hvordan den har blitt kategorisert. I tillegg er Hemit sentrale i mange henvendelser som driftsmiljøet på sykehuset får, gjennom at mange av systemene som drift har ansvar for også har grensesnitt mot IKT-systemene.

En slik strukturert form for kommunikasjon har sine klare fordeler gjennom at en blant annet kan bygge opp en solid driftshistorikk på utfordringer og løsninger, uten at historikken er knyttet til enkeltpersoner i organisasjonen. Det er en stor verdi for det IKT-tekniske miljøet at de med denne formen for strukturert kommunikasjon, selv kan legge opp rutiner i forhold til hvem i deres enhet som skal være adressat på de utfordringer som brukerne kommer med. Dette kan være grunnlag for lettere å avgjøre prioriteringer rundt tilgjengelige interne ressurser, og vil også gjøre det synlig når det trengs en intern koordinering for å kunne løse problemene. Når det gjelder organisasjonens risikosensitivitet er strukturert kommunikasjon spesielt positivt med tanke på muligheten til å arbeide systematisk med feil, ha en veldokumentert oversikt over hvilke systemer som svikter og gir brukerne problemer. Ved at Hemit sitter på så pass mye dokumentasjon, gjør også at de kan gjøre tyngre analyser og oppdage mer "skjulte" problemer. De ansatte vi snakket med i Hemit la vekt på at de var lojale mot denne kommunikasjonsformen, og at de ikke ønsket kommunikasjon med brukere over i uformelle kanaler. På spørsmål om klinisk personell forsøkte å gå utenom kommunikasjonslinjen, svarte en:

> *"Nei, det gjør de ikke. Det er enkelte som prøver seg, når jeg snakker med dem, når jeg ringer opp og slikt. Men i og med at jeg vet det at hvis jeg hadde begynt med det [dele ut direktenummer], så hadde jeg ikke rukket og gjort jobben min, egentlig. Jeg hadde i hvert fall ikke fått ro til å gjøre jobben."*

Også brukerne vi har snakket med ser fordelene, og er i stor grad fornøyd med ett sentralt punkt for kontakt angående IKT relaterte utfordringer.

---

[14] Selv om ITIL i seg selv ikke forutsetter outsourcing/BUM, er det rimelig å knytte slike modeller til NPM. Våre beskrivelser av modularisering som organisasjonsprinsipp i NPM og hvilke konsekvenser det har for en del sikkerhetskritiske forhold har er også relevante for ITIL som modell, uavhengig av om det benyttes internhandel i organiseringen (Almklov og Antonsen, 2010).

En utfordring med den strukturerte kommunikasjonsformen er at brukerne ikke vil kunne ta kontakt direkte med eksterne aktører som kan løse problemer umiddelbart. Siden kommunikasjon med eksterne skal foregå gjennom Hemit sin 1. linje, er brukerne nødt til å formulere problemet slik at Hemit blir i stand til å forklare problemet for den eksterne aktøren.

> *"[…] vi sender ikke ut en mann som på en måte skal fikse et problem som han ikke vet hva er. Så vi har retningslinjer på hva som må være med. Altså, vi må ha en feilmelding, vi må ha et PC-nummer, vi må ha en kontaktperson, et telefonnummer et cetera. Så de er nødt til å bidra før vi kan hjelpe dem videre."*

Brukerne av IKT-systemene på sykehuset vi har snakket med opplever at denne "ekstrarunden" enkelte ganger kan oppleves som unødvendig. Dette gjelder særlig i de tilfellene hvor det er snakk om kjente feil, hvor en vet hvem som sitter på løsningen på problemet. I intervjuer har brukere fortalt at det på enkelte gjentagende problemer med IT-systemene har blitt benyttet løsninger som går utenom "tjenestevei":

"[…] her sitter man hands on, man kjenner systemet, man vet hvilke problemer er det, og man har stort sett hvert borti det meste av utfordringer, så skal man beskrive det for Hemit, som igjen skal tolke det til en leverandør, som har behov for ekstraopplysninger […] og så tar det utrolig lang tid. Og så blir det mye lettere og kjappere å bare ta den direktekontakten."

Dette kan i første omgang være et problem for lojaliteten til kommunikasjonsformen, og vil siden det her er snakk om veldokumenterte utfordringer, i mindre grad være en utfordring for evne til å løse sikkerhetskritiske utfordringer. Generelt må selv gode rapporteringssystemer og rutiner kontinuerlig følges opp, for å unngå at det utvikles uheldige bruksmåter og snarveier.

Det ligger også en utfordring i å sikre at problemet får den riktige prioriteringen ved at brukerne i utgangspunktet kan ha vansker med å beskrive et problem på et system de ikke har oversikt eller kjennskap til. Det er mulig å se for seg at nye og uvanlige feiltyper kan bli feilkategorisert eller falle utenfor de systemene og saksflyten man har. Problemer som er mer intrikate og vanskeligere å dokumentere kan, enten på grunn av svakheter i dokumenteringssystemet i seg selv, på grunn av feil hos 1. linjeansatte, på grunn av kommunikasjonssvikt i grenseflaten opp mot klinikken eller 2. linjen (evt videre i linjen eller mot EDB), ikke resultere i de nødvendige aksjoner. En av de vi intervjuet beskrev utfordringen slik:

"Enhver person som ringer inn og har et problem, vil si at det er kritisk. […] Så du kan bli litt sånn immun når en person sier sånt som at det her er veldig kritisk."

En slik organisasjonsmodell forutsetter en så stor grad av standardisering av informasjonsflyten at det vil være en løpende oppgave å ivareta den multiplisiteten som kreves for at organisasjonen skal ha høy risikosensitivitet for hendelser som er unike og annerledes og vanskelig å se for seg på forhånd.[15]

Internt i første og andre linje på Hemit har de selv utviklet flere kommunikasjonskanaler for å støtte hverandre og som referansegrunnlag for feilsøking. Blant annet har de meldingssystemer som er relativt løse i formen for å dele erfaringer og holde hverandre oppdatert. De vi snakket med virket veldig fornøyde med disse systemene, og vi tror det at det er systemer som er kommet litt nedenifra og opp, gjør dem velegnede til dannelsen av et sterkt praksisfelleskap og god erfaringsutveksling i 1. og 2. linjen.

Det at førstelinjen, inngangspunktet til systemet, er en typisk rekrutteringsposisjon der mange av de ferskeste ansatte i Hemit sitter, forsterker noe av sårbarheten, og gjør at den interne kommunikasjonen og støtten i førstelinjen er svært viktig for å unngå at problemer ikke fanges opp. I intervjuene med ledere og ansatte i Hemit ble gjennomtrekk av personell i 1. linjen trukket fram som en trussel i forhold enhetens kunnskap om de medisinske miljøene:

"[om utskiftning av folk] Det er jo kritisk i forhold til evnen til å se store feil da. Kunne sette riktig kritikalitet på sakene. For det krever jo en viss erfaring. Det er jo det en får med erfaringen da. Det her er ekstremt viktig for sykehuset. Det må opp igjen om tjue minutter."

Denne kunnskapen er sett på som viktig for å kunne forstå kritikaliteten i feilmeldinger fra det kliniske miljøet og med dette ha høy risikosensitivitet.

At brukere i noen tilfeller ønsker å gå utenom de formelle kommunikasjonslinjene vil være en utfordring for lojaliteten til kommunikasjonsformen en har valgt å bruke. Dersom de formelle kommunikasjonslinjene ikke blir brukt, kan dette svekke evnen til å oppfatte svake feilsignaler gjennom at informasjon om feil spres mellom flere

[15] Weick (2004) og Nævestad (2009) er blant flere forskere som trekker fram variasjon i forståelsesformer og kommunikasjon som en ressurs for økt risikosensitivitet. Brizon og Wybo (2009) viser til en type hendelser som ofte faller utenfor de vanlige systemene for å oppfatte at noe galt er i gjære. Deres eksempel er hvordan en hetebølge i Frankrike medførte en svært høy dødelighet blant eldre, men at en del menneskelige og institusjonelle faktorer medførte at det gikk svært lang tid før krisen ble "oppdaget". Denne hendelsen er grundigere beskrevet i Poumadère et al (2005).

aktører. Dette vil på sin side kunne føre til at det tar lengre tid å identifisere feil og eventuelt sette sykehuset i en beredskapstilstand. Det må imidlertid understrekes at dette i utgangspunktet er en hypotetisk problemstilling, ettersom de formelle kommunikasjonslinjene per i dag ser ut til å fungere godt.

For Hemit sin del består en sentral del av kommunikasjonen med brukere i å informere om planlagte og uforutsette hendelser som angår IT-systemene. For at dette skal kunne gjøres, er Hemit avhengig av tett kommunikasjon med eksterne leverandører og driftsmiljøet slik at de kan ha oversikt over endringer på systemene som kan få følger for regulariteten. En av de vi intervjuet beskrev dette som en utfordring de stadig jobbet med:

> *"Nei, altså. Den store utfordringen vår er å bli god på helse. Vi må jo være god på helse hvis vi skal klare å levere det brukerne krever. Og så er det det med å få all kommunikasjonsflyten til å gå smertefritt overalt mellom oss og leverandører, EDB, Telenor og alt det der."*

Sentralt i dette arbeidet er å få fram kritikaliteten som feil med systemene kan ha for de kliniske miljøene. En av de ansatte på Hemit så det som en utfordring at i tidsrommet mellom et problem ble overlevert til eksterne og en løsning ble funnet, ofte ikke inneholdt noen tilbakemelding til Hemit på hva som ble gjort, og hvor i løypa i forhold til løsning leverandøren var. Hemit ble derfor ikke i stand til å kommunisere tilbake til brukerne om tidspunkt for løsning. Selv om Hemit har kontaktpersoner hos leverandører, opplevde Hemit-ansatte at det var vanskelig å adressere riktig person hos leverandør.

Hemit har med dette flere viktige roller i kommunikasjonen av risiko rundt IKT-systemer som kritisk infrastruktur for sykehusdriften. For det første har de en sentral rolle i å informere de kliniske miljøene om risiko forbundet med vedlikehold og oppgraderinger på IT-systemene som eksterne leverandører skal gjøre. For det andre vil Hemit, i kraft av å være førstelinje for driftsproblemer, også være "first responders" i eventuelle krisesituasjoner. Dette vil si at det er de som møter eventuelle problemer først, og får ansvaret for å forstå alvoret i hendelser, gjøre innledende tiltak, samt informere videre til riktige instanser i beredskapsorganisasjonen. For det tredje har Hemit en viktig rolle i å informere eksterne leverandører om kritikaliteten i systemene, det vil si den fare for liv og helse det innebærer hvis IT-systemene på sykehuset svikter som følger av deres arbeid på systemene.

Situasjoner der Hemit ønsker å varsle brukerne av sykehusets IKT-systemer om planlagte eller ikke-planlagte irregulariteter, for eksempel begrenset kapasitet eller heng i systemene, er av enkelte informanter sett på som utfordrende. Systemene og verktøyene for varsling finnes, men krever at 1. linjepersonellet gjør "manuelle"

grep, som av noen beskrives som tidkrevende i en allerede presset situasjon. Og selv om varslingen gjøres tilfredsstillende, har Hemit ingen garanti for at brukerne kjenner til videre rutiner og responser for den aktuelle situasjonen. En god håndtering av irregulariteter fordrer gode kommunikasjonskanaler, men også en viss grad av gjensidig forståelse mellom aktørene, og dette er krevende. Gjensidig forståelse og god kommunikasjon er også nødvendig i en situasjon der IKT-systemet har redusert kapasitet. I motsetning til en situasjon med sammenbrudd, der varslingsrutiner og rutiner for respons vanligvis er klare, er en situasjon med redusert kapasitet ikke nødvendigvis forbundet med like klare rutiner. For Hemit kan det midlertidig være nødvendig å få raske og gode tilbakemeldinger på slike forstyrrelser for å kunne ta nødvendige tiltak. Tiltakene kan for eksempel måtte baseres på en avveining av hvor lenge forstyrrelsen sannsynligvis vil vare (informasjon som ligger på IKT siden) og hvilken rolle systemet spiller i arbeidsflyten i klinikken (informasjon som ligger på klinikksiden).

Gode kommunikasjonskanaler for åpen diskusjon om risiko og farer er viktig for en organisasjons sensitivitet, spesielt mot det uventede. Selv om dagens system fremstår som relativt robust, vil en slik enkeltstående kanal være en potensiell begrensing. En løpende utfordring for alt sikkerhetsarbeid er å unngå å bli for opptatt av kun kjente feiltyper, og i denne sammenhengen vil utfordringen være å sikre at både personell og systemer i denne særs viktige IKT-infrastrukturen på St. Olav evner å være sensitiv og ta aksjon om også uvanlige og uforutsett problemer skulle oppstå.

Beredskap

Infrastrukturen er sammensatt av en rekke delsystemer, med tilhørende systemleverandører. Det er altså tett koblet og komplekst, noe som gjør det vanskelig å ha full oversikt over sårbarhetene i de enkelte delsystemene og infrastrukturen som helhet. Det er omtrent umulig å ha oversikt over de mange mulige interaksjonseffektene som kan oppstå ved en feil, og feilen kan spre seg ekstremt raskt. Hendelsen i 2009 illustrerer dette: Oppdatering av en så prosaisk ting som printerdrivere medførte at datalasten ble så stor at nettet ble overbelastet i løpet av svært kort tid. Som en direkte konsekvens av dette falt nettilgangen i praksis bort for brukerne. Dette innebærer at det å holde totaloversikten over potensielle sårbarheter blir en ekstremt krevende oppgave. Ansatte i Hemit illustrerer denne kompleksiteten ved å vise til at en kundekonsulent i førstelinjen potensielt har over 400 applikasjoner som de må kjenne til at sykehuset er bruker av. Dette forholdet er ekstra komplisert ved at ansatte i Hemit opplever at brukerne av disse applikasjonene også har lav allmenn IT-kunnskap. I tillegg til å sikre en robust drift og feilretting i det daglige, er det essensielt at både teknologi og organisasjon er innstilt på å kunne håndtere større uforutsette sammenbrudd.

Klinikkene prioriterer beredskapshensynet høyt,[16] og har på eget initiativ etablert flere backup-rutiner der de forsøker å sikre uavhengig redundans på kritiske funksjoner, for eksempel gjennom papirutskrifter av essensielle data eller mobiltelefoner til nøkkelposisjoner. En av klinikerne vi snakket med begrunnet dette slik:

> *"Det er erkjennelsen av at det er såpass sårbare systemer, at vi er nødt til å ha manuelle systemer. For da går det jo på å holde oversikt over pasienter, det går på muligheter til å bestille blodprøver, det går på røntgenrekvisisjoner. Så du må ha papirsystem som går på basic i forhold til […] et minimum av opplysninger knyttet til pasient."*

Mange av disse tiltakene er imidlertid lokalt initiert. Som eksempel kan nevnes at kvinne-barn-klinikken hadde mobiltelefoner som backup i forbindelse med en hendelse, men at AMK ikke kjente til at de hadde det. De var med andre ord tilgjengelige, men AMK visste ikke at de kunne nås.

Overgangen til nytt sykehus har på noen områder medført at man har flyttet bort fra bygg som hadde gamle tekniske løsninger som fungerte som uavhengig redundans i forhold til IKT-systemene generelt (analoge telefonlinjer, calling, hustelefon etc.). Overgangen til nytt sykehus har dermed medført at en på noen områder har fått IKT-løsninger som backup for IKT-løsninger, noe som kan innebære at de er sårbare for de samme forstyrrelser. Imidlertid ble det gjort et viktig grep i å beholde personsøkersystemet, noe som betyr en uavhengig redundans til IP-telefoni. Flere av de vi intervjuet var opptatt av denne problematikken og satte ord på problemet ved å vise til hendelser der sammenvevingen av IKT og tekniske løsninger ga "praktisk plunder og heft" i arbeidshverdagen. Dette gjaldt spesielt adgangskontroll, fysisk tilgang og tilgang til IKT-systemer. Det ble i intervjuene uttrykt skepsis til denne utviklingen der organisasjonen la "alle eggene i samme kurv". Samtidig var det få som mente at slike problemer ville resultere i tap av liv. De var klare på at når situasjoner oppstod, var organisasjonen godt forberedt på å takle disse, samt at klinikkene per nå hadde backup og tilgjengelige ressurser som de kunne sette inn i en beredskap som følge av IKT-bortfall.

Like fullt kan det se ut til at hensynet til beredskap mot interne hendelser ikke har vært tilstrekkelig prioritert i overgangen til nytt sykehus. Dette trekkes frem i noen av intervjuene, og også i en tredjepartsverifikasjon av overleveringen og driften av de nye IKT-løsningene i nytt sykehus. Denne ble gjennomført i etterkant av bortfallet i 2006. Her ble det blant annet konkluderte med at de risiko-/sårbarhetsvurderingene som ble gjort av IKT-løsningene i nytt sykehus ikke var

[16] Dette kan trolig knyttes til at et sykehus i praksis er en stående beredskapsorganisasjon for eksterne hendelser.

tilfredsstillende. Dette gjaldt i tilbuds- og designfasen av prosjektet, samt i testingen av systemet før idriftssettelse (CapGemini, 2006). Om man skal styrke dette, er valg av teknologi en viktig del av bildet, men det er også essensielt at organiseringen rundt eventuelle backupløsninger er gjennomtenkt og, i den grad det er mulig, øvd på.

Den økte kritikaliteten av IKT-infrastruktur krever en litt annen type beredskapstenkning enn det en tradisjonelt har lagt vekt på ved sykehus, hvor det primært har vært fokus på større eksterne ulykker. Leveransen av IKT-systemer har mer vært det som en av informantene omtaler som en "kjellerfunksjon", i betydningen at den ligger utenfor kjernevirksomheten på sykehuset. IKT har nå blitt langt tettere innvevd i kjernevirksomheten innenfor pasientdiagnostikk og -behandling. Dette innebærer at det stilles større krav til beredskapsevnen mot de interne hendelsene. Dette krever på sin side en høy grad av kunnskap om hvordan IKT-systemene inngår i diagnostikk og behandling, god evne til å finne redundante løsninger, og en grundig beredskapsplanlegging for interne hendelser. Ingen av informantene som vi snakket med hadde vært med på en strukturert gjennomgang av denne typen problematikk, med bortfall av IKT-systemene og håndtering av sykehusdriften uten disse, eller gjennomført øvelser der dette var et scenario. Det skal imidlertidig nevnes at sykehuset og IKT-leverandørene har erfaring med flere reelle beredskapssituasjoner og hendelser og at de har endret på IKT-systemer og rutiner som følge av læring fra disse.

Sykehuset øver på å håndtere hendelser knyttet til den ytre beredskapen. Den interne beredskapen mot hendelser som nettverksbrudd blir så vidt vi kan registrere ikke øvd på. EDB har imidlertid simulert hendelser som involverer totalt nettverksbrudd. Disse har vært kjørt som "testcase" som de ansatte ikke har vært informert om og vil derfor kunne gi realistisk trening i håndtering av slike hendelser. Det har så vidt vi har fått opplyst, ikke vært gjort øvelser på bortfall av IKT-systemer som går på tvers av de organisatoriske grenseflatene mellom Hemit, EDB og St. Olavs Hospital. Både med tanke på årsakssiden og konsekvenssiden har IKT-hendelser en tendens til å strekke seg ut over den enkelte organisasjons ansvarsområde. I så måte er det grunn til å tro at det ville være stor nytte i øvelser som involverer flere aktører.

Det kan også bemerkes at katastrofeplan for håndteringen av interne beredskapshendelser, herunder svikt i teknisk infrastruktur ikke har blitt oppdatert siden 2001 og således ikke er tilpasset den IKT-infrastrukturen som ligger i de nye sykehusbyggene.

Et siste punkt som kan bemerkes rundt IKT og beredskap, er at IKT (som forkortelsen også tilsier) inkluderer systemer som berører både kritiske informasjonssystemer som inngår i pasientbehandlingen, *og* systemer som er kritiske for kommunikasjo-

nen mellom aktørene som er involvert i sykehusdriften. Når informasjonssystemer faller ut, går kommunikasjonsbehovet opp. Dersom det skulle skje feil eller bortfall av systemer knyttet til diagnostikk og behandling vil det være kritisk å kommunisere overfor brukerne, både det faktum at systemene er utilgjengelige, og hvordan en skal forholde seg til problemet. Når en samler både kritiske informasjonssystemer og primære kommunikasjonskanaler i IKT-løsninger, innebærer dette at en kan komme i situasjoner hvor behovet for kommunikasjon rundt kritiske tjenester er stort, samtidig som de primære kanalene for kommunikasjon faller bort. Nettverksbrudd av typen som inntraff i 2006 er av denne typen. Beredskapsmiljøet på sykehuset er klar over denne sårbarheten og en av de vi intervjuet beskrev dette problemet for oss på denne måten:

> *"En umiddelbar følge av at datakrafta di forsvinner er at kommunikasjonsbehovet øker. Det har vi sett ganske klart. Og når du da i samme snuppen tar bort hovedkommunikasjonskanalene også, så blir det mye armer og bein. Så konsekvensene var, må jeg vel nærmest si, vesentlig mindre i gammeldelen av sykehuset. For dem hadde fremdeles telefonien sin intakt."*

Et "worst case" scenario i denne sammenheng vil følgelig være et sammenfall i tid mellom en stor *ekstern* krise som skaper stor pasientpågang, og en *intern* krise i form av at IKT-infrastrukturen går ned. For å redusere sårbarheten mot slike situasjoner vil det være kritisk å etablere (eller videreføre) kommunikasjonskanaler som er uavhengig av IKT-systemene. Eksempler på dette kan være analoge telefonliner, personsøkere, tradisjonelle calling-anlegg eller lignende. Slike (lavteknologiske) kommunikasjonskanaler vil etter all sannsynlighet ikke være eksponert for de samme problemene som høyteknologiske systemer. Et annet interessant scenario, som vi kun forsøksvis luftet i intervjuene, er hvordan IKT-beredskapen ville fungere i en situasjon der de interne saksbehandlingssystemene hos Hemit og EDB rammes.

6. Konklusjoner

IKT-systemene som er tatt i bruk i driften av sykehuset introduserer nye og ukjente risiko, så vel som nye muligheter og økt effektivitet. Vår studie konkluderer med at disse nye risikoene kan håndteres ved bruk av standardiserte arbeidsprosesser som sammen med en globalt standardisert teknologi gir mulighet for kontroll og oversikt selv ved raske endringer og med mange ukjente utfall. Sentralt for at dette skal fungere er: lojalitet til standardiserte arbeidsprosesser fra brukere og IKT-personell; tilgang til eksterne IKT-ressurser som forstår kritikaliteten til systemene; interne IKT-ressurser som har kompetanse om det kliniske miljøet og arbeidshverdagen på

sykehuset; beredskapstenking som omfatter interne hendelser på sykehuset som vil gi redusert kapasitet til pasientbehandling.

Denne rapporten er først og fremst tenkt som et siste innspill til vårt hovedprosjekt når det gjelder NPM og de tilhørende organisasjonsmodellene der og hva det betyr for sikkerheten til IKT-infrastruktur på St. Olav. I så måte er kjennetegnene ved teknologien (og hva dette betyr for driften sammenlignet med andre infrastrukturer), hvordan driften er forankret i standarder og at man har store kjeder av relevante aktører i driften, viktig å notere seg for prosjektet som helhet.

I tillegg har rapporten tatt for seg en del temaer som er viktige for robustheten overfor brudd/feil i IKT-infrastruktur i helsesektoren. Generelt har vi et positivt inntrykk av IKT-driften på St. Olav og flertallet av de potensielle problemene vi påpeker er allerede kjent der. I så måte har en del av funnene her kanskje like stor nytteverdi for andre organisasjoner i helsesektoren.

Hovedtema for denne studien er å se på ”hvilke endringer i risikobildet kan identifiseres som følge av nye organisasjonsprinsipper i IKT-driften ved St. Olavs Hospital?” De organisatoriske endringene vi har sett på har kommet samtidig med en utvikling der IKT på kort tid har blitt langt viktigere for sykehusdriften på flere områder, både for støttefunksjoner og for det kliniske arbeidet. Overgangen til nytt sykehus har også hatt sterke effekter på våre observasjoner, både fordi det innebærer en stor endring av driften, men kanskje spesielt fordi det er en endring som innebærer en eksplisitt IKT-strategi.

I analysen har vi valgt å skille konsekvensene av disse prosessene ut som separate faktorer som kommer i tillegge til bruken av Bestiller-Utfører-Modell og tjenesteutsetting i IKT-driften. Noe dette caset viser når det gjelder hovedprosjektets generelle problemstilling, er hvordan en standardisert arbeidsprosess og en globalt standardisert teknologi går hånd i hånd. Mens det å satse på lokale krefter og egne løsninger til en viss grad er et alternativ i de andre bransjene, er IKT-bransjen global og driften er sterkt standardisert, noe som medfører et annet risikobilde og andre muligheter til å trekke på eksterne ressurser i feilretting. Kjedene av leverandører og spesialiserte underleverandører er lange i bransjen, og det er vanskelig å se for seg at andre organisasjonsprinsipper enn standardisering av delprodukter og leveranser vil være mulige å benytte i normal drift. Dette skiller seg til en viss grad fra de andre bransjene vi så på siden driften der i stor grad var en arbeidsprosess som var knyttet til det å ha kjennskap til eget anlegg og lokale særegenheter. Med så mange aktører involvert er det en løpende utfordring for bestiller (Hemit og IKT-avdeling) å ha oversikt over hvilke potensielle sårbarheter og beredskapsressurser som ligger hos eksterne partnere. Samtidig må bestiller ta ansvar for å holde sine eksterne partnere oppmerksomme på risikoen som er forbundet med de systemene de skal levere. Eksterne

leverandører må forholde seg til at bortfall av systemer ikke bare kan gi et tradisjonelt produksjonstap, men at bortfallet i verste fall kan få konsekvenser for liv og helse.

Som nevnt har kliniske miljøer på sykehuset tatt bruk av flere løsninger som skal sikre den enkelte avdeling og sykehuset som helhet større redundans i forhold til de eksisterende systemer (bruk av mobiltelefoner, kurertjenester, papirkopier av journaler). Selv om økt redundans i seg selv er positivt, har det blitt reist bekymring for at denne praksisen også medfører økt kompleksitet. I tillegg må redundans alltid veies opp mot en økonomisk vurdering, for eksempel i vurderingen av hvor mange systemer en skal fortsette å vedlikehold og investere i.

Organiseringen etter ITIL-standarden er godt forenelig med de prinsippene og det tankegodset man forbinder med NPM. ITIL manifesterer seg tydeligst gjennom at den daglige informasjonsflyten i grensesnittet mellom sykehuset og Hemit, og Hemit og deres samarbeidspartnere, er sterkt formalisert og følger en regulert saksflyt. Vi er generelt imponerte over gjennomføringen og lojaliteten til ITIL-prinsippene og det ser også ut til å fungere godt sikkerhetsmessig. Vi har likevel påpekt en del fordeler og potensielle ulemper med organiseringen. Av ulemper, lufter vi en bekymring for at en så standardisert informasjonsflyt over så viktige grensesnitt[17] kan medføre at sikkerhetskritisk informasjon kan gå tapt, pga systemfeil eller på grunn av menneskelige feil, for eksempel knyttet til feilkategorisering og lignende. Vi ser det derfor som spesielt viktig at man satser på å opprettholde kompetansen i 1. linjen til Hemit (som står for feilkategorisering), spesielt med tanke på kjennskap til sykehuset. Selv om vi ser en klar nytte i at ITIL-systemet kanaliserer informasjonsflyten på denne måten, tror vi at det kan være nyttig med arenaer for mer uformell kommunikasjon *om* systemene og om samarbeidet generelt som et supplement til dette. For å sikre at slike arenaer ikke blir rene ledelsesøvelser, bør man involvere brukere og de hos Hemit og EDB som daglig interagerer med dem. Den lojaliteten som brukere og Hemit viser til standarden er en viktig suksessfaktor for systemet. Som vi har påpekt, finnes det tilfeller der brukere går utenom det strukturerte systemet for tilbakemelding og problemløsning, gjerne begrunnet med at det er mer effektivt. Erfaringsmessig kan slike omveier være en utfordring. En konsekvens kan være at det blir dårligere historikk og kompetanse rundt kjente feil og mulige løsninger på disse. Det er derfor viktig IKT-miljøet ved sykehuset kontinuerlig jobber med å sikre lojaliteten til standarden. En suksessfaktor i så måte er å arbeide med å redusere unødig prakk og byråkrati knyttet til det, siden slike hindringer kan lede til svikt i systemlojaliteten.

[17] Vi tenker spesielt på det mellom Hemit og St. Olavs, men det samme gjelder trolig også Hemit-EDB.

Med overgangen til nytt sykehus har St. Olavs Hospital gjennomgått store endringer i den informasjons- og kommunikasjonsteknologien som inngår i sykehusdriften. Dette introduserer en endring i "blandingsforholdet" mellom det vi kan kalle intern og ekstern beredskap. Tradisjonelt har beredskapstekningen i sykehusvirksomhet vært nærmest utelukkende orientert mot å foreberede seg mot og håndtere alvorlige hendelser som skjer *utenfor* sykehuset, for eksempel pandemier, branner, store ulykker innenfor samferdsel eller andre hendelser som innebærer stor og brå økning i antallet pasienter med behov for akutt behandling. Behovet for denne beredskapen har neppe blitt mindre. Imidlertid indikerer denne studien at endringene i IKT-infrastrukturer introduserer nye risikoer som stiller økte krav til det som best kan beskrives som *intern* beredskap. Dette er hendelser som skjer *innenfor* grensene av sykehusorganisasjonen, og som kan innebære alvorlige beredskapssituasjoner gjennom å redusere evnen til sikker pasientbehandling og diagnostikk. Nettverksbrudd (for eksempel hendelsen fra 2006) er et eksempel på interne hendelser som setter sykehuset i en beredskapssituasjon. Denne studien indikerer at det interne "trusselbildet" har endret seg betydelig i takt med endringer i den informasjons- og kommunikasjonstekniske infrastrukturen, og innebærer slik sett at en må vekte opp fokuset på den interne beredskapen. Vi har i denne sammenhengen spesielt pekt på at man bør ha alternative kanaler for kommunikasjon, og rutiner for og erfaring i å benytte disse. Dette fordi krisesituasjoner utløser et behov for fleksibilitet og gjensidig tilpasning som utløser et kommunikasjonsbehov i seg selv. Videre vil det være et behov for gjentagende vurderinger med tanke på konsekvenser av endringer i IKT-infrastrukturen. For å få en god oversikt over konsekvensene må det kliniske miljøet trekkes inn i arbeidet med å identifisere disse. For eksempel vil en sannsynligvis måtte øke fokuset på IKT-relaterte hendelser blant annet i gjennomføringen av ROS-analyser, øvelser, oppdatering av beredskapsplaner og i strategien for utvikling av beredskapskompetanse i sykehuset.

Til denne rapportens hovedspørsmål kan det konkluderes med at endringene i IKT-organiseringen i retning av en mer forretningslignende drift henger nært sammen med IKT-bransjens generelle organisering, selv om man nok kunne valgt ulike varianter av dette. Fra et sikkerhetsperspektiv innebærer disse endringene at et tungt fokus må hvile på det å holde oversikt over organisatoriske grenser og å kommunisere risiko på tvers av dem. Beredskapssituasjoner er grenseoverskridende, og fremtvinger gjerne brudd på formelle strukturer. IKT er pr i dag en risikofaktor i seg selv (fordi det er stadig tettere integrert i sykehusdriften) og det er en faktor også i andre hendelser. Det vil være en økende utfordring fremover å gjøre IKT til en integrert del av sykehusets arbeid.

7. Litteratur

Almklov, P. G., S. Antonsen, J. Fenstad, E. Jacobsen, A. Nybø og G. Kjølle (2008) 'Fra forvaltning til forretning: Restrukturering av norske nettselskaper og konsekvenser for samfunnssikkerhet' Rapport: NTNU Samfunnsforskning AS, Trondheim.

Almklov, Petter G. og Antonsen, Stian (2010) 'The commoditization of societal safety' *Journal of contingencies and crisis management* 18(3).

Almklov, Petter, S. Antonsen, J. Fenstad, J. Røstum, F. Sjøvold og R. Værnes (2010) 'Restrukturering av norsk VA-bransje og konsekvenser for samfunnssikkerhet', Rapport: NTNU Samfunnsforskning AS, Trondheim.

Antonsen, S., P. G. Almklov, J. Fenstad og A. Nybø (2010) 'Reliability consequences of liberalization in the electricity sector - Existing research and remaining questions' i *Journal of contingencies and crisis management.* 18(4) (under utgivelse).

Brizon, A. og J. Wybo (2009). 'The life cycle of weak signals related to safety.' *International Journal of Emergency Management* 6, 117-135.

de Bruijne, M. (2006) *Networked Reliability: Institutional Fragmentation and the Reliability of Service Provision in Critical Infrastructures* Delft: Delft University of Technology (PhD avhandling).

de Bruijne, M. og M. van Eeten (2007) 'Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment', *Journal of Contingencies and Crisis Management* 15(1):18-29.

Hood, C. og M. Jackson (1992) 'The New Public Management: A recipe for disaster?', in D. Parker og J. Handmer (eds), *Hazard Management an Emergency Planning. Perspectives on Britain* London: James and James Publishers.

Hood, C. (1991) 'A public management for all seasons', *Public Administration* 69(1):3-19.

Hood, C. (1995) 'The "new public management" in the 1980s: Variations on a theme', *Accounting, Organizations and Society* 20(2-3):93-109.

LaPorte, T., Consolini, P., 1991. 'Working in Practice But Not in Theory: Theoretical Challenges of High-Reliability Organizations'. *Journal of public administration research and theory* 1, 19-48.

Mintzberg, H. (1983) *Structure in Fives: Designing Effective Organizations*, Prentice Hall, Englewood, NJ.

Perrow, C., (1984) *Normal Accidents.* Basic Books, New York.

Poumadère, M., Mays, C., Le Mer, S., og R. Blong (2005). 'The 2003 heat wave in France: dangerous climate change here and now. *Risk Analysis* 25(6), 1483-1494.

Rasmussen, J. (1997) 'Risk management in a dynamic society: A modelling problem', *Safety Science* 27(2-3):183-213.

Roberts, K. (1990) 'Managing high reliability organizations.' *California Management Review* 32, 101-113.

Rudd, C. (2004) 'An Introductory Overview of ITIL®' Rapport. The IT Service Management Forum. Web:
http://learningnetwork.cisco.com/servlet/JiveServlet/downloadBody/3811-102-1-10591/High%20Level%20Overview%20of%20IT%20Infrastructure%20Library.pdf
(Sist nedlastet 17/6-2010).

Weick, K. E. (2004), 'Normal Accident Theory as a Frame, Link and Provocation', *Organization & Environment,* 17(1): 27–31.