

Driftssikkerhet ved bruk av elektronisk pasientjournal

Versjon 1.0
5. mars 2002

KITH Rapport 07/02
ISBN 82-7846-131-7

KITH-rapport



Tittel

Driftssikkerhet ved bruk av elektronisk pasientjournal

Kompetansesenter for IT i helsevesenet AS

Postadresse

**Sukkerhuset
7489 Trondheim**

Besøksadresse

Sverresgt 15, inng G

Telefon

73 59 86 00

Telefaks

73 59 86 11

e-post

firmapost@kith.no

Foretaksnummer

959 925 496

Forfatter(e)

**Bjarte Aksnes
Arnstein Vestad**

Oppdragsgiver(e)

Sosial- og helsedepartementet

Rapportnummer

R 07/02

URL

<http://www.kith.no/rapportarkiv/dsikk.pdf>

Prosjektkode

SHD-DSIKK

ISBN

82-7846-131-7

Dato

5. mars 2002

Antall sider

33

Kvalitetssikret av

Tor Olav Grøtan

Gradering

Ingen

Godkjent av

**Jacob Hygen
Adm. direktør**

Sammendrag

Bruken av elektronisk pasientjournal (EPJ) og andre kritiske IT-løsninger er økende innenfor helsevesenet, og dette stiller økende krav til driftsorganisasjon og teknologi for å sikre stabile og tilgjengelige løsninger. Overgangen til IT-løsninger fra papirbaserte systemer innebærer en økt sårbarhet for en rekke trusler men også redusert sårbarhet på enkeltområder samt en betydelig effektivisering i den daglige bruken av systemene. Dette gjør det vesentlig å komme fram til metoder som reduserer risikoen for tap og utilgjengelighet av kritisk informasjon samt ivaretar

Rapporten beskriver sikkerhetsutfordringer og angir mulige løsningsstrategier ved bruk av EPJ som eneste journalsystem.

Forord

Prosjektet ”Driftssikkerhet ved bruk av elektronisk pasientjournal” er gjennomført av Kompetansesenteret for informasjonsteknologi i helsevesenet AS på oppdrag for Sosial- og helsedepartementet.

Prosjektet har hatt som mål å beskrive sikkerhetsutfordringer og å angi mulige løsningsstrategier ved bruk av EPJ som eneste journalsystem, samt å komme med forslag til områder som det må arbeides videre med.

Målgruppe for dette dokumentet er ansvarlige for drift og sikkerhet av IT-systemer, og da spesielt elektronisk pasientjournal, på norske sykehus, samt sentrale beslutningstagere hos helsemyndigheter.

Denne rapporten kan godt benyttes som et utgangspunkt for gjennomføring av egne trusselvurderinger/risikoanalyser i forhold til EPJ (eller andre kritiske systemer). Ved å ta utgangspunkt i truslene beskrevet i kapittel 2, samt vurdere egen status i forhold til den aktuelle trusselen kan man komme frem til nåværende risikonivå. Dersom denne risikoen er uakseptabel kan man foreslå tiltak som beskrevet i kapittel 3 og 4.

Prosjektet har hatt en referansegruppe bestående av Ivar Berge (Rikshospitalet), Harald Strøm (Telemark Sentralsykehus) og Oskar Aanonsen (Aust-Agder Sentralsykehus). Vi takker disse for nyttige innspill.

Vi takker også EDB Teamco ved Bjørn Erik Nilsen for at vi fikk innblikk i hvordan deres systemer er lagt opp.

Innhold

BAKGRUNN	1
Endringer i lover og regelverk	1
Status for elektronisk pasientjournal	2
Sårbarheten ved bruk av EPJ i helsesektoren	3
Noen utfordringer ved overgang til elektronisk pasientjournal	4
Sykehusreformen	4
Scenarier	5
TRUSLER MOT DRIFTSSIKKERHETEN TIL EPJ	7
Tap av tilgjengelighet	7
Kabelbrudd	7
Strømbrydd.....	7
Brann eller vannskade	8
Overoppheting av tjenere	8
Kritiske tjenester er utilgjengelig	8
Problemer med nettverkskomponenter	8
Utilgjengelighet for tjenere som kjører EPJ	8
Overbelastning av nettverk eller nettverks-komponenter	8
Feil i programvaren (EPJ eller database-programvare).....	9
Planlagt stans.....	9
Følgefeil etter planlagt stans	9
Tap av store mengder data	9
Diskkrasj	10
Utsiktet sletting eller overskriving.....	10
Systemfeil.....	10
Tyveri av disker/tjenere.....	10
Katastrofer	10
Manglende/defekte sikkerhetskopier.....	11
Sabotasje	11
Manglende kapasitet eller ytelse	11
Systemer ikke skalert etter behov	11
Ingen prioritering av ressurser	11
Manglende ytelse på arbeidsstasjoner	12

PROBLEMSTILLINGER OG LØSNINGSSTRATEGIER	13
Intern kompetanse	13
Tjenesteutsetting	13
Fjerndrift av elektronisk journal	14
Servicespesifisering og oppfølging	15
Redundante systemer	16
Sikkerhetskopiering og gjenoppretting	16
Sentralisering av lagringsfunksjoner	18
Teknologiskifte	19
Lagringsnettverk	19
Skalerbarhet	19
ANBEFALTE TILTAK OG VIDERE ARBEID	21
Tiltak for å hindre tap av tilgjengelighet	21
Tiltak for å hindre tap av store mengder data	22
Tiltak for å hindre manglende kapasitet eller ytelse	23
Tiltak med virkning på flere av truslene	24
Organisering av driftsfunksjonen	24
Sikkerhetskopiering og gjenoppretting	24
Partisjonering	25
Beredskaps- og katastrofeplan	26
OPPSUMMERING FRA MØTE MED EN LEVERANDØR	27

Bakgrunn

Elektronisk pasientjournal (EPJ) blir stadig mer utbredt på norske sykehus, og denne utviklingen vil ventelig fortsette. Utgangspunktet for dette prosjektet er den økte sårbarhet knyttet til elektronisk pasientjournal. I denne rapporten vil vi derfor ta for oss driftssikkerhet i forbindelse med elektronisk pasientjournal. Vi vil starte med å gi litt bakgrunn ved å beskrive endringer i relevante lover og regler og gi status for elektronisk pasientjournal, samt peke på sårbarheter i forbindelse med elektronisk pasientjournal.

Med pasientjournal menes alle opplysninger om en persons sykdom og relevante personlige forhold nedtegnet av lege og annet helsepersonell. Journalen skal gi så riktige og tilstrekkelige opplysninger som mulig om pasienten og forhold av betydning for den hjelp personen trenger. En elektronisk pasientjournal (EPJ) er en pasientjournal hvor informasjonen er elektronisk lagret på en slik måte at den kan gjenfinnes ved hjelp av Edb-verktøy.

Driftssikkerhet i forbindelse med EPJ handler hovedsakelig om å:

- forhindre tap eller ødeleggelse av data som er lagret i EPJ, som følge av teknisk svikt eller materiell skade
- sikre tilgjengelighet til EPJ (herunder sikre at responstid og ytelse er akseptabel)

Selv om det ikke er mulig å trekke absolutte grenser mellom driftssikkerhet og generell informasjonssikkerhet har vi valgt å si at driftssikkerhet i liten grad handler om:

- å hindre uautorisert tilgang til data (sikring av konfidensialitet)
- sikre at dataene benyttes ifbm. tjenstlige behov
- hindre ondsinnede angrep på dataene (villede handlinger)

Disse temaene vil derfor i liten grad berøres i denne rapporten.

Endringer i lover og regelverk

I helsepersonelloven (lov om helsepersonell av 1999-07-02) er det åpnet opp for at pasientjournal kan føres elektronisk. Forholdene rundt dette er nærmere regulert i Journalforskriften (Forskrift om pasientjournal fastsatt 21-desember 2000) som er trådt i kraft fra 1 januar 2001. Denne åpner

for bruk av elektronisk pasientjournal (EPJ), enten ved at all dokumentasjon oppbevares elektronisk, eller ved en kombinasjon av elektronisk og papirbasert journal.

I merknader til §4 i journalforskriften er følgende påpekt:

”Bruk av kun elektronisk journal, uten ”papir-backup”, øker sårbarheten og krever gode rutiner m.v. for å forhindre tap og utilgjengelighet. Virksomheter som bare bruker elektronisk journal må sørge for å utarbeide rutiner og retningslinjer for dette. Departementet vil vurdere om det skal gis nærmere retningslinjer eller forskriftsfastsatte krav om hvordan disse forholdene bør eller skal ivaretas.

Ved bruk av elektronisk journalsystem kan det iblant bli nødvendig å lese inn en backupkopi av den elektroniske journalen. Det kan være foretatt retting og sletting i journalen etter at backupkopien ble tatt. Det må etableres rutiner som sikrer at det i slike tilfeller blir foretatt retting/sletting i den gjenopprettede journalen slik at den blir à jour med den tapte journalen. ”

Status for elektronisk pasientjournal

Elektroniske pasientjournaler skal bedre tilgangen til pasientinformasjon, være verktøy for legers medisinske beslutninger, gjøre slutt på at journaler forsvinner og ellers gjøre den medisinske hverdagen enklere, jfr. bla. ”Si @!”, Sosial- og helsedepartementets handlingsplan 2001-2003. Tanken om elektronisk pasientjournal har eksistert siden 70-tallet, men er ennå ikke tilgjengelig i det daglige arbeidet i alle norske sykehusavdelinger.

Det har vist seg å være mange hindringer for utbredelsen av elektroniske pasientjournaler. Organisatoriske, teknologiske og lovmessige forhold må løses. Mangel på felles definisjoner, spesifikasjoner og standarder for innhold og presentasjon gjør det vanskelig å ta i bruk systemer. I tillegg må det investeres i utstyr og tilgang til datamaskiner for brukerne av journalen. På den juridiske siden har også lovverket tidligere satt krav om at papirjournal skal være oppdatert med informasjonen i den elektroniske journalen, noe som til en viss grad begrenser tilleggsverdien ved elektronisk journal.

Mellom annet som en følge av endringene i lovverket begynner dette å endre seg, og mye kan tyde på at storskala bruk av elektroniske pasientjournaler er aktuelt i nær framtid. Per i dag er Doculive EPJ i ferd med å tas i bruk ved landets regionsykehus og en rekke lokal- og sentralsykehus har tatt i bruk DIPS og Infomedix. Grove anslag tilsier at omtrent halvparten av sengepostene ved norske sykehus har tilgang til EPJ.

Fra sentralt hold jobbes det med EPJ særlig gjennom Sosial- og helsedepartementets sitt program ”Standardisering av informasjons- og kommunikasjonssystemer i helsevesenet”. Fokuset her har i første rekke vært å beskrive kravene som må gjelde for å kunne gå vekk fra papirbasert lagring av journalinformasjon, for deretter å utgi en mer omfattende stan-

dard som bedre dekker de behov som må forventes av et slikt system. Særlig har dette vært:

- Spesifikasjon av format for deponering av journalinformasjon
- En grunnleggende journalarkitektur som gir mulighet for en fleksibel bruk av journalen ved å spesifisere generelle mekanismer, attributter osv. som er nødvendig for å strukturere journalen (denne standarden blir publisert i mai 2001)
- Nødvendige mekanismer for å styre informasjonstilgang i tråd med gjeldende regelverk slik at autorisert personell har enkel tilgang til nødvendig informasjon samtidig som det beskyttes mot uautorisert tilgang

Sårbarheten ved bruk av EPJ i helsesektoren

En overgang til EPJ kan gi en betydelig høyere sårbarhet for helsesektoren. Ved dagens bruk av papirjournaler, enten i tillegg til den elektroniske journalen eller som eneste pasientjournal, er det forholdsvis liten fare for at journalen skal gå tapt for godt. Ved overgang til EPJ som den eneste journalen, kan man risikere at store mengder journaler blir utilgjengelig eller går tapt samtidig. Sårbarhetsutvalget ledet av Kåre Willoch har i sin utredning pekt på at tele- og elektronisk kommunikasjon ved sykehus er et område som har høy risiko. En overgang til EPJ som eneste lagringsmedium vil kunne øke risikoen ytterligere, og det er derfor viktig at det settes i verk tiltak for å redusere denne risikoen.

Overgang til EPJ kan også øke muligheten for at uvedkommende får tilgang til store mengder pasientdata, fordi man raskt kan overføre store mengder informasjon ut av virksomheten. Dette er forhold som vi ikke vil gå nærmere inn på i denne rapporten med fokus på driftssikkerhet.

Økt bruk av elektroniske pasientjournaler, og spesielt det at papirkopier ikke lenger må oppbevares, medfører en rekke utfordringer og trusler som må tas alvorlig. Mens en papirjournal er et fysisk objekt som kan bæres fra sted til sted, forutsetter tilgang til elektroniske opplysninger en omfattende infrastruktur hvor alle elementer i kjeden, fra tjenere, databaseprogramvare, nettverksinfrastruktur, arbeidsstasjoner osv., må fungere og være effektive. Feil i enkelte ledd i kjeden mellom bruker og data-system vil ha ulike omfang av konsekvenser. Mens feil på den enkelte arbeidsstasjon vil ramme enkeltbrukere eller en mindre arbeidsgruppe, vil feil på mer sentrale komponenter kunne ramme hele virksomheten.

Frykten for totalt tap av all informasjon ved en virksomhet er alltid til stede ved bruk av databasert lagring. De fleste har opplevd elektroniske lagringsmedier som svikter, det være seg disketter som ikke fungerer, riper på cd-plater eller harddisker som krasjer. Men selv om elektronisk lagring gjør at trivielle hendelser kan ramme store mengder data, muliggjør teknologien at data som før kun befant seg på ett papir kan kopieres

til ulike systemer og sammenlignes automatisk. Data kan potensielt befinne seg på geografisk atskilte steder, men være tilgjengelig over alt hvor det finnes en nettilgang.

På enkelte områder kan sårbarheten kan reduseres ved å ta i bruk elektronisk pasientjournal. Det vil for eksempel være mulig å oppbevare sikkerhetskopier utenfor sykehuset, slik at ikke informasjonene går tapt ved en katastrofal hendelse som brann eller eksplosjon. Med dagens papirbasert systemer ville det være praktisk umulig å ta kopier av den store mengden papirjournaler, og all informasjon ville trolig ha gått tapt i et slikt tilfelle. Ved bruk av EPJ kan det stilles krav til redundans i it-systemene eller faste rutiner for sikkerhetskopiering og krav om lagring av sikkerhetskopier utenfor sykehuset. Ved å gjennomføre tiltak som reduserer sårbarheten til elektronisk lagret pasientinformasjon kan vi få nødvendig tillit til at elektronisk lagret informasjon er like robust og beskyttet mot tap som papirbasert informasjon.

Noen utfordringer ved overgang til elektronisk pasientjournal

Overgangen til elektroniske systemer vil også medføre spesielle utfordringer i overgangsfasen mellom papirbaserte og elektroniske journaler. De fleste større sykehus har enorme mengder med journaler lagret i store arkiver. For å tilby den nødvendige tilgang må denne informasjonen gjøres tilgjengelig for helsepersonell på en hensiktsmessig måte, for eksempel i innskannet form. Personell som skal ta beslutninger basert på innholdet i pasientjournaler må være sikker på at den versjonen de benytter, uavhengig av om den er papirbasert eller elektronisk, inneholder fullstendig og oppdatert informasjon.

En tilnæringsmåte er å tilgjengeliggjøre informasjonen systematisk, fra "A" til "Å". Mye av informasjonen i arkivene vil sannsynligvis aldri refereres igjen, enten pga. alder eller pasienter som har flyttet til andre sykehus eller avgått ved døden. En mer effektiv tilnæringsmåte som benyttes er derfor å starte med å tilgjengeliggjøre de journaler som er aktuelle for pasienter som skal innlegges i nær framtid, ved at en tar utgangspunkt i ventelister og planlagte avtaler/operasjoner.

Sykehusreformen

Sykehusreformen i 2002 har medført:

- At staten overtar eierskapet til de offentlig eide sykehusene
- At disse organiseres i foretak, dvs i egne rettssubjekter utenfor statlig forvaltning
- At staten bruker foretakene til å ivareta sektoransvaret for spesialisthelsetjenesten

Statlig overtagelse av sykehusene vil også få konsekvenser for hvordan man benytter informasjonsteknologi i helsetjenesten. I høringsnotatet ”statlig overtakelse av spesialisthelsetjenesten” er det sagt følgende om informasjonsteknologi:

”Ny teknologi for informasjon og kommunikasjon åpner for nye og ressursbesparende løsninger innen sykehus- og helsesektoren. Telemedisin er et eksempel på dette.

I Norge er vi nå i ferd med å bygge opp nye kommunikasjonsnett i helse-sektoren, basert på regioner. Her må det imidlertid satses på nasjonale løsninger. Disse utdypes i IT tiltaksplanen "SI@!"(januar 2001). Økt mulighet til standardisering og utvikling av felles løsninger vil kunne bidra til en mer optimal utbygging og raskere fremdrift i anvendelse av ny teknologi. Dette vil kunne bidra til bedret samhandling mellom sykehusene og primærhelsetjenesten. Slike felles løsninger vil det være enkle-re å realisere gjennom samordning av eierskapet.

Informasjonsteknologien gir også nye muligheter til å benytte informa-sjon om ressursbruk, behandling og befolkningens behov for helsetjenes-ter til å gi et samordnet og effektivt tilbud av tjenester til befolkningen.”

En statlig overtagelse kan gi større muligheter for å samordne og effekti-visere bruken av informasjonsteknologi innenfor helsevesenet, det kan blant annet. bli aktuelt å sentralisere driftstjenester og IT-kompetanse, også for EPJ. Sammenslåing av noen av dagens enheter kan også gi nye muligheter for å samordne EPJ-system for det som i dag er flere ulike sykehus. Den statlige satsingen på regionale og nasjonalt helsenett vil også ha stor betydning for hvordan slike løsninger kan legges opp.

Fritt sykehusvalg gir pasientene mulighet for å velge på hvilket sykehus de skal behandles, og det må derfor på sikt være mulig å få tilgang til pasientens (elektroniske) journalinformasjon fra det sykehuset han til enhver tid måtte befinne seg på, enten ved at dataene overføres det aktu-elle sykehuset eller ved at det gis en (begrenset) tilgang til nødvendige data.

Scenarier

Vi har utarbeidet et par scenarier som kan illustrere noe av den sårbarheten som en fullstendig overgang til EPJ kan medføre:

Scenario 1:

På natt til onsdag har et rør sprunget lekk i etasjen over datarommet på Sykehuset, og dette medfører at store mengder vann trenger inn i datarommet gjennom taket. Rommet har datagolv som gjør at utstyret ikke blir stående i vann, men en stor del av datautstyret blir skadet som følge av at vann har rent ned i utstyret. Dette medfører blant annet at tjeneren som kjører EPJ blir skadet, samt lagrings- og backupsystemet. Ingen får dermed tilgang til EPJ, og det er anslått at det vil ta inntil 1 uke å få alt utstyret opp å gå igjen i det samme lokalet. Heldigvis har sykehuset en fullstendig sikkerhetskopi fra sist fredag oppbevart utenfor datarommet, og det bør derfor være mulig å gjenopprette dataene fra til denne dagen. Imidlertid viser det seg at båndene bare lar seg lese med en

bestemt streamer-modell som er vanskelig å få tak i. Heldigvis lykkes sykehuset i å oppspore samme modell et sted i Sverige, og denne får de tilsendt som expressgods. Samtidig bestilles nye tjenere og datalagringsutstyr, og i løpet av 5 dager lykkes de i å ha systemet i full drift.

I denne perioden har ingen hatt tilgang til å lese eller registrere informasjon i EPJ, og siden sykehuset har gått helt bort fra papirjournaler har all historikk om pasientene vært utilgjengelig. Dette har medført at pasientene selv har måttet fortelle sin sykehistorie når dette har vært mulig, nye prøver er tatt og analysert, og en god del operasjoner og avtaler har blitt avlyst fordi man mangler nødvendige opplysninger om pasientene. Journalnotater fra denne perioden har blitt skrevet for hånd eller diktet, og man har dermed en stor mengde informasjon som venter på å bli registrert i journalen, og det vil ventelig ta mange uker å bli à jour for kontorpersonalet. Alle data som ble registrert i perioden fra fredag til onsdag er dessuten gått tapt. Alt i alt har situasjonen medført store økonomiske konsekvenser som følge av lavt aktivitetsnivå samt ekstraavgifter for å få systemene opp å gå igjen. I tillegg har pasientsikkerhetene vært i fare fordi helsepersonalet ikke har hatt tilgang til nødvendige opplysninger.

Scenario 2:

En sen vinterkveld i februar er et bedriftsidrettslag på hjem etter en utenbys fotballturnering. De har leid en buss, men pga. utsettelse kom laget seg ikke av gårde før i tidtiden. Det er langt å kjøre, og siden neste dag er arbeidsdag ønsker alle å komme seg hjem så fort som mulig. I en brå sving er uhellet ute, bussen får skrens og ruller utfor en liten bakke før den stopper. Heldigvis har en bil som lå bak bussen og så ulykken mobiltelefon og får varslet. Ambulanse og politi er på stedet etter 20 minutter.

På samme tidspunkt benytter noen driftsansvarlige de sene kveldstimmene til en rutinemessig oppgradering av noen rutere i sykehusets nettverk. Oppgraderingen er varslet på forhånd, og alle avdelingene har skrevet ut nødvendig informasjon for kvelden på forhånd. Når meldingen om en bussulykke med flere skadde kommer inn, varsles IT-avdelingen og de driftsansvarlige beslutter å avbryte arbeidet for å gjøre systemet tilgjengelig igjen. Av uklare grunner viser det seg at en server som skal håndtere pålogging av brukere har sluttet å utføre oppgaven sin.

I det skadede begynner å ankomme akuttmottaket ved sykehuset er journalsystemet fremdeles utilgjengelig. For de fleste pasientene kan de akuttmedisinske tiltakene utføres uten informasjon fra journalene, men en pasient viser seg å reagere allergisk på den smertedempende medisinen han er gitt. Hvis det medisinske personalet hadde tilgang til å kontrollere pasientjournalen i perioden før de skadede ankom kunne dette ha vært unngått, heldigvis oppdages problemet tidlig og skadevirkningene kan begrenses.

Siden ingen har tilgang til it-systemene må resultatene av blodprøver kontrolleres over telefonen, noe som fører til ekstraarbeid og forsinkelser både på laboratoriet og ved avdelingene. I tillegg må mye informasjon etterregistreres når journalsystemet igjen er tilgjengelig.

Trusler mot driftssikkerheten til EPJ

Kapittel

2

Vi vil i dette kapitlet peke på noen trusler som kan true driftssikkerheten til EPJ. Det er ikke gjennomført en fullstendig risikoanalyse, med vurdering av sannsynlighet og konsekvens, men vi vil peke på noen trusler som vi mener er vesentlige i forhold til EPJ. Det anbefales at den enkelte virksomhet selv gjennomfører risikoanalyser for å vurdere truslene i forhold til lokale forhold og iverksatte tiltak. Vi viser til rapporten ”Risikoanalyse – metodegrunnlag og bakgrunnsinformasjon” (KITH-rapport 13/00) for mer utfyllende beskrivelser av hvordan dette kan gjennomføres.

Tap av tilgjengelighet

Problemer i nettverket eller mangel på tilgang til kritiske tjenere eller tjenester kan være årsak til at EPJ ikke er tilgjengelig for brukerne i korte eller lengre tidsrom:

Kabelbrudd

Brudd på datakabler kan forårsake problemer for hele eller deler av nettverket. Dersom kabelbrudd skjer i det sentrale ryggradsnett og redundante (doble) linjer som er fysisk avskilt ikke finnes kan det skape problemer for hele nettverket. Kabelbrudd i fordelingsnett kan også påvirke store grupper av brukere, mens brudd på linjer til klientene normalt bare vil påvirke et fåtall brukere. Tilkoblingen til EPJ-tjeneren vil være spesielt kritisk. Årsaken til kablebrudd kan f.eks. være byggevirkosomhet, uhell, brann eller sabotasje.

Strømbrudd

Strømbrudd kan føre til at både EPJ og selve nettverket settes ut av drift. Dersom strømmen brått brytes, vil dette også kunne forårsake problemer for databaser og andre systemer som ikke blir avsluttet på en kontrollert måte. Data som nylig er registrert kan også gå tapt. Årsaken til strømbrudd kan være mangel i ekstern tilførsel, tekniske feil, feil av servicepersonell eller sabotasje. Nødstrøm vil kunne sikre fortsatt drift, men det er viktig at denne også omfatter nettverkskomponenter som ruter/switcher/brannmurer, og ikke bare kritiske tjenere. Batteristrøm eller

UPS vil kunne sikre tilførsel av strøm ved kortvarige strømbrudd, samt sikre en kontrollert avslutning av programmer.

Brann eller vannskade

Brann i datarom eller andre sentrale kommunikasjonsrom kan gjøre EPJ systemet utilgjengelig i lengre tid. Tjenere eller annet kritisk utstyr som utsettes for vann kan ødelegges. Flom, vannlekkasjer eller brannslukking i etasjer over kan føre til at vann trenger inn i datarom.

Overoppheting av tjenere

Tjenere som utsettes for høy varme kan slutte å fungere. Data- og kommunikasjonsutstyr utvikler dessuten mye varme, og det er derfor viktig at man har tilstrekkelig kjølig for kritisk utstyr. Svikt i kjølesystemet kan forårsake overoppheting av utstyr og tap av tilgjengelighet til EPJ.

Kritiske tjenester er utilgjengelig

Kritiske tjenester som tildeling av IP-adresser (DHCP), autentisering (Domenekontroller), navneoppslag (DNS og Wins) og katalogtjenester kan påvirke tilgangen til nettverket og tjenester. Manglende tilgang til en eller flere av disse tjenestene kan føre til at man ikke får tilgang til nettverket eller til EPJ.

Problemer med nettverkskomponenter

Feil på nettverkskomponenter som rutere, svitsjer og hubber kan forårsake problemer med tilgjengelighet for hele eller deler av nettverket. Stamnett-rutere vil være spesielt kritiske fordi de kan påvirke hele nettverket, men også rutere eller svitsjer som EPJ-tjeneren er tilknyttet vil være spesielt kritisk. Feilene kan ha sin årsak i komponentsvikt, feilkonfigurering eller overspenning som følge av lynnedslag.

Utilgjengelighet for tjenere som kjører EPJ

Tjeneren(e) som kjører EPJ systemet er spesielt kritisk. Feilkonfigurasjon eller maskinvareproblemer kan gjøre tjeneren(e) utilgjengelig. Problemer med strømforsyningen til den aktuelle tjeneren kan også forårsake utilgjengelighet. Disker og kontrollere er spesielt utsatt for svikt.

Overbelastning av nettverk eller nettverkskomponenter

I IP-nettverk er det komplisert å sørge for prioritering av trafikk eller allokering av båndbredde. Stor trafikk i nettverket kan derfor medføre problemer for tilgangen til EPJ. Andre tjenester som f.eks. web, telemedisin, e-post, filoverføringer kan generere så stor trafikk at tilgjengeligheten til EPJ påvirkes. Feilkonfigurasjon av tjenere eller klienter kan også

medføre at disse sender ut datapakker som belaster nettet unødvendig. Bruk av multicasting (f.eks. video-konferanser), uten at spesielle mekanismer for allokering av båndbredde tas i bruk, kan også knekke hele nettverket. Tjenestenektangrep ("Denial of service") rettet mot interne systemer eller komponenter kan også gjøre EPJ utilgjengelig.

Feil i programvaren (EPJ eller database-programvare)

Feil i EPJ-programvaren eller databasene som benyttes av EPJ kan gjøre at data som er lagret i EPJ ikke er tilgjengelig for brukerne. Årsakene kan være feil i programvaren fra leverandøren eller feilkonfigurering av systemet. Feil i EPJ-programvaren kan ha mange konsekvenser med ulik alvorlighetsgrad; fra at hele systemet er utilgjengelig til at enkelte deler av en journal gjøres utilgjengelig. Hvor alvorlige konsekvensene er avhenger også av om feilen blir oppdaget (tidsnok!), og om dataene lar seg tilgjengeliggjøre eller rekonstruere igjen, eller om de er tapt for godt.

Planlagt stans

Planlagt stans av en eller flere komponenter som skal til for å få EPJ til å fungere vil gi tap av tilgjengelighet. Eksempler på årsak til slik nedetid kan være preventivt vedlikehold eller omlegging/oppdateringer av strøm, UPS, nettverkskomponenter, operativsystem, database og brukersystemet. Dette vil ofte være den vanligste årsaken til tap av tilgjengelighet. Konsekvensene av slik stans kan reduseres ved gode rutiner for varslings og for nødruiner på avdelingene. Andre preventive tiltak kan være å etablere testmiljø å gjennomgå arbeide der først og å ha redundante miljøer slik at man kan vedlikeholde et miljø samtidig som et annet sørger for tilgjengelighet av systemene.

Følgefeil etter planlagt stans

Erfaring viser at mye tap av tilgjengelighet skjer etter service og installasjoner av ulikt slag. I mange miljøer er dette en svært hyppig årsak til driftsproblemer. Årsakene til dette kan blant annet være for dårlige rutiner ved endringer og for dårlig planlegging og testing. Noen følgefeil som oppstår etter omlegginger kan ofte være vanskelige å oppdage fordi de først får fokus på seg en tid etter omleggingen. Det er da viktig å ha gode oversikter over hvilke omlegginger som ble gjort når.

Tap av store mengder data

Tap av pasientdata er en svært alvorlig konsekvens, og vi vil her peke på noen årsaker til at dette kan skje:

Diskkrasj

Feil på de primære lagringsmediene er en trussel som kan medføre tap eller utilgjengelighet til store mengder data. Teknologien som benyttes i moderne harddisker er normalt meget pålitelig, men over tid kan data gå tapt enten pga. gradvis svikt i de magnetiske mediene eller mekanisk svikt i komponentene som benyttes til å skrive eller lese data. Feilraten til harddisker oppgis ofte som Mean Time Between Failures (MTBF), og denne vil typisk vise at en disk i gjennomsnitt svikter hver 5-10 år, med mange disk er det store muligheter for at dette vil skje på en av dem. Feilene kan komme plutselig eller oppstå over tid. ***Det siste kan medføre at feil også overføres til sikkerhetskopiene hvis problemet ikke oppdages i tide.***

Utsiktet sletting eller overskriving

Data på harddisker kan slettes eller overskrives ved uhell. Dette kan f.eks. skje i forbindelse med oppgradering av systemet eller ved at harddisken flyttes til et annet system enn den opprinnelig ble brukt på, og hvor det nye systemet ikke forstår filsystemet på harddisken. Sletting kan også forekomme hvis det benyttes lavnivå verktøy for å endre på harddisken, f.eks. for å skifte filsystem.

Systemfeil

Feil i operativsystemet, i grensesnittet mellom lagringsmediet og datasystemet eller i selve harddisken kan medføre at data ødelegges. Et område som er særlig utsatt er harddiskdriveren i operativsystemet som kan inneholde programfeil, særlig i tidlige utgaver av et operativsystem. Det kan være vanskelig å oppdage denne typen feil før dataene skal leses tilbake igjen.

Tyveri av diskertjenere

Tjenere er ofte meget kostbare datassystemer som kan være utsatt for tyveri, noe som medfører en risiko for tap av dataene som er lagret på systemene. Tyveri av tjenere er sannsynligvis først og fremst en trussel mot tilgjengeligheten til dataene, men også mot konfidensialiteten til de personopplysningene som er lagret på systemene.

Katastrofer

Datasystemer og harddisker inneholder følsom elektronikk som kan skades av ulike miljøfaktorer som brann, vann, røyk, vibrasjoner, eksplosjoner eller magnetfelt. I verste fall kan dette føre til at data går tapt for godt. Slike trusler kan oppstå i mange ulike sammenhenger, særlig utgjør byggarbeider eller ombygging i nærheten av datarom hvor tjenere er plassert, samt brannfarlige aktiviteter som sveising og reparasjonsarbeider en fare.

Manglende/defekte sikkerhetskopier

Manglende eller defekte sikkerhetskopier blir et problem først når uhellet har skjedd og primærsystemene er skadet eller data har gått tapt. Sannsynligheten for at både primærsystem og sikkerhetskopi skal feile til samme tid er derfor betraktelig mindre enn for at et system skal feile, men konsekvensen er desto verre. En slik situasjon vil kunne medføre at alle data går tapt, noe som for et sykehus vil være katastrofalt. Siden behovet for å legge tilbake informasjon fra sikkerhetskopi så sjelden oppstår, er det mange som ikke har tilfredsstillende rutiner for å teste dette. Dette gjør at det kan ta så lang tid før feil oppdages at man ikke er i stand til å tilbakeføre sikkerhetskopier, eller at den ikke har fungert som forventet.

Sabotasje

Data kan utsettes for sabotasje på mange måter, og sabotasjen kan foregå elektronisk eller ved å påføre utstyret fysisk skade. De fleste former for sabotasje faller inn under truslene beskrevet ovenfor, men hovedforskjellen ligger i at sabotasje er en bevisst handling som lettere kan målrettes mot de områdene som er mest utsatt, og at sabotøren kan omgå tiltak som skal beskytte mot tilfeldige feil. Sabotasje kan også utføres på de tidspunkter hvor de vil gjøre mest skade og rettes mot flere mål samtidig.

Manglende kapasitet eller ytelse

Utilstrekkelig kapasitet eller ytelse i EPJ kan medføre treg respons eller lang ventetid før man får tilgang til nødvendige opplysninger.

Systemer ikke skalert etter behov

Utilstrekkelig skalerte systemer medfører at tilgjengeligheten reduseres. I enkelte situasjoner kan dårlig ytelse på et journalsystem medføre at brukere ikke har tid til å vente på svar fra systemet og må ta beslutninger på manglende grunnlag. Alle leddene i kjeden fra tjener til bruker må være skalert til å håndtere den trafikken som genereres i systemet. Systemene må være skalert til å håndtere kapasitetskravene også i perioder med høy bruk, slik at tilstrekkelig kapasitet og ytelse kan garanteres til brukere i nødstilfelle selv i perioder med stor trafikk, f.eks. når mange brukere logger seg inn samtidig om morgenen. Systemet må også være i stand til å håndtere spesielt stor trafikk som følge av krisesituasjoner, f.eks. ved store ulykker.

Ingen prioritering av ressurser

En annen årsak til ytelsesproblemer kan være konflikt med andre it-systemer i sykehuset (se også trusselen overbelastning av nettverk). En rekke telemedisinske systemer, løsninger for bildeoverføring, e-post, webbruk osv. som benyttes eller vil innføres i sykehusnettverkene vil

stille store krav til infrastrukturen i form av overføringskapasitet og datakraft. Hvis journalsystemet må konkurrere på lik linje uten mulighet for prioritering, vil dette kunne føre til at tilgjengeligheten til disse reduseres. Mulige flaskehalsen kan oppstå i form av for lite båndbredde eller i brannmurer og andre nettverkskomponenter som skal kontrollere trafikken.

Manglende ytelse på arbeidsstasjoner

Også ytelsen på arbeidsstasjonen som benyttes til mot journalsystemet må være tilpasset behovet. Enkelte journalsystemer benytter seg av komponenter som må kjøre på den lokale arbeidsstasjonen, f.eks. ved at deler av journalen skrives i Word, noe som krever en relativt kraftig arbeidsstasjon for å gi tilstrekkelig ytelse.

Problemstillinger og løsningsstrategier

I dette kapitlet vil vi diskutere noen problemstillinger i forbindelse med EPJ i mer detalj. Vi vil spesielt se på hvordan ulike løsningsstrategier på noen utvalgte områder kan bidra til å redusere sårbarheten ved bruk av EPJ-systemet.

Intern kompetanse

IT og drift av it-systemer er kunnskapsintensivt arbeide og stiller store krav til en virksomhets kompetansenivå. Tilstrekkelig kompetanse er en forutsetning for at en it-avdeling ved et sykehus skal kunne tilby sine brukere effektive og tidsmessige it-verktøy, noe som stiller store krav til virksomheten. Mye av nødvendige kompetanseoppbygging kan foregå internt i virksomheten, f.eks. gjennom at medarbeidere sendes på kurs, intern opplæring eller ansettelse av nytt personale med riktig kompetanse.

Tjenesteutsetting

Av ulike grunner kan det likevel være naturlig å benytte ekstern kompetanse for å dekke de behov driftsavdelingen stilles ovenfor. Sentrale strategier vil være å leie inn eksterne konsulenter, fjerndrift, dvs. at en leverandør drifter systemer hos sykehuset over en nettilknytting, eller tjenesteutsetting (outsourcing), dvs. at en leverandør overtar drift av hele eller deler av it-systemene og utfører dette i hovedsak i egne lokaler. Merk at når vi snakker om leverandør i dette kapitlet så kan dette også være andre sykehus, helseforetak eller helsenett.

Tjenesteutsetting av deler eller hele driftsapparatet knyttet til en it-installasjon er blitt et stadig mer vanlig virkemiddel for organisasjoner som sliter med stadig vekslende teknologi og økende kompleksitet i it-systemene. Valg av tjenesteutsetting som strategi kan ha mange årsaker, f.eks. ønske om faste IT-kostnader eller manglende mulighet for å opprettholde tilstrekkelig kompetanse internt i organisasjonen på kritiske områder. Begge disse problemstillingene er sentrale for sykehus, og kan ventelig medføre at tjenesteutsetting velges som strategi for flere sykehus, i hvert fall på enkelte områder.

For enkelte sykehus kan tjenesteutsetting gi bedre driftssikkerhet, men tjenesteutsetting medfører også en del utfordringer og ulemper som må håndteres. Å sikre gode prosedyrer og retningslinjer for å beskytte infor-

masjonens tilgjengelighet, konfidensialitet og integritet når en tredjepart skal ha tilgang til virksomhetens interne nettverk er én klar utfordring. De administrative prosessene rundt håndtering av avtaler, kjøp og spesifisering av tjenester er en annen. En tredje utfordring er å velge et firma som har tilstrekkelig soliditet og kompetanse til å kunne ivareta sykehusets behov over tid. Det må også forutsettes at den som leier inn tjenester har tilstrekkelig kunnskap om risikoforhold til å utlede egne behov og ønsker og sette opp en bestilling som både kunde og leverandør forstår og kan bli enige om.

Tjenesteutsetting kan også medføre en rekke ulemper, som utarming av intern kompetanse. Andre ulemper kan være at man får mindre kontroll selv, og at det gir mindre fleksibilitet internt.

Dette er sentrale problemområder som virksomheten må håndtere og ha et bevisst forhold til ved valg av tjenesteutsetting som strategi.

Fjerndrift av elektronisk journal

Tjenesteutsetting innebærer som regel at databehandling utføres hos en tjenesteleverandør, eller at en tjenesteleverandør over en nettilknytting utfører tjenester i sykehusets eget nettverk. Nettilknyttingen mellom leverandøren og sykehuset blir da en meget kritisk faktor. Akkurat hvor kritisk tilknyttingen er; avhenger av strukturen i nettet og fordelingen av tjenester. Hvis alle pasientjournalene er lagret hos en leverandør vil tilknyttingen være betraktelig mer kritisk for sykehuset enn om en tilknytting kun benyttes for rutinemessige oppgraderinger av programvare og lignende. Før det tas avgjørelser knyttet til tjenesteutsetting bør det derfor utføres en risikoanalyse med fokus på tilgjengeligheten for å avklare trusler for eksempel knyttet til at kommunikasjonslinjene mellom leverandør og sykehus er utilgjengelig, problemer med strømforsyning hos både leverandør og sykehus osv.

Et viktig tiltak knyttet til en slik vurdering er å vurdere behovet for redundante kommunikasjonslinjer og nødsamband som kan dekke kommunikasjonsbehovet i krisetilfeller. Alle linjene behøver ikke nødvendigvis ha samme kapasitet, men kapasiteten må være tilstrekkelig til å dekke behovet i krisesituasjoner. Som eksempel kan ISDN eller annen type telekommunikasjon med lavere båndbredde benyttes. Den viktigste faktoren i planleggingen av slikt samband er å sikre at løsningene ikke har felles knutepunkter som kan ramme alle linjene samtidig. Slike planer bør også integreres med sykehusets katastrofeplaner, slik at overgangen til nødløsningen foregår planmessig og effektivt når behovet oppstår. Løsningen må også testes med jevne mellomrom.

Leverandøren trenger ikke å være en ekstern kommersiell aktør, også andre konstellasjoner kan dekke et sykehus behov for ekstern kompetanse, driftsstøtte osv. Større sykehus kan være en naturlig samarbeidspartner for mindre sykehus, for eksempel ved at journalsystem eller pasientadministrativt system deles eller at det større sykehuset drifter systemet

for det mindre. Også brukerstøtte og annen drift kan deles på denne måten. Som følge av sykehusreformen i 2002 kan det nå være aktuelt at det etableres en felles løsning for helseforetaket.

Innenfor en helseregion kan sentrale tjenester kjøpes inn felles for flere sykehus og benyttes gjennom et regionalt helsenett. Dette kan i tillegg til driftsmessige fordeler også gi større mulighet for elektronisk kommunikasjon mellom institusjonene ved at disse deler samme system eller benytter systemer fra samme leverandør.

Servicespesifisering og oppfølging

Når tjenester skal utføres av en ekstern virksomhet oppstår det et økt behov for å kontrollere at de tjenester man har bestilt gjennomføres på tilfredsstillende måte. Dette forutsetter en klar enighet mellom partene på hva som er spesifisert og et gjennomtenkt forhold til hvordan dette kan måles i ettertid. SLA'er – "Service level agreements" eller tjenestenivåavtaler har i det siste blitt ansett som den mest aktuelle måten å avtale dette på.

SLA skal definere, i spesifikke og med målbare kriterier, ansvaret til både leverandør og kunde. De sentrale stegene i prosessen med å inngå en slik avtale er først å avklare kundens behov for tjenester, kapasitet, ytelse og lignende, for deretter å avgjøre om leverandøren kan levere dette, og til hvilken pris. I dette arbeidet er det viktig å spesifisere tjenestenivå og ikke løsninger. For kunden er det kvaliteten på den tjenesten som leveres som er avgjørende, ikke hvordan tjenesten produseres. Dette stiller leverandøren fritt til å utnytte sin kunnskap om drift av it-systemer, til å levere tjenesten på en mest mulig effektiv og økonomisk måte. Merk at denne typen metodikk også kan brukes internt.

For å kontrollere at tjenesten virkelig leveres med den kvalitet som er avtalt må det utføres målinger, og det må etableres målemetoder som begge parter er enige om. Slike målinger bør:

- Motivere til riktig adferd, dvs. fokusere på de faktorene som er viktigst for kunden, eksempelvis basert på kostnad eller antall feilsituasjoner
- Være innenfor leverandørens kontroll og dermed være noe leverandøren kan påvirke med sin adferd. Hvis leverandørens evne til å møte avtalte mål avhenger av at kunden skal utføre noe, må dette tas hensyn til i målene
- Være lette å utføre, aller helst kunne samles automatisk for eksempel fra nettverksutstyr

En av de største utfordringene er å finne parametere som gir et godt bilde av situasjonen.

Eksempler på parametere som kan måles er:

- Oppetid på kritiske systemer

- Tilgjengelig båndbredde
- Svartid for henvendelser

Redundante systemer

Den kanskje viktigste faktoren for å oppnå høy oppetid er redundans i løsningene. Alle fysiske komponenter er utsatt for slitasje og kan få feilsituasjoner over tid. Kompleksiteten i moderne programvare innebærer at også her kan feil oppstå som vil kunne hindre kommunikasjonen, f.eks. feil i routing-software og lignende. Redundante systemer og kommunikasjonskanaler hindrer ikke at feilsituasjoner oppstår, men reduserer konsekvensene gjennom å tilby alternativer.

Å sikre redundans er kostnadskrevenende og innebærer en ikke-optimal utnyttelse av de ressursene som er til rådighet. For å ha kapasitet tilgjengelig når feilsituasjoner oppstår, må noe kapasitet være ledig, for eksempel i form av nettverkskabler eller harddisker. For å minimalisere ekstrakostnadene er det derfor nødvendig å gjøre en grundig analyse av hvilke ressurser som bør gjøres redundante og hvilke som ikke er så kritiske.

En slik analyse må se på hele kjeden av it-utstyr og komponenter som er ansvarlig for å gjøre informasjon tilgjengelig for riktig bruker, fra servere, nettverkskomponenter, kabler og arbeidsstasjoner. Noen viktige faktorer som bør vurderes er:

- Hvor mange brukere rammes av en feilsituasjon i komponenten (eksempelvis 1-5 for en arbeidsstasjon, alle for en sentral server)
- Hvor utsatt er komponenten for slitasje (leverandører har gjerne opplysninger om gjennomsnittlig feiltid og lignende)
- Kostnad
- Mulige andre alternativer som ikke innebærer å bytte ut komponenten

I arbeidet med å kartlegge systemet må det også tas hensyn til komponenter og delsystemer som påvirker den aktuelle tjenesten (i dette tilfellet EPJ), men som har lett for å bli oversett fordi de regnes som en del av infrastrukturen. Dette kan være tjenester som bidrar til nettverkskommunikasjonen, som DHCP, DNS og lignende navnetjenester, påloggingsservere osv.

I stedet for å bygge opp et redundant kabelbasert nettverk, har en del sykehus tatt i bruk trådløse nettverk som et supplement og redundant løsning til det tradisjonelle nettverket.

Sikkerhetskopiering og gjenoppretting

Målsetningen med sikkerhetskopiering av EPJ er å hindre at data i EPJ går tapt for godt. Sikkerhetskopiering er spesielt viktig når man ikke

lenger har papirkopier. Det kan være behov for sikkerhetskopier ved katastrofale hendelser som brann, eksplosjon eller flom, men også etter sammenbrudd i enkelte deler av IT-utstyret som disketter el. I tillegg kan det være behov for å hente data tilbake fra sikkerhetskopier ved utilsiktet sletting, feil eller sabotasje.

Ved en fullstendig overgang til EPJ kan datamengdene bli svært store og det kan medføre at dagens løsninger for sikkerhetskopiering får problemer med å håndtere dette. Det kan være en rekke andre systemer og programmer man er avhengig av for at EPJ skal fungere tilfredsstillende, som pasientsystemet, katalogsystemer, brukerdatatabasen. Derfor må det sørges for at det tas også sikkerhetskopier av disse systemene.

Noen av utfordringene med sikkerhetskopiering av EPJ:

- Verktøy for sikkerhetskopiering må tilpasses databasesystem/operativsystem som benyttes av EPJ
- Datamengden kan være så store at man får problemer med kapasiteten
- Løsningene må kunne skaleres for å kunne håndtere de raskt voksende datamengdene
- Det kreves ofte spesialistkompetanse for å sette opp og drifte løsninger for sikkerhetskopiering
- Det er vanskelig å få testet om sikkerhetskopiene lar seg legge tilbake på systemer som er i drift
- Løsningen for EPJ bør integreres med virksomhetens løsninger for sikkerhetskopiering av andre systemer

I en helsevirksomhet med døgntilgjengelig aktivitet vil det være uakseptabelt at EPJ ikke er tilgjengelig døgnet rundt. Det må derfor være mulig å ta sikkerhetskopi av systemet mens det er i drift, uten at dette i betydelig grad går ut over ytelsen. Ideelt sett bør systemet for sikkerhetskopiering fungere med minst mulig grad av menneskelig inngripen. Den daglige inngripen bør begrenses til bytting av medium for sikkerhetskopiering og kontroll av logger, og dersom feilmeldinger eller lignende vises må dette følges opp. Ved behov for å ta sikkerhetskopi av store mengder data bør man også vurdere installasjon av taperobot eller lignende som i stor grad automatiserer prosessen. Det må uansett være avklart hvem som har ansvaret for å følge opp sikkerhetskopieringen, samt hvem som overtar når vedkommende er borte.

Dersom man blir rammet av en katastrofe som brann, eksplosjon eller vannskade i eller i nærheten av datarommet er det stor sannsynlighet for at både originaldataene på tjenerne samt sikkerhetskopier som oppbevares i nærheten også rammes, og selv med brannsikkert skap er det begrenset hvor lenge dette kan beskytte kopiene ved en brann. Med en papirbasert journal ville man ha mistet alle dataene ved en brann i journalarkivet. Men med en (relativt fersk) fullstendig sikkerhetskopi oppbevart

på en annen geografisk lokasjon, vil det være mulig å gjenopprette dataene. Et alternativ kan være å ha en fullstendig speiling av databasen til en annen geografisk lokasjon. For å legge tilbake sikkerhetskopiene er man ofte avhengig av samme type utstyr og programvare. Derfor bør behovet for å også oppbevare utstyr og programvare for lesing av sikkerhetskopiene på et annet geografisk sted vurderes. Alternativt kan det etableres en avtale med en leverandør eller en annen helsevirksomhet som har slikt utstyr tilgjengelig.

Systemet for sikkerhetskopiering må sees i sammenheng med helsevirksomhetens behov og hvilken strategi de har for lagring av data. Behovene kan ha sammenheng med virksomhetens størrelse og hvor utbredt bruken av EPJ er, samt hvilke krav man stiller til gjenoppretting av tapte data. I et system med utstrakt bruk av duplisering og der de samme dataene lagres på geografisk atskilte tjenere, kan behovet for daglige sikkerhetskopier være mindre enn for en virksomhet som ikke har slike systemer.

I tillegg til sikkerhetskopier av selve databasen er det viktig at det tas kopier av programvaren, og spesielt innstillinger og spesialtilpassinger som er gjort. Det kan derfor være nødvendig å ta kopier av hele systemet hver gang det gjøres betydelige endringer.

Sentralisering av lagringsfunksjoner

Funksjoner for lagring og sikkerhetskopiering kan med fordel sentraliseres eller settes bort til en tjenesteleverandør. Ofte vil det være hensiktsmessig at hovedlageret (det man jobber mot vanligvis) er lokalt, slik at de høye kravene til tilgjengelighet kan tilfredsstilles, samtidig med at dataene speiles eller kopieres over til et sentralt lager med jevne mellomrom. Dette stiller høye krav til båndbredde og tilgjengelighet, men det vil ikke være kritisk for den daglige sykehusdriften dersom man får noen problemer med kommunikasjonen med sentrallageret. Dataoverføringen kan dessuten legges til tider på døgnet da trafikken på nettverket tradisjonelt er lav. Spesielt kan det være aktuelt at de nye helseforetakene bygger opp et sentralt lager for foretaket, samtidig med at de ulike enhetene har egne lokallager for "sine" pasienter.

Ved en tradisjonell form for sikkerhetskopiering kan selve gjenopprettingsjobben ta svært lang tid, og det er en betydelig fare for at gjenopprettningen feiler. Et sentralt lager vil kunne fungere som en backupløsning ("hot-site") ved eventuelle problemer lokalt, og en vil til enhver tid ha data som er så godt som oppdaterte, og som kan gjøres tilgjengelig umiddelbart. Ved behov kan det sentralt lageret i tillegg ha funksjoner for sikkerhetskopiering til tape el., ved at det tas ut fullstendige og/eller inkrementelle sikkerhetskopier med jevne mellomrom. En slik løsning kan eliminere behovet for lokale sikkerhetskopier helt, og man overlater ansvaret for løsningen til en sentral enhet eller en leverandør.

Teknologiskifte

En problemstilling som berører EPJ som de fleste andre IT-systemer er større teknologiskifter. Vi kan med stor sikkerhet si at det vil komme teknologiskifter som vil være minst like ”dramatiske” som overgangen fra stormaskinløsninger til klient/tjener løsninger var. Vi kan også forvente at det vil komme nye generasjoner av journalsystemer, til dels basert på ny teknologi. Det er vanskelig å gi generelle råd for hva man bør gjøre ved denne typen teknologiskifter, men generelt vil vi råde sykehuse til å ha et langsiktig tidsperspektiv og å være konservative ved overgangen til nye løsninger og ny teknologi for kritiske systemer som EPJ. Teknologien bør ha nådd et visst modenhetsnivå, og være prøvd ut på andre systemer som er mindre kritiske før man tar den i bruk for EPJ. Samtidig må man være på vakt slik at man ikke blir sittende igjen med en løsning basert teknologi som ikke lenger støttes (eller prioriteres), eller der det vanskelig å få tak i reserveutstyr eller kompetent personell.

Lagringsnettverk

Tidligere var disksystemene vanligvis direkte koblet til tilhørende tjener. Dette har ofte ført til dårlig utnyttelse av kapasiteten og problemer med å skalere ytelse og lagringskapasitet. Lagringsnettverk er et forsøk på å løse disse problemstillingene, og det betyr at datalagringsenhetene kan skilles fra selve tjenerne.

De er hovedsaklig to løsninger som benyttes for lagringsnettverk, og disse kan kombineres for å få effektive lagringsnettverk:

- NAS (Network Attached Storage) - benytter filsystemprotokoller (NFS, CIFS, med flere) for å kommunisere med klienter og tjener. Data fra ulike systemer (Unix, NT) kan deles på samme disksystem.
- SAN (Storage Area Network) - benytter SCSI-protokollen via Fibre Channel for å sende informasjon mellom tjener og lagringsløsningen. Tjener som kjører på ulike plattformer og fra ulike leverandører kan benytte det samme lagringsnettverk, og SAN kan dermed skape en pålitelig og skalerbar infrastruktur for datahåndtering.

Skalerbarhet

En skalerbar løsning er en løsning der man kan øke kapasiteten/ytelsen forholdsvis jevnt etter økende behov, uten at dette koster uforholdsmessig mye. I enkelte tilfeller vil man stange mot kapasitetsgrenser som krever at det gjøres store endringer eller utskiftninger for å øke kapasiteten/ytelsen ytterligere.

EPJ-løsningene må designes slik at de er i stand til å skalere etter varierende behov. Det må være mulig å utvide antall brukere innenfor rimelighetens grenser uten at dette krever store endringer i systemet. Tilsvarende må systemet være i stand til å takle at brukerne blir mer krevende

og utnytter systemet bedre, og det må være mulig å legge til ny funksjonalitet i systemet. Noen faktorer som man må ta hensyn til ved vurdering av løsningenes skalerbarhet:

- Antall totale brukere
- Antall samtidige brukere
- Antall samtidige operasjoner/oppgaver som innebærer stor belastning på en tjeneste
- Lagringskapasitet
- Kapasiteten i nettverket (båndbredde)
- Muligheter for å legge til ny funksjonalitet i EPJ (oppgradering/utvidelse av programmet)
- Antall samtidige pålogginger (autentisering)
- Kapasitet til sikkerhetskopieringsløsningen
- Kapasitet til løsningen for tilbakekopiering og oppretting (restore).

For alle disse faktorene må det vurderes om det finnes noen grenser som gjør at det krever store utskiftninger eller investeringer å overstige, og disse grensene må ligge godt innenfor det som forventes å bli behovet i nærmeste framtid. Som eksempel dersom det per i dag brukes 1 TB lagringskapasitet, så er estimert behov om to år det dobbelte, altså 2 TB. Løsningen må derfor være slik laget at den kan utvides til å dekke lagringsbehovet i mange år fremover, men uten at det må investeres i disketter og lignende før behovet er der. For kritiske systemer som EPJ er det alltid farlig å operere like under kapasitetsgrensene, og det må derfor alltid være gode marginer til grensene.. For å klare dette er det viktig å ha en kontinuerlig overvåkning av viktige parametere som graden av utnyttelse av systemet (CPU, minne, diskplass, båndbredde, sesjoner, responstider) og sette i gang tiltak når systemet nærmer seg kapasitetsgrensene.

Anbefalte tiltak og videre arbeid

Prosjektets ressursrammer har bare gjort det mulig for oss å gå i detalj på anbefalinger til tiltak ved fullstendig overgang til EPJ. Vi har kun pekt på relativt generelle og overordnede tiltak, og disse bør detaljeres og utfylles med videre arbeid innenfor området. Vurderingen av hvilke tiltak som bør iverksettes må også ledsages av kost/nytte vurderinger.

De tre første underkapitlene gir overordnede tiltak for å håndtere hver enkelt trussel beskrevet i kapittel 2, og i siste underkapittel angis noen tiltak som virker inn på flere trusselområder.

Tiltak for å hindre tap av tilgjengelighet

Kabelbrudd og stømbrudd:

Det bør etableres redundante løsninger for data- og strømkabler til kritisk datautstyr for EPJ. Det bør være to uavhengige strømforsyninger (tilknyttet uavhengige UPS-er) til alt kritisk utstyr. Redundans for datanettverket kan også oppnås ved å etablere et trådløst nettverk internt i tillegg til det kabelbaserte. Ved tjenesteutsetting eller fjerndrift må det være minst to uavhengige veier til leverandøren. Man må også passe på at de ulike linjene ikke er koblet sammen hos telekommunikasjonsleverandøren(e).

Brann eller vannskade:

Datarom og kommunikasjonsrom må beskyttes mot brann- og vannskader. Kritisk utstyr bør plasseres slik at de er minimalt utsatt for skader forårsaket av vannsøl. Det må etableres tiltak for automatisk varsling ved branntilløp eller ved vanninntrenging.

Overoppheting av tjenere:

Det må etableres tilstrekkelig kjøling i områder der EPJ-tjenere og kritisk kommunikasjonsutstyr er plassert. To uavhengige løsninger for kjøling bør vurderes, f.eks. et strømbasert og et basert på isvann.

Kritiske tjenester er utilgjengelig

Kritiske ressurser som DHCP, DNS, katalogtjenester, bør være redundant og tilgjengelig fra ulike nettverkssegmenter. De redundante løsningene bør fortrinnsvis plasseres fysisk adskilt fra hverandre.

Problemer med nettverkskomponenter

Man bør basere seg på utstyr med høy stabilitet. Alle veier i stamnettet bør være redundante, det vil si at det bør være minst to mulige veier mellom alle sentrale svitsjer, slik at man tåler at en svitsj faller ut. I tillegg bør man sikre tilgang til reservekomponenter ved å ha eget lager, avtale med leverandører (responstidsavtaler) eller avtaler med andre brukere av tilsvarende utstyr.

Utilgjengelighet for tjenere som kjører EPJ

EPJ bør kjøre på tjenere med høy stabilitet. Kritiske tjenere kan dubleres eller det kan opprettes klynger (cluster) av flere tjenere. Alternativt må det etableres katastrofeplan for hvordan EPJ kan kjøres dersom en sentral tjener svikter.

Overbelastning av nettverk eller nettverks-komponenter

Vurdere mekanismer for prioritering av trafikk eller allokering av båndbredde. Vurdere bruk av virtuelle nettverk (VLAN) for å begrense spredningen av trafikken. Dersom man i tillegg har etablert trådløse nettverk kan dette brukes til å avlaste det tradisjonelle nettet.

Feil i programvaren (EPJ eller database-programvare)

Teste programvaren godt før den settes i drift. Etablere eget testmiljø der ny programvare (versjoner) kan testes. Ha god beredskap når nye programvare settes i drift.

Planlagt stans

Legge planlagte stans til tider der manglende tilgjengelighet ikke har store konsekvenser. Forberede og teste ut mest mulig på forhånd. Varsle avdelinger (berørte brukere) i god tid og sørger for at disse tar nødvendige forhåndsregler. Ved redundante systemer kan endringer gjøres på et system mens det andre er i drift. Vær oppmerksom at endringer i andre systemer kan påvirke EPJ, og test alltid EPJ etter at det er gjort endringer i andre systemer.

Følgefeil etter planlagt stans

Sørge for at kvalifisert personell, både internt og hos leverandør, er tilgjengelig (eller i beredskap) også en tid etter at systemene er satt i drift igjen. Vær forberedt på feilsituasjoner som kan oppstå.

Tiltak for å hindre tap av store mengder data**Diskkrasj**

Benytte lagringssystem som har høy stabilitet, samt bruke speilede disker (RAID 1 el. 5) slik at data ikke mistes selv om en disk svikter. Samt sørge for at løsningen for sikkerhetskopiering er tilfredsstillende. Man

bør sørge for å ha nye disketter og kontrollere tilgjengelig enten ved å ha de på eget lager, eller ved å avtale med leverandører el.

Utsiktet sletting eller overskriving

Etabler rutiner for hvem som skal ha skrivetilgang til kritiske tjenester og databaser på disse, og kontrolleres om disse følges. Det må også kontrolleres hvem som har mulighet for tilgang ved hjelp av administratorrettigheter.. Ta alltid sikkerhetskopier av dataene før det gjøres endringer i konfigurasjoner eller før ny programvare installeres.

Systemfeil

God rutiner for sikkerhetskopiering, samt tiltak som beskrevet under diskrasj.

Tyveri av disketter/tjenere

Etabler god fysisk sikkerhet i form av autorisasjon, adgangskontroll, fysiske sperrer, alarmer og vaktthold til områder som inneholder kritisk utstyr. Ansatte må dessuten være oppmerksom på personer med mistenkelig oppførsel.

Katastrofer

Etablere alternativt driftssted, selv eller i samarbeid med leverandør eller andre sykehus, for bruk ved større katastrofer. Utarbeide og teste katastrofe/beredskapsplan for slike situasjoner.

Manglende/defekte sikkerhetskopier

Sørge for at kvalifisert personale har satt opp løsningen for sikkerhetskopiering. Etablere klare rutiner for sikkerhetskopiering (se eget avsnitt). Kontrollerer tilbakelegging med jevne mellomrom. Sikkerhetskopier må oppbevares på et annet sted enn der lagringssystemet befinner seg.

Sabotasje

Tiltak for fysisk sikkerhet (se tyveri av disketter/tjenere) kan hindre sabotasje. Sabotasje utført via datasystemer kan hindres/oppdages ved å implementerer mekanismer som brannmurer, virusprogramvare og overvåkingssystemer (IDS- intrusion detection systemer), samt ved en aktiv oppfølging fra IT-personalet.

Tiltak for å hindre manglende kapasitet eller ytelse

Systemer ikke skalert etter behov

Kontinuerlig overvåkning av nettverk og systemer for å avdekke flaskehals. Innhenting og evaluering av brukererfaringer for å finne ut om kapasiteten er tilstrekkelig. Dersom det avdekkes flaskehals må tiltak for å utvide kapasiteten iverksettes.

Ingen prioritering av ressurser

Ta i bruk mekanismer for prioritering av trafikk eller allokering av båndbredde. Regulere bruken av andre systemer ved stor belastning eller i krisesituasjoner (som web-tilgang). Se også under overbelastning av nettverk eller nettverkskomponenter.

Manglende ytelse på arbeidsstasjoner

Sjekke at arbeidsstasjonene har tilstrekkelig ytelse til å brukes mot EPJ ved å måle responstider og hente inn brukererfaringer. Sjekke også hvilke anbefalinger leverandøren av EPJ gir for arbeidsstasjoner som skal benyttes. Vurdere oppgraderinger eller kjøp terminalløsninger for arbeidsstasjoner som har manglende kapasitet.

Tiltak med virkning på flere av truslene*Organisering av driftsfunksjonen*

Ansvaret for driftssikkerheten bør deles mellom to separate funksjoner:

1. Ansvar for drift av informasjonssystemet, herunder alle sikkerhetsfunksjoner og rutiner for konfigurering og administrasjon av disse.
2. Operativt ansvar for å påse at sikkerhetspolicy og rutiner blir fulgt - herunder at personale og avdelinger har og følger hensiktsmessige rutiner og prosedyrer, bedømming av risikobilde, samt oppfølging av sentrale rutiner (som autorisering av brukere) og avgjørelse av enkeltsaker. Denne rollen vil ha en "controller"-funksjon i forhold til informasjonssikkerhet.

Virksomheten må sørge for at avhengigheten til enkeltpersoner for drift av EPJ ikke blir for stor, ved å sørge for kompetanseoverføring til flere personer internt, samt å dokumentere kritiske operasjoner rundt driften av EPJ, slik at det også er mulig å utføre operasjonene uten at "eksperter" på systemet er tilstede. Eksempler på operasjoner som må være dokumentert er oppstart av systemet etter stans, tilbakelegging av data fra sikkerhetskopier.

Det må etableres hensiktsmessige vaktordninger, slik at problemer kan rettes opp også utenom vanlig arbeidstid. Vaktpersonalet bør få automatisk beskjed ved en del kritiske hendelser som strømstans, fulle disk med mer.

Sikkerhetskopiering og gjenoppretting

Følgende punkter kan benyttes som en sjekkliste:

- Det må minimum taes sikkerhetskopi av siste dags endringer i EPJ hver dag (inkrementell). I tillegg må det eksistere en transaksjonslogg på et annet fysisk medium.

- Fullstendig sikkerhetskopi må tas minst en gang i uken. Et alternativ er speiling av hele databasen.
- Sikkerhetskopier bør oppbevares i brannsikkert skap og beskyttes for uautorisert tilgang.
- En fullstendig sikkerhetskopi må med jevne mellomrom (minst ukentlig) tas ut og oppbevares geografisk atskilt fra virksomhetens EPJ-tjenere og løsning for sikkerhetskopiering (fjernkopi). Oppbevaringsstedet må sikres med tilfredsstillende fysisk sikring.
- Transporten av sikkerhetskopieringsmedium mellom datarom og oppbevaringssted må skje på en sikker måte.
- Det må utnevnes en ansvarlig for sikkerhetskopiering, samt stedfortreder(e), samt en prosedyre for varsling av stedfortreder ved vedkommendes fravær.
- Det må utarbeides en prosedyre som beskriver oppgavene til ansvarlig for sikkerhetskopiering, denne må også omfatte rensing av utstyret og når gamle medium skal tas ut av bruk.
- Det må etableres en loggbok der ansvarlig for sikkerhetskopiering kvitterer for at medium er skiftet og logger er sjekket med mer, denne bør oppbevares i brannsikkert skap sammen med taper. Medium skal merkes med 'personopplysninger' samt andre data for å kunne identifisere når og hva kopien stammer fra.
- Ved problemer/feil med sikkerhetskopi som ikke kan løses umiddelbart skal dette varsles til nærmeste overordnede (f.eks. IT-sikkerhetsansvarlig).
- Det bør etableres en avtale med leverandør el. for rask bistand ved problemer med løsningen for sikkerhetskopiering.
- Det må etableres en rutine for jevnlig verifisering av sikkerhetskopier. Dersom det er praktisk mulig bør man teste tilbakekopiering (restore) med en fullstendig sikkerhetskopi.
- Det må utarbeides en prosedyre for gjenoppretting av data fra sikkerhetskopi, og denne må testes med jevne mellomrom.
- Dersom man velger å sentralisere eller å sette bort tjenester for sikkerhetskopiering vil en rekke av de ovenfor nevnte tiltakene kunne utføres av den aktør som er valgt til å utføre disse tjenestene.

Partisjonering

Poenget med partisjonering eller segmentering er å samle ressurser og brukere som hører logisk sammen funksjonelt, og etablere barrierer mot andre segmenter. På denne måten kan man redusere faren for at brukere og/eller systemer som befinner seg i ulike segmenter påvirker hverandre. Uønsket trafikk kan stoppes eller begrenses i barrierer/filter (svitsjer,

rutere eller brannmurer) mellom ulike segmenter. Hovedbegrunnelsen for å gjøre dette er å redusere kompleksitet og øke stabiliteten i nettverket. Metoden kan også ha en viss effekt for å begrense tilgangen, men her må man supplere med andre mekanismer (tilgangskontroll med mer), fordi partisjoneringen i hovedsak baserer seg på IP-adresser som lett lar seg forfalske. EPJ-systemet, og i de minste kritiske brukere av systemet, bør plasseres i et eget segment, som i minst mulig grad påvirkes av aktiviteten i andre segmenter. Brukere som ikke har så kritiske behov kan godt plasseres i et annet segment og gis tilgang over barrieren.

Beredskaps- og katastrofeplan

Det må etableres en beredskapsplan/katastrofeplan som omhandler alternativ drift i/etter en krisesituasjon samt hvordan komme tilbake til normal drift. Kopi av planen og andre relevante prosedyrer må oppbevares utenfor virksomheten. Denne må spesielt omhandle:

- hva som skal erklæres som en krisesituasjon
- manuelle rutiner i en krisesituasjon
- etablering av alternativ databehandling
- gjenoppretting av normal driftsfunksjon
- testing og revisjon av kriseplanen

Katastrofeplanen må også inkludere planer for hva brukere/avdelinger som er avhengige av EPJ skal gjøre i en situasjon der EPJ ikke er tilgjengelig.

Det er vanskelig å få testet en katastrofeplan fullstendig, men man bør uansett gå gjennom denne "på papiret" med faste intervall, og gjennomføre tester/øvelser på områder der dette er mulig.

Oppsummering fra møte med en leverandør



Som en bakgrunn for arbeidet med driftssikkerhet ved bruk av EPJ ønsket vi å se på hvordan en kommersiell aktør kan tilby driftssikre løsninger, og vi var så heldige å få besøke EDB Teamco fasiliteter.

Møtet fant sted i EDB Teamco's fjellhall i Oslo, som er tilknyttet deres sikre fjellanlegg. Fjellanlegget ble opprinnelig bygd som militært "utflyttingssted" og er tilpasset for at mennesker skal kunne oppholde seg der over lengre tid, med bla. vannlagre, klimakontroll og luftfiltre. Teamco har i ettertid tilpasset anlegget for egen bruk som datadriftshaller. Anlegget ble bygget på slutten av 80-tallet, og i perioden fra 1997-2000 har det blitt investert 700 mill. kr for å tilpasse og bygge opp dagens anlegg.

Viktige prinsipper ved designet av løsningen har vært å gi mulighet for speiling, clustring og remote backup. Det skal være mulig å tilby så høyt tjenestnivå som det er i praksis er mulig å tilby. Anlegget skal også kunne tjene som katastrofeløsning for Teamco's anlegg på Skøyen, og vica versa. Det ble også lagt vekt på å skille mellom "høy tilgjengelighet" som går på å minimere planlagt nedetid, og katastrofeløsninger som går på "ikke planlagt" nedetid (nøddrift).

Anlegget består pr. i dag av to separate haller hver på to etasjer med individuell strømforsyning og kjøling. Hver hall har også individuelle UPS-løsninger og dieselgeneratorer. Både strøm og kommunikasjonskabling har to separate innføringer til hver datahall, og alt utstyr har to separate strømtilførsler. Alt utstyr har 4 nettverkskort som er knyttet til hhv WAN, SAN, Driftsnett og et Katastrofenett. Ut fra anlegget er det to separate kommunikasjonsløsninger til datasenteret på Skøyen.

Senteret kan tilby ulike løsninger for backup. Backup kan foregå til robotstyrt tapeserver lokalt, evt. også til en tapeserver i driftslokalet på Skøyen.

Det er lagt stor vekt på kundene enkelt og raskt kan utvide løsningene sine f.eks. ved behov for større prosesseringskapasitet eller lagringsplass. Dette kan gjøres ved at man alltid har litt å gå på, og ved at utstyrleverandører plasserer utstyr som er klart for å tas i bruk i Teamcos lokaler. Ved behov aktiveres utstyret og kostnadene begynner å løpe.

Etter vår vurdering kan en slik løsning gi svært god driftssikkerhet, ved at en profesjonell aktør tar seg av driften av en del kritisk utstyr. Ved å samle utstyr fra mange ulike kunder, og dele kostnadene på mange aktører er man i stand til å lage driftsomgivelser med en driftssikkerhet som langt overgår det hver enkelt aktør kan klare å gjøre på egen hånd, både i forhold til fysisk sikkerhet og driften av systemene. I tillegg får man nyte godt av den erfaring og kompetanse som slike leverandører har bygd opp over mange år. En annen fordel er at løsningene er overvåket hele døgnet, og at vaktpersonell er klare til å gripe inn dersom det oppstår problemer. Kun svært store virksomheter vil være i stand til å ha en slik beredskap på egen hånd. Vi har ikke gjort noen vurdering av kostnadene for slike løsninger, men vi vil peke på at kostnadene må vurderes i forhold til hvilket nivå for driftssikkerhet (f.eks. oppetid) man legger seg på.