IT-haverier i vården

Erfarenheter och förslag till åtgärder från aktuella fall

Kamedo-rapport 96

Socialstyrelsen

Kamedo – Katastrofmedicinska observatörsstudier – har funnits sedan 1964 och hette tidigare Katastrofmedicinska organisationskommittén. Verksamheten startade inom ramen för Försvarsmedicinska forskningsdelegationen och år 1974 överfördes Kamedo till Försvarets Forskningsanstalt (FOA), som i dag heter Totaltförsvarets forskningsinstitut. Sedan 1988 är Kamedo knutet till Socialstyrelsen.

Kamedos huvudsakliga uppgift är erfarenhetsåterföring som kan ske genom att sakkunniga observatörer sänds till platser som drabbats av allvarliga händelser. Observatörerna sänds ut för att samla in relevant information genom kontakter med berörda personer inom sjukvården, räddningstjänsten, polisen, övriga myndigheter och organisationer. Den insamlade informationen används i syfte att återföra erfarenheter till Sveriges krishanteringssystem och i vetenskapliga sammanhang. Det är främst de medicinska, psykologiska, organisatoriska och sociala aspekterna av allvarliga händelser som studeras.

Verksamheten bedrivs som projekt där en utredare vid Socialstyrelsen ingår tillsammans med andra sakkunniga externa personer. Till sitt stöd har projekten en intern styrgrupp samt en extern referensgrupp.

Resultaten publiceras i Kamedo-rapporter som finns förtecknade på Socialstyrelsens webbplats. Från och med nummer 74 finns hela rapporten att hämta där men för tidigare rapporter finns endast en sammanfattning. Från och med rapport 34 översätts sammanfattningen till engelska och från och med rapport 55 publiceras översättningen endast på webbplatsen. Från och med rapport 89 översätts hela rapporterna till engelska.

Författarna svarar själva för innehållet och slutsatserna, och Socialstyrelsen drar inga egna slutsatser i dokumentet. Experternas sammanställning kan dock bli underlag för myndighetens ställningstagande.

ISBN	978-91-86885-87-8
Artikelnr	2011-12-24
Omslag	Tiina Laukkanen, Socialstyrelsen
Omslagsfoto	Ilja Hendel / SCANPIX, Darren Kemper/Corbis / SCANPIX, Luis Alonso Ocaña / AGE / SCANPIX
Sättning	Edita Västra Aros
Tryck	Tryck: Edita Västra Aros, Västerås, mars 2012

Förord

Med anledning av det ökande antalet incidenter av typen IT-haverier som har drabbat hälso- och sjukvården har Socialstyrelsen beslutat att skriva en tematisk Kamedo-rapport om IT-haverier och de lärdomar som kan dras av dem. En tidigare rapport (Kamedo-rapport 93, ”Strömavbrottet på Karolinska Universitetssjukhuset Huddingen den 7 april 2007) har studerat det omfattande strömavbrott som drabbade Karolinska Universitetssjukhuset Huddinge och som ledde till allvarliga störningar i sjukvårdsverksamheten under flera timmar, och kan utgöra ett komplement till föreliggande rapport.

I rapporten har några olika typer av it-haverier beskrivits och kommenterats. I det sista kapitlet presenteras slutsatser som bör beaktas av myndigheter och vårdgivare inom hälso- och sjukvården.

Åsa Ljungquist
Tillförordnad enhetschef, Enheten för krisberedskap

Författare och uppgiftslämnare

Författare

Lars-Göran Angantyr, Socialstyrelsen
Johan Carlstedt, Socialstyrelsen
Björn-Erik Erlandsson, Kungliga tekniska högskolan
Susannah Sigurdsson, Socialstyrelsen
Åsa Molde, Socialstyrelsen
Helena Andersson, Myndigheten för Samhällsskydd och Beredskap
Svante Nygren, Myndigheten för Samhällsskydd och Beredskap

Extern granskare

Helge Brändström, Västerbottens läns landsting

Intervjuade personer och uppgiftslämnare

Lennart Wallén, Region Skåne
Axel Tonning, Region Skåne
Ann-Christin Andersson, Region Skåne
Rolf Ohrlander, Region Skåne
Lars-Olof Almquist, Region Skåne
Svante Baehrendtz, Karolinska Universitetssjukhuset
Bo Vikström, Karolinska Universitetssjukhuset
Petter Könberg, landstinget i Kalmar län
Eva Ingesson, landstinget i Kalmar län
Ulf Hansson, Akademiska Sjukhuset i Uppsala
Anders Björklind, landstinget i Uppsala län
Filippa Nyberg, Akademiska Sjukhuset i Uppsala
Per Adolfsson, Akademiska Sjukhuset i Uppsala
Per Foyer, Akademiska Sjukhuset i Uppsala
Peter Olsson, landstinget i Uppsala län
Per Liss, Bild och Funktionsmedicinskt centrum

Nyckelord

IT
IT-haverier
Incidenter
Patientsäkerhet
Kvalitetssystem
Standarder
Författningar
ITIL

Innehåll

Förkortningar

ASIH	Avancerad sjukvård i hemmet
CSTC	Centrum Samverkan TakeCare
EN	European Norm
IEC	International Electrotechnical Commission
ISO	International Standards Organisation
ITIL	Information Technology Infrastructure Library
KBM	Krisberedskapsmyndigheten
KiB	Kommunikatör i beredskap
LVFS	Läkemedelsverkets författningssamling
MDD	Medical Devices Directive
MT	Medicinsk Teknik
MTC-RS	Medicinteknisk chef i Region Skåne
PACS	Picture Archiving and Communication System
RIS	Radiologiskt informationssystem
RSIT	Region Skånes IT-avdelning
SAN	Storage Area Network
SIS	Swedish Standards Institute
SLL	Stockholms läns landsting
SLL-IT	Stockholms läns landstings IT
SLSO	Stockholms läns sjukvårdsområde
SOSFS	Socialstyrelsens författningssamling
TIB	Tjänsteman i beredskap
UPS	Uninterruptible Power Supply/Source
VC	Vårdcentral

Sammanfattning och erfarenheter

Sammanfattning

I denna rapport redovisas fyra olika typer av störningar i IT-system som inträffat i svensk sjukvård under perioden 2008-2009. Hälso- och sjukvården har inte fungerat tillfredsställande i dessa fall och det har funnits risk att man inte har kunnat upprätthålla patientsäkerheten vid undersökning, vård och behandling. Orsaken till störningarna i IT-systemen har varit av helt olika slag och rapporten kan därför ge en uppfattning om hur sårbar informationstekniken är idag och vilka konsekvenser det kan bli om tekniken inte fungerar. Tre av händelserna har anmälts till Socialstyrelsen enligt lex Maria och i det fjärde fallet besökte Socialstyrelsens tillsynspersonal det berörda sjukhuset för bedömning av pågående IT-problem.

De slutsatser och erfarenheter som presenteras i rapporten handlar mycket om ledning och styrning av IT-verksamheten. Dessa frågor bör beaktas både av vårdgivarna, som har yttersta ansvaret för kvalitet och patientsäkerhet, och av berörda myndigheter i sin tillsyn. En annan viktig fråga som belyses i rapporten är i vilken omfattning vårdgivarnas katastrofplaner innehåller handlingsplaner för hur organisationen ska agera vid störningar i IT-systemen. Skyddet mot yttre hot mot IT-verksamheten och uppbyggnaden av säkra infrastrukturer är andra ämnen i rapporten. Upphandling av IT-system och IT-tjänster samt avtal med leverantörer är andra angelägna frågor som tas upp. I alla dessa frågor är ändamålsenliga system för ledning och uppföljning på både övergripande och verksamhetsnivå avgörande för en säker vård och omsorg.

De fyra händelser som belyses i rapporten är:

E-virusangrepp i Region Skåne

Den 3 januari 2009 uppstod problem med att logga in på Region Skånes intranät. Virusskyddet identifierade inte något virus, men det stod ändå snabbt klart att det rörde sig om ett virusangrepp av ett tidigare okänt virus. Cirka 10 000 datorer och cirka 500 servrar inom Region Skåne smittades och därmed uppstod många slags problem och stundtals svårigheter att upprätthålla en god och säker vård.

Direkta problem i vården, som uppstod till följd av att man inte kunde använda nätverket, blev att man inte kunde läsa patientjournaler, att

centralenheten i intensivvårdsövervakningen inte fungerade, att remisser varken kunde skickas eller läsas, att patientadministrativa system ej var åtkomliga, att man inte kunde använda arbetsstationer kopplade till diagnostik- och laboratorietjänster med mera. E-posten fungerade inte och man kunde inte heller nå Internet. Medicinteknisk utrustning med inbyggd datorfunktion eller med separat ansluten dator drabbades också om de var anslutna till intranätet. Problemen ökade under årets första veckor i takt med att personalen återkom efter nyårshelgen och loggade in på intranätet och då fick sina datorer smittade. Inga patienter blev skadade på grund av att vårdinformation inte var tillgänglig, men många undersökningar och behandlingar blev inställda eller försenade. Avbrottet medförde betydande merarbete för all personal och en stressig arbetsmiljö.

Den 5 januari informerade IT-enheten Regional Medicinsk Katastrofledning i Skåne (RMKL), tjänsteman i beredskap (TiB) och kommunikatör i beredskap (KiB). TiB fick ingen information om virusangreppets omfattning och blev inte medveten om att patientsäkerheten kunde vara i fara. KiB lade ut information om störningen på IT-enhetens hemsida. Någon annan information gavs inte till regionens sjukhus och vårdinrättningar vid inledningen av den stora störning i IT-systemen som skulle följa. RKML höjde aldrig beredskapsnivån.

Mycket arbete lades ner på att felsöka, identifiera och rensa ut viruset, uppdatera antivirusprogram och installera säkerhetspatchar. Den 26 mars var all virus utrensad och alla tekniska säkerhetsåtgärder vidtagna.

Journalsystembortfall inom Stockholms läns landsting

Den 18 december 2008 uppstod problem med åtkomsten av framförallt det elektroniska patientjournalsystemet TakeCare. Svarstiderna blev onormalt långa och det ledde i ett senare skede till att vissa patientdata gick förlorade. Detta medförde säkerhetsrisker vid undersökning och behandling av patienter. Intranätet var ostabilt.

Stabsläge enligt Karolinska Universitetssjukhusets katastrofplan intogs tidigt och möten i stabsgruppen hölls fortlöpande under den tid problemen förekom. Felsökning kunde starta kort efter att felet uppstått. Flera samverkande faktorer orsakade avbrottet i TakeCare. Lagringssystemet SAN var överbelastat och övervakningen var inte tillfredsställande. När man med hjälp av en säkerhetskopia skulle återska-

pa databasen fungerade inte detta. Dessutom låg transaktionsloggen[1] på det krånglande lagringsutrymmet och kunde därför inte användas. De uppgifter som registrerats i patientjournalsystemet under cirka två timmar kunde därför inte återskapas.

Systemet stod stilla i 25 timmar och var åter i drift 20 december.

Haveri i serverhall i landstinget i Kalmar län

På morgonen kl. 06:20 den 14 augusti 2008 nödstoppades majoriteten av landstingets 240 IT–system. Detta berodde på att temperaturen steg okontrollerat i en datorhall. Hälso- och sjukvården förlorade kontakten med alla vårdinformationssystem, inklusive patientjournalerna. Driftstoppet varade fram till cirka klockan 12 samma dag.

Orsaken till temperaturstegringen var att ett motorskydd utlöst i en fläktmotor i kylanläggningen. Det fanns två parallella kylsystem som vid problem i det för tillfället aktiva systemet automatiskt skulle växla över kylfunktionen till det andra. Att denna övergång inte skedde berodde på en felprogrammering av styrsystemet. Skiftningen till det fungerande systemet fick göras manuellt av inkallad driftpersonal.

Efter händelsen installerades dubbla och av varandra oberoende temperaturövervakningar och styrsystemet omprogrammerades. En ny serverhall på annan ort skapades och där placerades kopior av de kritiska IT-systemen. Dessutom placerades läskopior av patientjournalsystemet Cosmic på alla tre sjukhusen i landstinget.

Bildhanteringssystem i landstinget i Uppsala län

År 2004 togs ett landstingsbeslut att alla medicinska bilder skulle kunna läsas från patientjournalsystemet Cosmic. Senare samma år beslöts också att befintligt bildsystem, RIS/PACS/bildarkiv, skulle ersättas. Av olika skäl påbörjades inte installationen av bildsystemet förrän under februari 2007. Innan det nya systemet var driftsatt gjordes ingen uppgradering av det gamla bildsystemet. På grund av en alltmer ökande tröghet i det gamla systemet driftsattes det nya systemet under oktober 2008 innan alla tester var klara. Detta ledde till problem med funktion och säkerhet under slutet av 2008 och 2009 och ett totalt stopp inträffade den 3 februari 2009. Alla bilder försvann.

1 Transaktionslogg är löpande registrering av transaktioner i en databas som möjliggör spårning av vilka händelser som förekommit. Med hjälp av transaktionsloggen kan man återställa databasen om den skulle skadas.

Efter en utdragen felsökning gjordes en total ominstallation av bildsystemet. De förlorade bilderna kunde återskapas. Orsaken till problemen visade sig vara ett unikt fel i säkerhetskopieringen.

Integrationen av Cosmic i verksamheten var inte genomförd vid utgången av 2010.

Erfarenheter

I detta avsnitt anges inte referenser till författningar, standards eller andra relevanta dokument. Dessa uppgifter återfinns i stället löpande i texten i de följande kapitlen.

1. **Vårdgivarna har ett övergripande ansvar för informations- och IT-säkerheten.** Erfarenheterna från de beskrivna händelserna visar att kvalitetsledningssystemen måste innehålla mer av aktiv styrning och uppföljning av vårdgivarens patientkritiska IT-system. De standarder som finns om säkerhetstekniker och ledningssystem för informationssäkerhet bör användas. Ytterligare ledning för att skapa en god informations- och IT-säkerhet finns i Socialdepartementets skrift om nationell IT-strategi för vård och omsorg och i Socialstyrelsens slutrapport om nationell informationsstruktur. Den tidigare krisberedskapsmyndigheten KBM har systematiskt granskat sårbarheten i IT-system i sin temaserie. Det finns således mycket kunskap om hur man kan skapa en säker IT-verksamhet.
2. **Katastrofplanen** för ett sjukhus eller landsting/region måste beskriva förfarandet vid störningar i organisationens informationssystem som begränsar sjukhusets möjlighet att upprätthålla normala medicinska kvalitetskrav. Erfarenheterna i de beskrivna fallen visar att förlust av eller avbrott i förbindelsen med patientjournaler och andra IT-baserade vårdinformationssystem kan medföra betydande risker för patientsäkerheten. Störningar i IT-system bör därför med automatik medföra att beredskapsnivån höjs. Gör man inte det finns risk att organisationen aldrig hinner i fatt om störningarna blir omfattande. Om det i ett senare skede visar sig att incidenten inte är allvarlig kan beredskapsnivån sänkas och den ordinarie underhållsfunktionen åtgärda störningen.
3. När det inträffar störningar i försörjnings- och informationssystemen är det viktigt att snabbt **informera nyckelfunktioner** enligt beredskapsplan om störningens omfattning och när man beräknar att ordinarie system åter kan vara i drift. Dessa funktioner avgör när man ska övergå till reservrutiner. Organisationen måste planera för att kunna

sprida information om de elektroniska informationskanalerna (intranät, telefoner, fax, sökare) inte fungerar.

4. Skyddet mot skadlig kod – **e-virus** – måste kontinuerligt uppdateras. Skydd och system för autentisering måste kontinuerligt och utan dröjsmål hållas aktuella. Säkerhetspatchar och programuppgraderingar som utges av tillverkarna måste installeras omgående.
5. Det måste finnas **strikta regler** som anger villkor för att få ansluta datorer, medicinteknisk utrustning och externa enheter, till exempel USB-minnen, till organisationens nätverk. Med interna regelbundna kontroller måste organisationen förvissa sig om att alla användare rättar sig efter dessa regler.
6. **Tillverkarnas ansvar** för skyddet mot virus i medicinteknisk utrustning som innehåller datorfunktioner måste beskrivas tydligt i upphandlingsavtal och i avtal om underhåll. Avtalen måste också precisera vilka åtgärder av detta slag som kundens serviceorganisation får göra utan att tillverkaransvaret överflyttas till användaren.
7. Då **externa eller interna leverantörer** anlitas för drift och underhåll av såväl IT- som medicintekniska system (MT-system) är det viktigt att ansvarsförhållandena blir tydliga i de avtal som upprättas. Detta är särskilt viktigt då flera aktörer är inblandade. Systemägarens krav på IT-systemens tillgänglighet måste utgå från sjukvårdens behov. Leverantörens organisation, bemanning och beredskap för olika underhållsinsatser måste definieras i avtalen mellan kunden/vårdgivaren och säljaren/leverantör .
8. **Dataprogram** som är avsedda att användas för samma syften som en medicinteknisk produkt ska betraktas och bedömas som en sådan. Detta får två konsekvenser, dels ska dataprogram för dessa ändamål som inköps från kommersiella tillverkare bedömas och hanteras i enlighet med gällande författningar för medicintekniska produkter, dels ska sådana program som skapas inom sjukvården genomgå en egentillverkningsprocedur vid konstruktionen som syftar till att göra programmet säkert på samma sätt som det krävs av en kommersiell tillverkare. Vårdgivaren ansvarar för att det finns rutiner för egentillverkning av medicintekniska produkter.
9. **IT- och MT-enheterna måste samverka** eftersom deras respektive ansvarsområden alltmer integreras. Behovet av samarbete blir uppenbart när problem med intranäten uppstår eftersom nätverksansluten medicinteknisk utrustning kan påverkas och patienterna därmed utsättas för risker.

Inledning

Med anledning av det ökande antalet IT-haverier som har drabbat hälso- och sjukvården har Socialstyrelsen beslutat att skriva en tematisk Kamedo-rapport om IT-haverier och de lärdomar och erfarenheter som kan dras därifrån.

Hälso- och sjukvården är i hög grad beroende av en fungerande informationsteknik. Störningar och avbrott påverkar ekonomin men framförallt patientsäkerheten negativt.

Till Socialstyrelsen inkommer anmälningar enligt lex Maria när störningar i IT-system orsakat eller kunnat orsaka allvarliga skador på patienter. Sjukvården drabbas dock av långt fler problem med IT-systemen än vad som anmäls. I denna rapport redovisas fyra helt olika typer av störningar i IT-system som inträffat i svensk sjukvård under perioden 2008-2009. Tre av dessa har anmälts till Socialstyrelsen enligt lex Maria.

De störningar som presenteras i denna rapport är:

- e-virusangrepp i Region Skåne
- Journalsystemsbortfall inom Stockholms läns landsting
- Haveri i serverhall på Länssjukhuset i Kalmar
- Införandet av bildsystem i landstinget i Uppsala län

Det är fyra typhändelser som väl illustrerar vad som kan hända, konsekvenser och möjliga åtgärder som minskar risken för upprepning.

Informationsteknik, IT-strategi, informationsstruktur, informationshantering, informationssäkerhet, IT-säkerhet är alla begrepp och uttryck som används i standards – internationella och nationella – och andra dokument som beskriver detta område. Det finns standards för ledningssystem för informationsteknik avsedda för hälso- och sjukvården och det finns lagar och myndighetsföreskrifter som reglerar informations- och IT-tekniken. Socialdepartementet har tagit fram en nationell IT-strategi och Socialstyrelsen en slutrapport om den nationella informationsstrukturen. Vårdgivarna ska ge direktiv och säkerställa att ledningssystemet för varje verksamhet är ändamålsenligt med mål, organisation, rutiner, metoder och vårdprocesser. Ytterligare ledning i IT-säkerhetsarbetet finns i KBM:s temaskrift om IT och sårbarhet.

Inom den offentliga sjukvården finns vanligen en på landstingen centralt placerad IT-verksamhet med driftansvar för landstingets intranät och de

gemensamma administrativa IT-systemen. Den medicintekniska verksamheten är oftast organiserad som medicintekniska enheter på sjukhusen i landstingen. Den organisationsformen har uppkommit ur vårdens behov av att ha nära tillgång till medicinteknisk expertis. Ett nära samarbete mellan dessa två teknikfunktioner är nödvändigt för att upprätthålla en god patientsäkerhet.

Patientjournaler och andra vårdinformationssystem kommuniceras idag över sjukvårdens intranät och i en framtid troligen också över Internet. Bildarkiv för röntgen, ultraljud och andra bildgivande system med krav på stora digitala lagringsutrymmen placeras centralt i nätverket och är åtkomligt för behörig vårdpersonal. Utvecklingen går mot fler vårdinformationssystem som ska vara tillgängliga för flera enheter. I gruppen medicintekniska produkter finns både avancerade och enkla apparater som innehåller datorfunktioner. En del av dessa kopplas ihop med andra utrustningar eller med arbetsstationer via datanätverk. Sjukhusens intranät utnyttjas ofta för detta ändamål.

De områden som har studerats i denna rapport är den beredskap att hantera allvarliga IT-haverier som funnits landstingens och sjukhusens katastrofplaner och hos de organisationer som har driftansvaret för IT-systemen. Vidare beskriver rapporten händelseförloppet samt skador och störningar som uppstått i den sjukvårdande verksamheten. Uppgifter om akuta och långsiktiga åtgärder samt bakomliggande orsaker har inhämtats. Särskilt har observerats om man har kompletterat katastrofplanerna eller på annat sätt vidtagit åtgärder på ledningsnivå för att skapa säkrare IT-system. De tekniska delarna i händelseförloppet och de tekniska åtgärderna för att återställa funktionerna beskrivs i rapporten men gör inte anspråk på att vara utförliga i detalj.

Det är författarnas uppfattning att man efter de inträffade IT-haverierna på alla håll aktivt och grundligt har arbetat med att göra IT-systemen driftsäkrare och att handlingsplaner tagits fram för att minska konsekvenserna vid framtida störningar i IT-systemen.

Risk (hot och sårbarhet)

Med *informationssäkerhet* avses i denna rapport säker hantering av information med avseende på önskad tillgänglighet, kvalitet, sekretess och *spårbarhet.* IT-säkerhet är den delen som avser den tekniska hanteringen av information som bearbetas, lagras och kommuniceras elektroniskt samt administrationen kring denna. När man diskuterar informations- och IT-säkerhet är det lämpligt att skilja på hot och sårbarhet. Begreppet sårbarhet härstammar från interna svagheter och brister i infrastrukturen, såväl separata som sammansatta i större system. *Hot* har sitt ursprung i att brister i systemkonstruktionen kan medföra att oförutsedda eller medvetet accepterade risker kan påverka informationen negativt. Dessa definitioner av begreppen är hämtade ur KBM:s temaserie 2003:5 om IT och sårbarhet [1].

De nedan beskrivna riskerna i IT-system är exempel på både sårbarheter och hot. Exemplen är till största delen grundade på erfarenheter från händelser som inträffat i hälso- och sjukvården.

Beroenden av vårdnära IT-system

Hälso- och sjukvården är starkt beroende av informationssystem. Den mesta informationen är numera lagrad i databaser på servrar. Registrering, åtkomst och bearbetning av data sker huvudsakligen via datanätverk. I denna rapport används benämningen IT-system som ett samlande begrepp för servrar, datanätverk, lagringsutrustning, arbetsstationer, programvara samt registrerade data.

Grundläggande och avgörande för patientsäkerheten är att data som registrerats är åtkomliga av behöriga, att de inte förändras eller förstörs av IT-systemen och att sekretessen upprätthålls.

IT-system som kommunicerar med varandra över fasta eller tillfälliga förbindelser är beroende av säkra nätverk. Som exempel kan nämnas att man från ett patientjournalsystem kan skicka remisser över nätverket till andra vårdenheter för medicinska åtgärder. Därefter kan remissvar, utlåtande och andra data erhållas över nätverket. Radiologiska bildsystem och laboratoriesystem har etablerade funktioner med denna teknik.

Hemsjukvården utvecklas och alltmer avancerad vård kan skötas i hemmet med hjälp av medicinteknisk utrustning som kan kommunicera med sjukvården. Utvecklingen av denna vårdform är i hög grad beroende av fungerande datakommunikationer.

Patienter vårdas av olika huvudmän under olika tidsperioder. Den vårdinformation som är nödvändig för fortsatt god vård överförs oftast mellan vårdgivarnas IT-system. Patientsäkerheten är således beroende av säkra förbindelser och rutiner. Kommunikationen mellan de olika vårdsystemen sker då ofta över allmänna kommunikationsnät.

Bokning av och utskrift av kallelse till undersökning och behandling av patienter sker i IT-system. Debiterings- och betalsystem kan vara kopplade till bokningssystemen.

Akutsjukvården har stora krav på snabb tillgång till vårdinformation alla tider på dygnet. När en akutpatient inkommer till sjukhuset kan det vara avgörande för utgången att ha uppgifter tillgängliga om patientens läkemedel, eventuella överkänslighetsreaktioner eller sjukdomar.

Sjukvårdens planering av sin dagliga verksamhet sker i allt större omfattning med hjälp av datorbaserade program.

Patienten blir alltmer involverad i informationsflödet och får tillgång till sin egen journal över internet eller med hjälp av annat IT-stöd. Tidbokning kan göras av patienterna över internet. Denna funktion är under uppbyggnad och kompletterar nuvarande metoder med bokning över telefon eller per brev. Detta innebär att systemen måste kunna garantera individens integritet och att information enbart ska vara tillgänglig för den som behöver den och som har individens samtycke att informationen får delges.

Beroende av infrastruktur i övrigt

Patientsäkerheten kan påverkas av andra IT-systems påverkan på infrastrukturen. Som exempel kan nämnas att om de IT-baserade styrsystemen för elförsörjningen inte fungerar vid ett strömavbrott så kan det medföra att reservkraften inte startar. Det innebär att medicintekniska produkter och IT-system enbart fungerar så länge det finns någon form av avbrottsfri kraft (Uninterruptible Power Supply/Source, UPS).

Telefonsystemen förändras och ansluts till och ingår i stora IT-system och blir därmed alltmer beroende av dels elförsörjning på alla nivåer, dels IT-systemens egen driftsäkerhet. Haverier i sådana IT-system kommer inte att behandlas i denna rapport.

Hälsoekonomi

I en risk- och sårbarhetsanalys av IT-system bör, utöver de rent patientsäkerhetsmässiga effekterna av en störning, även samhällsekonomiska överväganden beaktas. Ett IT-haveri kan innebära att patienter måste förlänga sin sjukskrivningstid och därmed ha rätt till stöd av de offentliga och pri-

vata sjukvårdsförsäkringssystemen. Arbetsgivare kan tvingas att försöka hitta ersättare för en sjukskriven medarbetare.

En annan konsekvens av att IT-systemen inte fungerar är att patienter måste ta ledigt fler gånger från sitt arbete för att undersökningar och att behandlingar inte kan genomföras som planerat.

Störningar och avbrott i IT-system medför att vårdpersonal på flera nivåer drabbas av merarbete, dels under störningen när alternativa metoder måste användas, dels med att registrera de uppgifter som under störningen noterats på andra sätt när IT-systemen åter är i funktion. Detta medför kostnader för personalens extra arbete. Dessutom leder störningarna ofta till utgifter för extern servicepersonal och för investeringar i driftsäkrare teknik.

Tillgänglighet

Frågor som uppkommer vid riskbedömning är: Vilken tillgänglighet kan och ska ett modernt samhälle kräva av IT-systemen? Vilka avbrottstider kan accepteras? Vilken upptid[2] kan vi kräva av ett IT-system som vi önskar ska fungera 24/7, det vill säga alltid? Dessa frågor bör koordineras med den Nationella IT-strategin[3] [2], och det internationella arbete som sker inom EU där sjukvården ska kunna nå väsentlig information från kritiska system. Utvecklingen inom sjukvården går mot att viktig information om patienten måste finnas tillgänglig för alla som är inblandade i vården oberoende av vilken vårdgivare som för tillfället har vårdansvaret.

För att göra bilden ytterligare något mer komplicerad så trädde det reviderade medicintekniska direktivet i kraft den 21 mars 2010 [3 och 4] vilket medför att medicinska informationssystem som påverkar patientsäkerheten räknas som medicintekniska produkter och ska därför uppfylla direktivets väsentliga krav, det vill säga kraven på säkerhet och effektivitet. Här har Läkemedelsverket arbetat fram en rapport för att belysa frågeställningen och ge förslag till riktlinjer [5].

---

2 Upptid är den tid som systemet är tillgängligt enligt specifikation.

3 Sverige har antagit en Nationell IT-strategi för att lösa och effektivisera IT-användningen i samverkan med alla aktörer inom vården. Med hjälp av IT som ett strategiskt verktyg ska förutsättningarna för en säker, tillgänglig och effektiv vård och omsorg bli bättre.

Bakgrund

Situationen före händelsen

E-virusangrepp i Region Skåne

Region Skånes nätverk (Skånet) är ett regionalt nät som år 2009 bestod av cirka 21 000 PC-arbetsplatser för administrativa ändamål och cirka 1 300 servrar/kluster. Till detta kom 3-4 000 datorer i medicintekniska produkter och datorer som universitetets forskare anslutit till nätverket. Därutöver kopplades externa minnesenheter, såsom USB-minnen, in på datorer anslutna till nätet.

Via nätet kunde man även ansluta till Internet, Sjunet[4] och distansarbetsplatser. Säkerheten hanterades primärt genom ett skalskydd bestående av centrala brandväggar men det fanns även en regional standard för virusskydd och säkerhetsuppdateringar. Detta gällde dock inte datorer i medicintekniska produkter.

Nätet var fullt redundant med olika kabelvägar till alla tolv inkopplade sjukhus. Vissa system hade full redundans i enlighet med den avtalade tillgängligheten. Nätverket hade en grundkapacitet av 1 Gb/s i stamnätet. Merparten av anslutningshastigheten för användare var 100 Mb/s men det förekom även 10 Mbit/s.

Regler och instruktioner för anslutning av datorer, medicinteknisk utrustning, externa minnesenheter med mera fanns och kunde läsas på intranätet av alla anställda inom regionen.

Informationstekniktjänster i Region Skåne (ITT) var benämningen på Region Skånes centrala IT-förvaltning vid tiden för den aktuella händelsen. ITT förvaltade och ansvarade för driften av IT-infrastrukturen och de administrativa applikationerna. Universitetets datorer förvaltades också av ITT med undantag av de datorer som forskare anskaffade på forskningsanslag. De datorer som ingick i medicintekniska tillämpningar/ utrustningar förvaltades av de lokala medicintekniska avdelningarna på respektive sjukhus.

Journalsystemsbortfall inom Stockholms läns landsting

Vårdinformationssystemet TakeCare används vid Karolinska Universitets-

[4] Sjunet är ett kommunikationsnät för vård och omsorg skilt från Internet. Nätet används för videokonferenser, överföring av patientjournaler, e-recept, röntgenbilder med flera.

sjukhuset Solna och Huddinge, S:t Eriks Ögonsjukhus, Södertälje sjukhus, vårdcentraler, geriatriska och psykiatriska sjukhus och avdelningar samt i kommunal och privat vård inom hela Stockholms läns sjukvårdsområde (SLSO). Det används även på Visby sjukhus, samt på vårdcentraler och i kommunal vård på Gotland. TakeCare används av mer än 1100 vårdenheter och innehåller patientdata för cirka 1,6 miljoner individer. Ofta är upp till 10 000 användare samtidigt uppkopplade till TakeCare.

Stockholms läns landsting (SLL) har en gemensam IT-verksamhet (SLL-IT) och sjukhusen är tillsammans med bland annat Hälso- och sjukvårdsnämnden beställare av IT-tjänster. Karolinska Universitetssjukhuset hade emellertid en egen IT-funktion, benämnd IT-Forum fram till årsskiftet 2008/2009. Vid Karolinskas två sjukhus Solna och Huddinge fanns under 2008 cirka 180 IT-system som IT-Forum hade driftansvar för. TakeCare var ett av dessa system. Från och med 2009 övertog SSL-IT ansvaret även för Karolinska Universitetssjukhusets alla IT-System.

Beställarrollen för TakeCare är dock centraliserad till Centrum Samverkan TakeCare (CSTC) som är organisatoriskt knuten till Karolinska Universitetssjukhuset. CSTC är en stab som arbetar praktiskt med att driva och förvalta TakeCare. Företaget ProfDoc Care AB är leverantör av vårdinformationssystemet TakeCare.

Den primära installationen finns på en server på Karolinska i Huddinge, vilket innebär att TakeCare normalt körs på denna. Den sekundära installationen finns på en server på Karolinska i Solna. All registrering av data till TakeCare görs parallellt till båda servrarna och lagras i var sitt Storage Area Network (SAN) bestående av ett nätverk med lagringsenheter (hårddiskar, bandstationer) och ett system för säkerhetskopiering. Företaget Dell var leverantör av det aktuella SAN:et till SSL. Om den primära installationen i Huddinge är ur funktion kan Solna-servern ta över driften. Detta övertagande sker dock inte automatiskt utan måste göras av en IT-tekniker efter bedömning av situationen. Mellan dessa två servrar finns två geografiskt skilda fasta fiberförbindelser. Dessutom kan även SSL-net användas i ett krisläge.

För att inte förlora information om varje patients läkemedelsordinationer vid driftstörningar i TakeCare har ett separat program för säkerhetskopiering utvecklats, kallat läkemedelsbackup (LM-backup). Detta program och TakeCare ska vara installerat på en särskilt utvald, märkt och stationär dator på varje avdelning som använder TakeCare. Datorn startas om en gång per dygn och läkemedelslistor i TakeCare på inskrivna patienter kopieras till den lokala datorn och sparas. Vårdenheterna har själv ansvar för att skapa en rutin för detta. Till datorn är en lokal skrivare ansluten. Datorn och skrivaren ska vara kopplade till eluttag för reservkraft.

När problemen med TakeCare inträffade på morgonen den 18 december 2008 hade IT-personal under natten flyttat ett annat IT-system (Echopac) till det ena av de två SAN som TakeCare använder. I samband med detta arbete utökades lagringskapaciteten i SAN:et. Expansionen genomfördes utan problem.

Haveri i serverhall på Länssjukhuset i Kalmar

Vid Länssjukhuset i Kalmar fanns två serverhallar, en i hus 17 och en i hus 18. Serverhallen i hus 18 innehöll landstingets alla gemensamma IT-system medan serverhallen i hus 17 innehöll servrar och lagringssystem för säkerhetskopiering. All information som lagrades i systemen i hall 18 kopierades över till ett lagringssystem (SAN) i hall 17. Här gjordes kopior av vårdinformationssystemet Cosmic. Denna backup var dock i sin tur kopplad till en bandrobot[5] som var placerad i serverhallen i hus 18. Man var medveten om att det inte var full redundans i IT-systemen eftersom ett uppkommet fel i hall 18 skulle innebära att man först var tvungen att åtgärda detta problem innan återläsning från kopior i hall 17 skulle kunna göras.

Vid sjukhusen i Oskarshamn och Västervik hade man fram till maj 2008 läskopior av innehållet i Cosmic. Då ansåg dock landstingets IT-förvaltning att uppdateringen av dessa databaser inte var tillräcklig snabb, en fördröjning på 15-20 minuter ansågs äventyra patientsäkerheten, och beslutade därför att ta bort dessa läskopior. Något annat system för säkerhetskopiering skapades inte.

För dataförbindelsen mellan sjukhusen i landstinget används Telias nätverk med näst intill dubblering. Till hälsocentralerna, tandvården och andra perifera enheter finns separata, men inte dubblerade förbindelser. De lokala nätverken på sjukhusen är till stor del dubblerade. Nätet till serverhallarna är dubblerade.

Serverhallen i hus 18 försörjdes med ventilation och kyla av två återcirkulationsaggregat för att hålla temperatur och fuktighet inom tillåtna gränser. Dessa aggregat växlade i drift två gånger per dygn. Aggregaten fungerade också som varandras reservsystem för att öka den totala driftsäkerheten. Aggregaten var placerade i var sin del i ett apparatskåp och matades från olika kraftsystem. Det ena aggregatet elförsörjdes från ett dieseldrivet reservkraftaggregat (prioriterad kraft) och det andra från det allmänna elnätet (oprioriterad kraft). Varje apparatskåpsdel hade övervakning av inkommande elförsörjning. De två aggregaten övervakades och

[5] Bandrobot är en ”intelligent” säkerhetskopieringsenhet som byter och katalogiserar band som används för säkerhetskopiering av elektronisk data. Typiskt består en bandrobot av ett bandbibliotek, ett antal bandstationer och en mekanisk arm som kan byta band. [Wikipedia]

styrdes av ett gemensamt styrsystem. Detta i sin tur strömförsörjdes med avbrottsfri kraft, UPS.

Kylt vatten tillfördes systemet alternativt från kylanläggningar i två olika byggnader. Växling mellan dessa skedde automatiskt om kylvattnet fick för hög temperatur. Det fanns även en möjlighet att förse cirkulationsaggregaten med kyla via tappkallvatten om ingen av kylanläggningarna fungerade.

Mätgivare för luftkvalitet och temperatur fanns i serverhallen och var kopplade till styrsystemet. Vid mätvärden från givarna som låg utanför givna toleransgränser utlöstes larm. Dessa larm har olika prioritet (benämnt klasser i larmsystemet) och i driftpersonalens rutiner angavs vilka åtgärder som skulle vidtas. Se vidare under Beredskap, detta kapitel.

Elförsörjningen av IT-utrustningen i serverhallen skedde via två UPS:er på 63 kW. Den ena UPS:en matades med reservkraft och den andra med oprioriterad kraft. Växling till alternativ matning skedde automatiskt om matande spänning försvann. UPS:erna var konstruerade så att de vid ett eventuellt laddningsavbrott hade möjlighet att mjukvarumässigt styra ner serverutrustningen. Denna funktion var dock inte driftsatt.

Vårdinformationssystemet Cosmic med modulerna Läkemedel, Vårddokumentation samt Remiss och Svar användes vid de tre sjukhusen i landstinget. I primärvården användes Swedestar patientjournalsystem och inom Folktandvården används tandvårdsprogrammet T4. Drift och underhåll av Cosmic sköts av en särskild grupp inom landstingets IT-förvaltning. Här finns också den formella systemägaren och styrgruppen för Cosmic.

Redan år 2007 diskuterades en dubblering av kylsystemen i serverhall 18 i Kalmar och en preliminär kostnadsberäkning gjordes. IT-förvaltningen förutsåg att värmebelastningen skulle öka under den närmaste framtiden på grund av att allt fler IT-system installerades. Under våren 2008 fördes också samtal mellan landstinget och ett externt el-företag om att inrätta en ny serverhall på Länssjukhuset i Kalmar.

Bildhanteringssystem i landstinget i Uppsala län

Landstinget i Upplands Län beslutade i juni 2004 att alla bilder som skapades med röntgen, ultraljud, PET-CT och andra bildgivande system skulle kunna ses via patientjournalsystemet Cosmic. Det fanns vid den tiden inte något annat sjukhus i världen där detta fungerade. I november samma år togs beslutet att upphandla ett för hela landstinget gemensamt system för registrering, hantering och arkivering av bilder från alla typer av bildgi-

vande källor (RIS[6]-PACS[7]-Arkiv). Avsikten var att det nya bildhanteringssystemet skulle vara på plats och i full funktion under 2005. En styrgrupp under ledning av landstingets chefläkare skapades för att leda projektet. I denna ingick bland andra verksamhetscheferna för de olika röntgenenheterna i landstinget.

Efter beslutet att upphandla ett nytt gemensamt RIS-PACS-Arkiv för hela landstinget gjordes ingen uppgradering av det befintliga RIS-PACS.

I december 2005 antogs en leverantör till bildsystemet och avtal tecknades under juni 2006. Man planerade att införa systemet från och med mars 2008. Emellertid påbörjades inte installationen förrän under oktober 2008. Det blev således en försening på cirka 3 - 3,5 år från planerad leverans till faktiskt införande.

Kontakt togs under våren 2008 med Socialstyrelsens regionala tillsynsenhet på grund av de allt större problemen med det gamla och tröga bildsystemet. Socialstyrelsen besökte Akademiska sjukhuset i Uppsala för att bli informerad om situationen. Man framhöll då att man förväntade sig att det fanns fungerande reservrutiner så att patientsäkerheten skulle kunna upprätthållas. Man diskuterade också om en lex Mariaanmälan skulle göras. En bidragande orsak till problemen var att antalet bilder ökade från 0,5 miljon till 44 miljoner under loppet av ett fåtal år.

Det nya PACS-systemet bestod av två servrar. En applikationsserver och en databasserver. Till dessa var en bildlagringsdatabas kopplad som en gemensam resurs. I händelse av driftbortfall av applikationsservern skulle databasservern kunna ta över applikationsserverns arbetsuppgifter. Applikationsservern och databasservern övervakar varandra med hjälp av en så kallad *heartbeat*-mekanism vilken fungerar så att respektive server med jämna intervall anropar grannen för att få bekräftat att den är i aktiv drift. Om *heartbeat* uteblir ska grannen anses vara ur drift och konstaterande server ta över.

Utöver PACS:s gemensamma bildlagringsdatabas fanns ett nytt långtidsarkiv anslutet. I arkivet lagras alltid allt bildmaterial och alla undersökningsdata. Undersökningar som för tillfället inte finns lagrade i PACS hämtas därifrån, i huvudsak historiska data. Efter att data hämtats från arkivet lagras det en tid i PACS för att snabbt vara tillgängligt om data behövs igen. I PACS-databasen som sådan är riktmärket att de senaste tio månadernas undersökningar alltid ska finnas direkt tillgängliga. Äldre undersökningsdata raderas undan för undan ur PACS och hämtas sedan vid behov från långtidsarkivet.

---

6 **R**öntgen **I**nformation **S**ystem

7 **P**icture **A**rchiving and **C**ommunication **S**ystem

Den gemensamma bildlagringsdatabasen kopierades två gånger dagligen till applikationsdatabasen och till databasservern.

Beredskap

Region Skåne

Region Skånes övergripande regionala kris- och katastrofplan från 2007 beskrev regionens uppgifter när det gäller händelser såsom stor olycka, katastrof, extraordinär händelse, samt höjd beredskap och väpnat angrepp. Den regionala medicinska katastrofledningen (RMKL) ingår som en del i den övergripande planen. Kris- och katastrofplanen innehöll inte några tydliga instruktioner om hur störningar i de gemensamma IT-systemen skulle hanteras. Det fanns inga instruktioner för hur och när Informationstekniktjänster i Region Skåne (ITT) skulle informera krisledningen när störningar inträffar. Däremot angavs i planen att ITT skulle informeras och involveras när någon av planens beredskapsnivåer aktiverades.

Tjänsteman i beredskap TiB ingår i den regionala medicinska katastrofledningen (RMKL). TiB larmas genom SOS Alarm. För att hantera information om interna problem och händelser som kan ha betydelse för samverkan i sjukvården inom regionen finns en kommunikatör i beredskap (KiB). Enligt den då gällande kriskommunikationsplanen ska TiB larma KiB vid allvarlig händelse eller kris. KiB etablerar därefter kontakt med ansvariga inom berörda förvaltningar och externa parter beroende på händelsens allvarlighetsgrad.

ITT hade tre beredskapslinjer: nätverk och kommunikation (inkl brandväggar), serverinfrastruktur (inkl drift av serverhallar) och applikationsdrift avseende centrala och lokala applikationer, databaser och inloggningssystem. Inställelsetiden var två timmar från påringning från centrala Helpdesken som var öppen dygnet runt.

Stockholms läns landsting

Katastrofplanen 2007 för Karolinska Universitetssjukhuset Solna och Huddinge innehöll instruktioner om att chefläkarorganisationen och katastrofkommittén skulle informeras av IT-Forum vid IT-incidenter av större karaktär. Men katastrofplanen är skriven så att denna information ska ske när den efterfrågas av chefläkaren eller katastrofkommittén. Någon motsvarande skyldighet för IT-Forum att på eget initiativ informera katastrofkommittén var inte inskriven i katastrofplanen.

På IT-Forum fanns en beredskapsplan mellan systemägaren TakeCare och IT-Forums driftavdelning. På icke kontorstid hade IT-personal bered-

skap i hemmet, kallad Framjouren. Användare kunde ringa till Framjouren vid problem. Framjouren kontaktade sedan den IT-tekniker i beredskap som hade rätt kompetens för att lösa uppkomna problem. För TakeCare fanns en särskild överenskommelse om tillgänglighet. Kopplingen mellan sjukhusets katastrofplan och IT-Forums beredskapsplan fanns men var otydlig. Inte heller fanns någon plan för samordnad informationsspridning i händelse av störning i IT-systemen.

För vårdenheterna fanns inga gemensamt framtagna riktlinjer eller instruktioner om hur personalen skulle agera om IT-systemen upphörde att fungera och inte heller hur man skulle kontakta ansvariga om ett stort fel inträffade i kommunikationssystemen. Däremot fanns en rutin att använda läkemedelsbackupen i TakeCare för att spara läkemedelslistorna i händelse av avbrott i TakeCare-systemet. Det avgjordes på klinik- och avdelningsnivå om denna rutin skulle användas.

Landstinget i Kalmar län

I landstingets katastrofplan för 2008 fanns inte några instruktioner om hur störningar i de gemensamma IT-systemen skulle hanteras.

Larm vid driftstörningar i fastighetsanknutna system går till Landstingsfastigheters jourorganisation. Vid larm med högsta prioritet (benämnt klass A) från styr- och övervakningssystem i serverhallen inkallas Landstingsfastigheters jourpersonal direkt. De har en maximal inställelsetid på 45 minuter. Vid larm, som har lägre prioritet (klass B), tas problemet om hand endast under dagtid.

Landstingets IT-förvaltning hade inte någon jourverksamhet 2008, vilket innebar att problem med IT-systemen endast kunde anmälas till och bedömas av IT-service under kontorstid.

Landstinget i Uppsala län

I den regionala katastrof- och beredskapsplanen i landstinget i Uppsala län från 2005 konstaterades att i stort sett all verksamhet i landstinget är beroende av ständigt fungerande IT-stöd. Däremot fanns det inte någon handlingsplan för hur katastroforganisationen ska agera vid störningar i patientkritiska IT-system.

Den lokala katastrofplanen för Akademiska sjukhuset i Uppsala innehöll inte heller någon handlingsplan för åtgärder i händelse av störningar i IT-systemen.

När problem med IT-systemen uppträder kontaktas Medicinsk Informatik och Teknik (MIT), som är landstingets resurs för drift och underhåll av landstingets IT-system. MIT har två beredskapslinjer, en för bildsystemet

inom Bild- och funktionscentrum (BFC) och en för patientjournalsystemet Cosmic. För dessa system gäller att felsökning ska påbörjas inom högst 2 timmar under alla tider på dygnet 365 dagar om året.

När de i denna rapport beskrivna problemen med det gamla bildhanteringssystemet blev alltmer frekventa och allvarliga tillsattes en krisgrupp för att kontinuerligt ta ställning till åtgärder. Chefläkaren ingick i krisgruppen. Möten hölls varje vecka kring aktuella problem. I krisgruppen planerade man också för vilka åtgärder som skulle vidtas vid oförutsedda händelser och avbrott som följd av den utdragna övergången till det nya bildsystemet och integrationen med Cosmic patientjournalsystem.

Händelseförlopp och akuta åtgärder

I detta kapitel beskrivs händelseförloppen och de akuta åtgärder som vidtogs i anslutning till händelserna för att återställa driften. Tidsangivelser och uppgifter är hämtade från händelserapporterna i handlingarna från respektive vårdgivare. I vissa moment har förklarande kommentarer lagts till. Även författarkommentarer förekommer för att uppmärksamma betydelsefulla omständigheter.

E-virusangrepp i Region Skåne 2009

Tidpunkt	Händelse	Åtgärder i det akuta skedet	Kommentar
3 januari	Besvär med övervakningsutrustningen på Thoraxkliniken intensivvårdsavdelning (THIVA) vid Universitetssjukhuset i Lund.		
4 januari	Stora svårigheter att koppla upp mot intranätet konstateras på flera ställen inom Region Skåne	Lokal medicintekniker kallas till THIVA på Universitetssjukhuset i Lund. Denne kontaktar i sin tur servicetekniker från leverantören av övervakningsutrustningen på THIVA. Felsökning påbörjas. Region Skånes IT-jour (ITT-jour) ser att det görs flera misslyckade inloggningsförsök mot regiondomänen. Nu misstänker man att det kan vara ett e-virusangrepp Kl. 23:00 läggs information om problemen ut på ITT:s driftinformationssida	Ingen misstanke fanns om virusangrepp på något av sjukhusen utan man arbetade utifrån fel på utrustningarna. Säkerhetsåtgärden att konton låstes när fel lösenord användes mer än fem gånger inträffade allt mer frekvent. När datorerna spårades såg ITT-jouren att dessa datorer inte hade något logiskt samband med kontona.

5 januari	Inloggningsproblem och begränsad eller obefintlig åtkomst till journalsystemet Melior, röntgensvar Kundrad, digital diktering och patientadministrativa system (PASIS) på Universitetssjukhuset i Malmö	När inte vårdinformationssystemen fungerar övergår man till manuella rutiner för att dokumentera uppgifter om patienter, läkemedel, remisser, labbsvar m.m.	***Författarkommentar:*** *Redan här borde regional och lokal krisledning ha aktiverats.*
	Problemen ökar på vissa av Region Skånes sjukhus, datanätet är långsamt , problem med uppkoppling till diagnostik- och laboratorienära arbetsstationer, e-post, Internet och andra gemensamma tjänster. E-viruset påverkar nu många användare och stör vårdproduktionen. Upp till 600 konton låses per 30 minuter.	ITT sätter samman en katastrofledningsgrupp bestående av tjänstgörande personal, tekniker och chefsläkare. ITT inför den s.k. ”snurran” vilket innebär att låsta konton låses upp efter 30 minuter. Detta ger användarna möjlighet att komma in på sina konton men öppnar samtidigt för nya angrepp från e-viruset vilket leder till att konton låses igen. ITT får informell information från en större leverantör om att de också har drabbats av e-virus. Leverantörens antivirusprogram har identifierat viruset och därför stängt ner sitt intranät.	Gruppen lyckades identifiera skadlig kod i ett USB-minne, men man fick inte någon respons av antivirusprogrammet. ITT lyckades dock isolera det och skickade koden för analys till företaget F-Secure i San Diego, USA.
5 januari		ITT-jour kontaktar Tjänsteman i beredskap (TiB) och Kommunikatör i beredskap (KiB) och informerar om inloggningsproblem på datorerna. KiB informerar om inloggningsproblemen via ITT:s hemsida. Informationen når emellertid inte vårdpersonalen.	TiB fick ingen information om virusangreppets omfattning och var inte heller medveten om dess effekt på patientsäkerheten. Någon ytterligare information gick därför inte ut till sjukhusen . ***Författarkommentar:*** *Detta illustrerar att ITT-jour inte hade full insikt i konsekvenserna för patientsäkerheten*.

6 januari		ITT erhåller kod för detektering och rensning av e-viruset W32/ Downadup.CM och stänger nu funktionerna Autorun och Autoplay på samtliga datorer inom regiondomänen. Avsikten är att förhindra spridning av e-virus genom olika minnen såsom USB och DVD.	ITT kunde inte påverka någon funktion på medicintekniska datorer/ produkter utan leverantörens godkännande. Leverantören ansvarar för produktens egenskaper vid avsedd användning i enlighet med det medicintekniska direktivet [3]
7 januari	Hässleholms sjukhus informerar TiB om problem med övervakningsutrustning. En patient flyttas till sjukhuset i Kristianstad. Endast Helsingborgs lasarett kan ta emot och tolka alla regionens ambulans-EKG då deras Mobimed[8] inte är angripen av e-virus.	TiB kontaktar ITT med anledning av problemen på Hässleholms sjukhus men blir hänvisad till regionens medicintekniska chef (MTC-RS). MTC-RS kontaktar lokalt medicintekniskt ansvarig på Hässleholms sjukhus.	
	30 % av regionens datorer och 50 % av dess servrar är infekterade av e-virus Upptäcks att cirka 1000 datorer inklusive medicintekniska utrustningar, som smittats av e-virus, inte har installerat den säkerhetspatch som Microsoft släppte i oktober 2008.	ITT informerar nu på bred front om virusangreppet och MTC-RS informeras via e-post att även medicintekniska produkter kan vara drabbade. Från och med denna dag hålls telefonkonferenser med alla förvaltningscheferna i regionen två gånger dagligen så länge som problemen varar.	Flera kanaler användes: - 1:a sidan på intranätet (långsam och tidvis otillförlitlig) - Telefon till alla förvaltningschefer (18 st) - Information i pressen - ITT:s egen hemsida
	Region Skånes telefonileverantör har problem med vidarekoppling och hänvisning av samtal.		
8 januari		ITT erhåller en ny virusdefinitionsfil från F-Secure.	
		MTC-RS informerar Läkemedelsverket och Socialstyrelsen om e-virusangreppet i Region Skåne	

9 januari		TiB sammankallar samordningsgrupp mellan ITT, medicinsk teknik och kommunikatör. Dagliga avstämningsmöten. MTC-RS informerar dagligen regionens produktionsdirektör.	
10 januari		TT skickar en CD med information om hur man rensar e-virus till MTC-RS. Den distribueras vidare till alla medicintekniska avdelningar i regionen.	
12 januari	Antalet smittade datorer ökar efter några dagars fallande trend.		Långledig personal kom åter i tjänst och startade sina datorer
15 januari		En större leverantör av röntgensystem beslutar att uppdatera sitt eget antivirusprogram och att installera Microsofts säkerhetspatch. Leverantören ger också instruktioner om hur virusskyddet kontinuerligt skall uppdateras.	
16–19 januari		Nya förbättrade virusdefinitionsfiler kommer från F-secure.	

[8] MobiMed är ett pre-hospitalt beslutsstödssystem, bestående av en mjukvara, som används i ambulanser och på sjukhus. Information om patienten och dess tillstånd matas in i MobiMed och utbyte av patientinformation mellan ambulanspersonalen och medicinsk expertis på sjukhuset möjliggörs. Ett beslut om direktintagning till primärvård, akutvård eller specialistvård kan därför tas redan under transporten

22 januari	En medicinteknisk dator blockeras under en pågående patientbehandling på Arythmilab på sjukhuset i Lund. Behandlingen var turligt nog inte inne i ett kritiskt skede, i så fall hade blockeringen medfört stor risk för allvarlig skada. Behandlingen kan återupptas när blockeringen hävs	ITT använder fjärrstyrning av den medicintekniska datorn för att rensa ut e-virus. Personal på Arythymilab lyckas efter flera minuter få kontakt med ITT och begära att fjärrstyrningen av datorn släpps.	Händelsen blir föremål för en särskild utredning och anmäls enligt Lex Maria till Socialstyrelsen
10 februari		Patientövervakningen på Landskrona lasarett kontrolleras och man upptäcker att leverantören inte har installerat säkerhetspatchen.	
8 januari – 26 mars		E-virus rensas ut, säkerhetspatchar installeras och antivirusprogram installeras och uppgraderas. Säkerhetspatchen i patientövervakningssytemet i Landskrona installeras.	Man hade kontakt med leverantörer av medicintekniska utrustningar för att framhålla deras ansvar.
26 mars		E-viruset är utrensat, IT-miljön uppdaterad och någon återsmitta är förmodligen inte längre möjlig.	

Journalsystemsbortfall inom Stockholms läns landsting 2008

Tidpunkt	Händelse	Åtgärder i det akuta skedet	Kommentar
18 december 09.40	Driftstörning i vårdinformationssystemet TakeCare uppstår och användare av TakeCare upptäcker att systemet inte fungerar		

09.45	Helpdesk får den första informationen från användare om driftstörningen		Inget larm från TakeCare-systemet erhölls eftersom det var trögt. TakeCare-förvaltningen CSTC larmades enligt lista. Man fick tag i 8:e personen på listan!
10.00		Kort information om driftstörningen läggs ut i en liten ruta ”Driftinformation” på SLSO:s hemsida. Information om avbrottet sprids internt på kliniker och enheter.	Sidan ser i övrigt ut som vanligt med mycket annat innehåll och informationen om driftstörningen missas av många.
		Chefläkaren beslutar att Karolinska ska övergå till stabsläge, dvs. lägsta beredskapsnivå enligt den lokala katastrofplanen	***Författar-kommentar:*** *Riktig åtgärd att tidigt inta stabsläge.*
10.00		Extern servicetekniker i serverhallen startar felsökning omedelbart. Arbetet inleds med att säkerställa en problemfri driftsmiljö och göra TakeCare-data tillgängligt för TakeCare-leverantören. Denne arbetar med att säkerställa TakeCare-data och att reparera skadade filer. Parallellt fortsätter felsökning och åtgärder i det felande lagringssystemet.	När felet kunde härledas till lagringsutrustningen togs kontakt med leverantören. Kontinuerlig kommunikation etablerades med leverantörens personal i Irland och USA.
10.14		Från denna tidpunkt läggs löpande information ut på CSTC:s hemsida, med cirka 1 – 1.5 timmars intervall	

10.19	TakeCare stängs	När TakeCare inte kan användas övergår man (avdelningar, mottagningar, laboratorier med flera) till manuella rutiner med papper, stämplar och penna, blanketter för remisser, lappar för interna meddelanden och telefonsamtal till apotek, laboratorier m.m. Läkemedelsrecept skrivs ut på papper. Utdelning av läkemedel görs efter särskild läkarbedömning – eller till och med på ”känsla” på de enheter som inte har en fungerade läkemedelsbackup.	
10.51		Informationsavdelningen sänder ut fax till alla användare därför att intranätet är instabilt.	Man kunde inte lita på att alla nåddes av informationen
11.15		Stabsmöte hålls enligt sjukhusets katastrofplan	
Ca 12.00		Ledningen för SLSO blir informerad, delvis genom andrahandsinformation.	
	Under dagen upptäcks problem med att öppna lokala säkerhetskopior av läkemedelslistor (LM-backup)		
19 december 07.45-14.45		Löpande information om status för TakeCare läggs ut på KS:s hemsida	
09:45	TakeCare är åter i drift		
17:00		Information om att TakeCare återstartades 09.45 läggs ut på SLSO:s intranät. Information på intranätets förstasida om att remissvar kan vara förväxlade.	

Haveri i serverhall på Länssjukhuset i Kalmar 2008

Tidpunkt	Händelse	Åtgärder i det akuta skedet	Kommentar
14 augusti 06.20	Ett motorskydd till en av fläktmotorerna i ventilationssystemet löser ut. Detta medför att temperaturen i serverhallen hastigt stiger.		
07.00	En IT-tekniker, som arbetar på distans mot servrar i serverhallen, upptäcker att vissa servrar inte är igång. Majoriteten av landstingets 240 IT-system har nödstoppats	IT-teknikern åker till serverhallen för att på plats undersöka vad som hänt.	Servrarna stannade automatiskt efter hand för att hårdvara och lagrad information inte skulle skadas.
07.40		IT-teknikern larmar Landstingsfastigheters tekniker och IT-chef och meddelar att det är varmt i serverhallen och att ett antal servrar har stannat. IT-chefen larmar IT-förvaltningens chef och patientjournalsystemet Cosmics operativa systemägare. Kris- och beredskapssamordnaren och landstingsdirektören informeras	Kris- och beredskapssamordnaren diskuterar läget med landstingsdirektören. Denne beslutar att man inte behöver inta stabsläge. ***Författarkommentar:*** *Stabsläge borde ha intagits*
07.46	Landstingsfastigheters tekniker konstaterar att fläktarna i server-hallen står stilla och att temperaturen stigit till 47 grader.		
07.58		Teknikern återställer motorskyddet till fläktmotorn och startar kylanläggningen manuellt.	
08.30		Incidentens omfattning är fastställd och ytterligare information går ut till informationsenheten	Intranätet fungerade inte vid denna tidpunkt

08.30		Intern information om datorstoppet med hjälp av allanrop över snabbtelefonsystemen på de tre sjukhusen	Snabbtelefoner fanns inte längre på alla avdelningar på sjukhusen. Systemen kommer inte att ersättas när de utrangeras. ***Författarkommentar:*** *Tekniska brister ledde till att inte alla fick information*
09.00		Landstinget meddelar i radio att det är problem med IT-systemen. Man ber allmänheten att endast ringa till sjukhusen i akuta fall för att minska trycket på telefonsystemen	
09.26	Temperaturen är åter normal i serverhallen		
09.40		Över lokalradion uppmanas allmänheten att kontakta sjukvården via sjukhusens telefonväxlar istället för via mottagningarnas ordinarie telefonnummer	
10.00	Vitala system är uppe.	För att inte riskera patientsäkerheten är man dock tvungen att kontrollera att data i prioriterade system är oskadade innan användare kan få börja använda dessa	
11.00	Patientjournalsystemet (Cosmic) är i funktion och användare kan logga in		
12.00	Övriga viktiga system som t.ex. journalsystemen Swedestar och T4, systemet för telefonkö TeleQ fungerar korrekt		
12.00	95 % av landstingets drygt 240 IT-system är åter i drift		

Under dagen		Pressmeddelanden skickas ut om att ett ”omfattande driftstopp inträffat som påverkar majoriteten av landstingets datasystem” Pressmeddelanden skickades senare ut om att landstingets datasystem åter var i drift	

Bildhanteringssystem i Uppsala läns landsting 2008-2009

Tidpunkt	Händelse	Åtgärder i det akuta skedet	Kommentar
2008 januari – september	Ett antal oplanerade driftsstopp inträffar och trögheten i det gamla bildhanteringssystemet är alltmer besvärande.		Arbetsmiljön påverkas negativt. Stor oro bland läkare att bilder inte skulle finnas till hands
2008 oktober	Installationen av det nya bildhanteringssystemet påbörjas		Beslut om installation tas av projektets styrgrupp. Detta görs trots att alla tester inte hade genomförts
Oktober-	Från starten uppstår det många kortvariga stopp fram till början av december och det är trögt att få fram bilder.		Arbetsmiljön är fortsatt besvärlig
1 dec 2008 – 31 jan 2009	Systemet trögt men det inträffar inte några oförutsedda stopp längre.		Problemen var identifierade och skulle åtgärdas
2009 3 februari kl. 00:36	PACS slutar att fungera. Alla bilder försvinner	Leverantören inkallas och arbetar intensivt med att lösa problemet.	

3 februari kl. 14:00	PACS i drift igen. Undersökningar och akuta operationer återupptages.	Leverantören gör en total ominstallation av PACS-systemet	Pressmeddelande skickas ut med information om att ”… det nya röntgenbildsystemet vid Akademiska sjukhuset stannade natten till måndagen. Nu vid lunchtid kom systemet igång igen.” Vid denna tidpunkt finns dock inga bilddata i PACS
4 februari -		Bilderna kan successivt återhämtas dels från bildgivande utrustningar, dels från långtidsarkiv. Proceduren för att rekonstruera data blir komplicerad och tidsödande. Den omfattar tre delar: • Färska bilddata återläses från modaliteter till PACS • Bilddata från de föregående tio månaderna återläses från långtids arkiv till PACS för att som tidigare vara snabbt åtkomliga. • Alla undersökningar i långtidsarkivet länkades till PACS för att där markeras som tillgängliga. Återläsning från modaliteter tog liten tid i anspråk medan resten av återläsningen pågick till och med vecka 10 2009.	
Slutet maj 2009	Datastruktur, alla bilder och data återställda		Integrationen med Cosmic patientjournalsystem är dock inte genomförd

Skador

Ingen av de fyra händelserna medförde att någon patient skadades direkt. Huruvida inställda eller försenade operationer, diagnoser och undersökningar senare har lett till skador har inte kunnat fastställas. Samtliga vårdgivare påpekar dock att man bara kan bedöma att det är sannolikt att man inte åsamkat skada, men framhåller att risk för skada har förelegat. Det ska också framhållas att informationsbrister kan orsaka lidande och praktiska besvär för patienterna då vårdgivaren inte kan genomföra undersökningar eller behandlingar.

Vid e-virusangreppet i Region Skåne blev cirka 10 000 datorer, varav ett antal datorer i medicintekniska utrustningar, och cirka 500 servrar infekterade. Här är skadorna främst ekonomiska: investeringar i hård- och mjukvara samt arbete utfört av egen personal och entreprenörer.

När TakeCare patientjournalsystem blev utslaget i Stockholms läns landsting gick uppgifter som lades in under cirka två timmar förlorade. Dessa kunde inte återskapas.

I Kalmar uppstod inte några skador i registrerade data eller i servrarna när dessa stoppades automatiskt på grund av för hög temperatur.

När PACS bildarkiv på Akademiska sjukhuset i Uppsala återstartades efter avbrottet kunde alla bilder återläsas utan att någon information gick förlorad.

Störningar

Generellt

Produktion

De störningar som uppstod på grund av IT-problemen påverkade vården och omsorgen negativt i större eller mindre grad. Vårdproduktionen är beroende av att information finns tillgänglig vid undersökning och behandling av patienterna. Om information inte finns tillgänglig kommer man antingen att skjuta upp vad som skall genomföras, vilket medför tillkommande kostnader, eller också utför man ytterligare undersökningar, provtagningar eller behandlingar, som kanske inte är nödvändiga. Detta medför också högre kostnader. Andra faktorer som behöver beaktas är att om IT-systemen slutar att fungera så kommer reservåtgärder förr eller senare att sättas in, till exempel mer personal vid intensivvårdsavdelningar.

Säkerhet

I samtliga fall påverkades patientsäkerheten och tre av händelserna anmäldes enligt lex Maria till Socialstyrelsen. När information inte finns tillgänglig kommer både utredningar och behandlingar att störas. Fördröjs en insats kan detta leda till uppenbara säkerhetsrisker vid till exempel en intensivvårdsavdelning. Vid ambulanstransport av akutpatient till sjukhus måste informationsöverföringen mellan ambulans och sjukhus fungera för att omhändertagandet ska bli optimalt säkert. I detta kapitel beskrivs de patientsäkerhetsrisker som uppstod vid de fyra händelser som rapporten omfattar.

Hälsoekononomi

Vård och omsorg omsätter cirka 350 miljarder kronor varje år. Störningar i utredning eller behandling av patienter innebär konsekvenser för ekonomin inom sjukvården och i samhället i övrigt genom att produktionen på patientens arbetsplats påverkas. I de fall anhöriga följer med patienten till sjukvården vid undersökning eller behandling medför detta också ökade kostnader för samhället genom att sjukförsäkringssystemet får betala ut mer ersättning.

Vårdgivarna har inte gjort någon uppskattning av de direkta eller indirekta kostnaderna för de fyra händelserna.

Aktuella händelser

E-virusangrepp i Region Skåne

Samtliga förvaltningar inom Region Skåne drabbades i varierande omfattning. De huvudsakliga problemen var störningar i inloggningsfunktioner och därmed begränsad tillgänglighet till journalhandlingar, operationsplanering, röntgenbilder, provsvar m.m. Även betydande påverkan uppstod på e-post, e-receptfunktionen och telefonisystemet.

Ett flertal medicintekniska utrustningar påverkades också, främst övervakningsutrustningar och bildlagring på flera sjukhus.

En pågående patientundersökning fick avbrytas därför att de medicintekniska datorerna som användes vid behandlingen av patienten utan förvarning fjärrstyrdes av ITT för att rensas från e-virus. Händelsen anmäldes separat enligt lex Maria till Socialstyrelsen. Myndighetens beslut [6] innehöll bland annat krav på att riskanalyser ska göras då medicinsk utrustning ansluts till och utnyttjar gemensamma nätverk.

På Hässleholms sjukhus fungerade inte övervakningsutrustningen tillfredställande.

En del patientundersökningar ställdes in på grund av att medicintekniska datorer var smittade med e-virus.

Patientjournalsystemet Melior, radiologisystemet Kundrad, digital diktering och det patientadministrativa systemet kunde inte nås eller användas.

Produktionen på Kemilaboratoriet störtes genom att smittade datorer startade om utan yttre påverkan. Dessa i praktiken medicintekniska datorer var inte registrerade som medicintekniska produkter i ITT:s register.

Allvarliga störningar uppstod i Philips Xcelera, ett system som används vid akut hjärt- och kärldiagnostik, och i Mobimed som används i ambulanssjukvården för att skicka EKG till sjukhusen.

Region Skånes telefonileverantör hade problem med vidarekoppling och hänvisning av samtal på grund av att e-virus kommit in i 21 av deras servrar.

Journalsystembortfall inom Stockholms läns landsting

Samtliga användare av vårdinformationssystemet TakeCare och samtliga system som har utbyte av information med TakeCare påverkades under 25 timmar.

Utan tillgång till TakeCare kunde man inte använda systemet för bedömningar, daganteckningar, epikriser, remisser, intyg och dylikt och det var inte möjligt att svara på vissa frågor från anhöriga per telefon. Denna brist på information om patienter under vård och behandling kunde leda

till felaktig medicinering, felaktig eller utebliven behandling med mera. Risken för allvarliga skador kunde inte uteslutas även om personalen var vaksam och kunnig.

Några få mindre operationer fick skjutas upp.

Det blev vidare svårt att genomföra ronder och vårdplaneringsmöten utan tillgång till aktuell journal. Händelsen inträffade strax före en långhelg då många patienter skulle skrivas ut för hemgång eller permission vilket innebar att extra många vårdplaneringsmöten behövde hållas.

Svar på prover kunde inte registreras i TakeCare och remisser kom inte fram till utförande laboratorium. Patienter kom till röntgen eller för provtagning, men dessa enheter hade ingen information om vad som skulle röntgas eller vilka prov som skulle tas. Dessutom kunde inte remitterande läkare få resultat av prover som utförts före avbrottet.

Det fanns risk för förväxling av laboratorieprover eftersom det blev fel i beställningsnummerserien vid återstarten av TakeCare. Detta ledde till risker för allvarliga fel i medicinering och behandling.

Inneliggande patienters läkemedelslistor kunde endast tas fram på de avdelningar där man använde den särskilda läkemedelsbackupen i TakeCare.

Haveri i serverhall på Länssjukhuset i Kalmar

På alla hälso- och sjukvårdsenheter uppstod stora problem när man inte kunde komma åt journalanteckningar, läkemedelslistor och laboratorieanalyser. I den slutna vården innebar det svårigheter vid ronder och läkemedelshantering. Tjänstgörande personal som inte arbetat skiftet innan datorstoppet saknade information kring patienterna.

Alla hälso- och sjukvårdsenheter rapporterade att datorstoppet medförde en högre arbetsbelastning då inga normala rutiner fungerade. När IT-systemen åter var i funktion krävdes ytterligare extra arbetsinsatser för att i efterhand registrera alla manuellt gjorda anteckningar under avbrottet.

Besök till mottagningarna på sjukhusen fick ställas in i vissa fall eftersom remisser saknades.

Laboratorie- och bloddatasystemen vid Länsenheten för klinisk kemi var ur funktion.

Psykiatriförvaltningen rapporterade att den kontinuerliga kontakten med psykiatripatienter och kontakten med andra vårdgivare och kommuner via uppringning inte kunde upprätthållas.

Primärvårdsförvaltningen rapporterade dålig kvalitet vid besök hos läkare när journal inte var tillgänglig. Diktering av journaler fungerade inte. Dessutom framhölls att patienterna hade svårigheter att nå primärvården när inte TeleQ telefonkösystem fungerade.

I alla dessa fall innebar bristen på aktuell information risk för att patientsäkerheten inte skulle kunna upprätthållas. Men eftersom avbrottet inte varade mer än några timmar skedde inga allvarliga incidenter .

Folktandvården framhöll att datorstoppet innebar direkt minskade intäkter och en risk för minskat förtroende för organisationen, detta skulle kunna leda till färre antal patienter i framtiden.

Serviceförvaltningen rapporterade att passersystemen inte gick att nå. Detta hade kunnat bli allvarligt vid ett längre avbrott. Arbetsordersystemet fungerade inte liksom ett antal administrativa system.

Från teleservice rapporterades att allanrop inte fungerade i alla hus vid Länssjukhuset i Kalmar. Belastningen på televäxlarna ökade när inte telefonkösystemet TeleQ fungerade.

Informationsenheten rapporterade att den externa webbplatsen låg nere vilket hindrade att information till allmänheten kunde spridas den vägen.

Bildhanteringssystem i landstinget i Uppsala län

Bilder fanns inte tillgängliga direkt via PACS för ronder och operation. Bilder kunde dock hämtas manuellt från långtidsarkivet eller vid akut bildtagning direkt vid den individuella arbetsstationen. Verksamheten kunde fortsätta men det fanns en oro bland läkarna att man inte skulle kunna genomföra ronder om man inte kunde få fram bilder.

Det gick inte att överföra bilder till eller från andra enheter inom regionen för konsultationer, till exempel skalltraumabilder som skickades för bedömning.

Bilderna kunde efter de akuta åtgärderna successivt återläsas från långtidsarkivet till PACS, men det tog drygt tre månader innan alla bilder och bilddata var återlästa.

Bakomliggande orsaker

När verksamheterna kom igång igen efter de akut vidtagna åtgärderna har ansvariga hos huvudmännen gjort noggranna händelseanalyser. I några fall har man tagit hjälp av externa experter. Genom dessa analyser har bakomliggande orsaker identifierats.

I detta kapitel beskrivs de bakomliggande orsakerna till händelserna.

E-virusangrepp i Region Skåne

E-viruset W32/Downadup.CM kom in i Region Skånes intranät Skånet via ett USB-minne som anslöts till en dator. Viruset använde flera olika metoder för att sprida sig såsom att gissa nätverkslösenord och infektera USB-minnen och genom att utnyttja en sårbarhet i Windows Server Service, ett problem som Microsoft sedan dess åtgärdat.

Ett typiskt problem som masken orsakar är att den stänger ute användare från nätverket. Det sker genom att masken försöker gissa nätverkslösenord vilket till slut aktiverar den automatiska utestängningen .

När väl masken infekterat en dator skyddar den aggressivt sig själv genom att aktiveras tidigt i en dators uppstartprocess och genom att sätta rättigheter på filer och registernycklar som hör till masken så att användare inte kan ta bort eller ändra dem.

Masken laddar ner modifierade versioner av sig själv från en lång rad webbsidor. Namnen på webbsidorna genereras av en algoritm baserad på nuvarande datum och klockslag. Eftersom det finns hundratals olika domäner som kan användas av den skadliga koden är det svårt för säkerhetsföretag att lokalisera och stänga ner dem i tid. Följden blev att det var ovanligt svårt att helt radera den skadliga koden när den väl fanns inne i nätverket.

En orsak till att e-viruset under så lång tid kunde sprida sig i regionens nätverk var bland annat att säkerhetspatch KB968644 från oktober 2008 inte blivit installerad på flera avstängda datorer. Information om att installera patchen sändes ut till berörda men det fanns inga tydliga regler eller ansvar för att utföra installationen och inte heller någon rutin för att följa upp att den blivit genomförd.

E-viruset kunde därför ta sig förbi de delvis bristfälliga barriärer och skydd som fanns och kom därmed in i cirka hälften av Region Skånes servrar och datorer och in i flera medicintekniska utrustningar.

Det saknades rutin för att sprida information vid virusangrepp. Informa-

tionen om angreppet lästes inte av vårdpersonalen då denna information endast fanns på regionens hemsidor.

Det fanns också brister och otydlighet i kommunikationen och ansvarsfördelningen mellan TiB, ITT och medicinsk tekniks olika enheter på sjukhusen.

Det rådde otydlighet om hur interna och externa IT-relaterade säkerhetsmeddelanden skulle hanteras inom den medicintekniska verksamheten.

Regionens telefonileverantör var långsam då det gällde att på ITT:s uppmaning skydda telefonisystemet mot e-virus.

Det var inte allmänt känt ute i verksamheten att datorer i medicinteknisk utrustning skulle vara registrerade i ett centralt register före inkoppling i intranätet Skånet.

Det fanns ingen katastrofledningsplan på ITT för att hantera allvarliga angrepp av e-virus och det fanns inga etablerade kontakter mellan medicinteknisk personal på sjukhusen och ITT. Som tidigare nämnts innehöll inte heller regionens kris- och katastrofplan några tydliga instruktioner om hur man skulle agera vid en störning i IT-systemen

Journalsystembortfall inom Stockholms läns landsting

Den primära orsaken till händelsen var att lagringsutrustningen (SAN) inte var uppdaterad med den senaste säkerhetspatchen. Enligt leverantören Dell var denna uppgradering inte klassad som kritisk och det fel som uppstod var inte tidigare känt. Det pågående arbetet med utökning av en datavolym i det lagringssystem som TakeCare var installerat i genererade på grund av detta fel onormalt mycket belastning. Detta försämrade prestanda markant både för läsning från och skrivning till systemet. Driftutrustningen tillsammans med manuella rutiner borde, enligt Dell, ha kunnat hantera problemet utan vare sig driftsavbrott eller informationsförlust.

Enligt den utredning som gjordes av Dell kan man inte peka ut en enskild avgörande orsak till incidenten. Flera faktorer samverkade. De viktigaste var:

- Återläggning av säkerhetskopia var inte testad. Därmed fanns ingen insikt i att transaktionsloggen inte kunde återställa information med utgångspunkt från senaste säkerhetskopia. Transaktionsloggen borde dessutom ha lagrats på ett separat disksystem.
- En bidragande orsak var den alltför begränsade övervakningen av driftutrustningen. Överbelastningen i lagringssystemet upptäcktes inte i tid vid incidenten. Kapacitetsutnyttjandet av lagrings-

systemet från andra applikationer än TakeCare hade ökat under en längre tid.

- Övervakningen av TakeCare var inte tillfredsställande.
- Stilleståndstiden kunde troligen ha kortats om man i tid insett att mängden trasiga filer var för stor för att kunna repareras manuellt.
- IT-systemen var inte prioritetsklassade. Rutinerna för eskalering av åtgärder vid inträffad incident var bristfälliga. Rollerna och ansvaret mellan IT-Forum, SLL-IT, systemansvarig och tredjepartsleverantör var otydliga.
- Bristen på IT-katastrofplan eller kommunikationsplan medförde att det inte blev en samordnad styrning av informationen om avbrottet i TakeCare.
- Systemet var inte testat i den miljö som det nu skulle fungera i efter att det överförts från den ursprungliga. Vid en så stor förändring måste kvalificeringstester genomföras i enlighet med gängse kvalitetskriterier.

Haveri i serverhall på Länssjukhuset i Kalmar

Den utlösande orsaken till händelsen var att motorskyddet i en fläktmotor i kylanläggningens ena aggregat löste ut av oklar anledning. Kylanläggningen blev stående utan att växla över till det andra aggregatet, som stod i reserv, därför att larmet som skulle indikera att fläkten stod stilla var blockerat. Denna blockering aktiverades genom att driftindikeringen försvann när motorn stannade. När driftindikeringen från det aggregat som skulle vara i funktion saknades växlade således inte styrprogrammet över funktionen till det andra kylaggregatet. När övervakningsprogrammet konstruerades förutsåg man inte denna situation.

Larmet från det utlösta motorskyddet var ett s.k. B-larm. Dessa larm observeras endast under dagtid.

Utan fungerande kylning i serverhallen steg temperaturen okontrollerat och alla IT-system stannade automatiskt vilket är en skyddsåtgärd för att inte skada hårdvara och lagrad information. Temperaturlarmet i serverhallen fungerade inte heller och detta berodde på att larmet var felprogrammerat.

Bildhanteringssystem i landstinget i Uppsala län

Den tekniska utredningen visade att bildhanteringssystemet slutade fungera på grund av ett konstruktionsfel i PACS-systemet. RIS-systemet påverkades inte. Den kommunikationslänk som förband applikationsservern och databasservern slutade att fungera. Detta innebar att båda servrarna uppfattade att den andra servern inte längre fungerade. Detta medförde att båda servrarna samtidigt försökte läsa och skriva i den gemensamma bildlagringsdatabasen med följden att denna skrevs sönder, en så kallad ”split brain” situation uppstod.

Under de akuta försöken att återskapa bilder och bilddata hämtades detta från bildlagringsdatabasen, men eftersom den inte längre innehöll någon aktuell och korrekt säkerhetskopia fungerade inte detta.

Återställande och återhämtning

Efter de akuta insatserna för att få IT-systemen snabbt i drift igen har ytterligare åtgärder vidtagits och planerats hos de drabbade verksamheterna. Åtgärderna handlar om genomgripande förändringar av teknik, organisation, procedurer, informationsmetoder med mera samt planering för framtida förändringar för att ytterligare öka driftsäkerheten i IT-system. Särskild uppmärksamhet har alla vårdgivarna ägnat åt sjukvårdens kris- och beredskapsplaner[9]. Dessa har i samtliga fall antingen förtydligats, kompletterats eller totalt reviderats och kompletterats med handlingsplaner för hur störningar i försörjnings- och informationssystemen ska hanteras.

I detta kapitel beskrivs de åtgärder som genomförts till och med årsskiftet 2010-2011. I en del fall finns även information om åtgärder som planeras genomföras på längre sikt.

E-virusangrepp i Region Skåne

Planering av långsiktiga åtgärder

Efter e-virusangreppet i januari 2009 genomfördes en händelseanalys, en sårbarhetsanalys och en åtgärdsplan togs fram. Åtgärdsplanen resulterade i ett projekt som fick benämningen ”Handlingsplan e-virus”. Det övergripande syftet med handlingsplanen är att kraftigt minska risken för e-virusangrepp, men också då angrepp konstateras, kunna arbeta i en väl genomtänkt process för att mildra effekter och hantera information och kommunikation på ett adekvat sätt. Handlingsplanens innehåll sammanfattas under nedanstående rubriker. Många av de beslutade åtgärderna är klara medan i andra fall återstår ytterligare en tids arbete för att slutföra handlingsplanen.

Krishanteringsplan

En krishanteringsplan för Region Skåne har fastställts i juni 2009. Den initierades redan 2007 och innehåller bland annat krav på risk och sårbarhetsanalyser. I planen konstateras att Region Skånes verksamhet är beroende av att kritiska system fungerar. Frågor som rör funktionssäkerhet, försörjningssäkerhet, robusthet och beroendeförhållanden ska därför integreras och klarläggas i risk- och sårbarhetsarbetet på alla nivåer. Här nämns till exempel att avbrott i tele- och IT-systemen måste betraktas som avbrott i samhällskritisk verksamhet.

Kommunikationsvägarna mellan IT och TiB, respektive mellan IT och den medicintekniska verksamheten MT, har tidigare inte varit tillräckligt utbyggda. Åtgärder ska därför vidtas för att förbättra dessa och – inte minst viktigt – att anpassa IT-informationen språkligt till de sjukvårdande verksamheterna. Journummer till ledningen för IT och till regionens medicintekniska chef MTC-RS har upprättats.

Organisation, procedurer och rutiner

En ”Krishanteringsplan för IT och informationssäkerhet” har utarbetats och fastställts. Planen är ett styrande dokument för hantering av stora incidenter i IT-system. Parallellt har en ”Handlingsplan för hantering av e-virus och större incident” upprättats riktad mot den medicintekniska verksamheten. Vidare har ett arbete påbörjats för att uppdatera och komplettera ledningssystemet för informationssäkerhet, informationssäkerhetshandboken, utgående från standarden SS-ISO/IEC 27000: 2009 [7]. Den tidigare informationssäkerhetshandboken följde standarden ISO/IEC 17799: 2005.

Den tidigare ITT-förvaltningen har ersatts av Region Skånes IT-avdelning RSIT och ingår nu i en kommunikations- och IT-förvaltning, som är direkt underställd regiondirektören.

Centralt på regionen finns en medicinteknisk chef, MTC-RS. Den medicintekniska verksamheten i Region Skåne består i övrigt av medicintekniska enheter som ingår i varje sjukhus organisation. Omständigheten att IT och MT har olika organisationsformer har i samband med e-virusangreppet skapat särskilda problem vad gäller ledning, information och kommunikation vid hantering av stora eller omfattande händelser i de IT-system som utnyttjas för både administrativa och medicinska uppgifter. Ansvarsroller och uppgifter måste därför tydliggöras i samstämmiga handlingsplaner för hela regionen. Samverkansformerna mellan RSIT och de sjukhusanknutna medicintekniska enheterna ska göras tydligare och gränserna för respektive organisation ska preciseras.

Den interna tillsynen i Region Skåne måste förbättras. MTC-RS har fullt ansvar för att säkerhetsanvisningar följs och är korrekt implementerade i alla medicintekniska produkter. För att möjliggöra detta ska organisationerna för både MT- och IT-verksamheterna på sjukhusen revideras och troligen kompletteras för att skapa former för bättre samverkan, kontroller och åtgärder. Detta arbete pågår.

MTC-RS har tagit fram en handlingsplan för den medicintekniska

[9] Kris- och beredskapsplanerna har olika benämningar hos huvudmännen, vilket återspeglas i underrubrikerna

verksamheten i regionen vid e-virusangrepp. Den innehåller anvisningar på konkreta åtgärder som måste vidtas av den medicintekniska personalen dels i förebyggande syfte, dels vid ett konstaterat e-virusangrepp. I handlingsplanen framhålls att det är viktigt att ha tydliga överenskommelser med produktleverantörerna om vem som har ansvaret för olika slags skyddsåtgärder.

Utbildningsinsatser krävs på alla nivåer inom sjukhusens organisationer. Utbildningen i krisberedskap måste förbättras så att framförallt alla nyckelfunktioner får tillräcklig och adekvat information. Medvetenheten måste ökas hos Region Skånes medarbetare avseende risker och följder av e-virusangrepp.

En kommunikationsplan ska upprättas för hur informationsspridning ska ske om Region Skåne blir utsatt för e-virusangrepp.

Under 2010 har en del av Region Skånes IT-tjänster upphandlats och under 2011 beräknar man att alla IT-tjänster i regionen ska vara upphandlade och avtal skrivna med externa företag.

Tekniska åtgärder

”Handlingsplan för e-virus” innehåller konkreta skyddsåtgärder. Här finns krav på åtgärder för att stärka skyddet mot alla typer av e-virus i datorer och servrar i nätverket, genomföra regelbundna uppdateringar av program och säkerhetspatchar med mera. Virusskyddet är uppdaterat till en version som även innehåller en brandvägg.

För att kunna logga in på nätverket skärps kraven på säkra användarnamn och lösenord. Säkerhetshandboken ska kompletteras med tydliga regler för inkoppling på Region Skånes intranät och för hantering av säkerhetspatchar. Kraven för att få använda flyttbara minnesmedia har skärpts. Samtidigt har funktionen auto-run i operativsystemet i alla datorer i nätverket kopplats bort, vilket gör att eventuella drivrutiner i ett anslutet USB-minne inte läses in i datorn. Ett förslag att endast tillåta USB-minnen av ett fabrikat och modell bordlades eftersom det inte bedömdes vara möjligt att upprätthålla och övervaka en sådan regel.

En patchserver har driftsatts vilket innebär att patchuppdateringar snabbare kan distribueras till alla datorer anslutna till intranätet.

En överenskommelse om gemensam policy och rutiner för anslutning till Region Skånes intranät ska tecknas med universitetet.

Handlingsplanen handlar också om de krav som måste föras fram vid anskaffning av medicintekniska produkter som ska samverka med IT-system. För medicinteknisk utrustning finns särskild lagstiftning [8] som anger att tillverkaren har ansvar för produkternas funktion när de används

enligt tillverkarens anvisningar. Socialstyrelsens föreskrifter [9] preciserar begränsningarna för vad användaren kan göra utan att överta tillverkarens produktansvar. Rollen som System Integrator (SI) har därför skapats vid den medicinska enheten på varje sjukhus för att bevaka att integrationen av den medicintekniska utrustningen med datanätverket sker på ett patientsäkert sätt och att ansvarsrollerna för tillverkare respektive sjukvårdens aktörer är tydligt beskrivna. Detta innebär också att medicinsk teknik måste ställa krav på virusskydd och eventuella avtal med tillverkare vid upphandling av medicintekniska produkter.

Ett nytt intranät upphandlas vilket ska öka möjligheten att kontrollera och spåra oönskad trafik och skadlig kod.

Journalsystembortfall inom Stockholms läns landsting

Planering av långsiktiga åtgärder

Bristerna uppmärksammades i en haverirapport som överlämnades till en arbetsgrupp med uppdrag att åtgärda problemen. Medverkande i arbetsgruppen har varit systemägarorganisationen CSTC, TakeCare-leverantören ProfDoc Care AB och driftavdelningen SSL-IT. Målet var att åtgärda de påtalade bristerna senast under 2010.

Med utgångspunkt i haverirapporten initierades ett åtgärdsprogram i april 2009 med målet att samtliga punkter i rapporten skulle åtgärdas. Åtgärdsprogrammet består av tre delar: drift, applikationer och organisation. I det följande redovisas översiktligt de olika åtgärdsförslagen.

Kraven på funktionaliteten i TakeCare har utgått från vårdgivarnas krav. Underlag för dessa har varit författningar riktade mot vårdgivarna och då framför allt Patientdatalagen och Socialstyrelsens föreskrift (SOSFS 2008:14) om informationshantering och journalföring i hälso- och sjukvården [18].

Katastrofplan

En ny katastrofplan för Karolinska Universitetssjukhuset har tagits fram och börjar gälla från och med 2011. I den är ett av målen för katastrofplaneringen ”… att vid hot mot det robusta sjukhuset minimera konsekvenserna för såväl patienter som för fastighet, egendom och verksamheter”. Med hot mot det robusta sjukhuset avses händelser som påverkar el, tele, datakommunikation, vatten, värme och motsvarande anordningar för viktiga tekniska försörjningsfunktioner. Larm om allvarlig händelse inom sjukhuset kommer till säkerhetscentralen direkt eller via fastighetsägarens driftcen-

tral, via SLL IT eller på annat sätt. Säkerhetscentralen kontaktar SOS-alarm, ordningsvakter, chefläkare/stabschef och säkerhetschef samt loggar händelsen till dess respektive katastrofledningsgrupper tar över. Chefläkaren/stabschef beslutar i samråd med säkerhetschefen om beredskapsläge och kontaktar fastighetsägarens katastrofledning

Organisation, procedurer och rutiner

Karolinska Universitetssjukhusets IT-verksamhet IT-Forum ingår från och med 2009 i Stockholms läns landstings IT-avdelning SSL-IT.

Stockholms läns sjukvårdsområde (SLSO) har en infrastruktur för att ta emot e-post i mobilen. Den aktuella händelsen visade att detta inte fungerade i alla verksamheter. En översyn av rutinerna inom SLSO har därför gjorts för att hålla e-postlistor aktuella så att CSTC kan hålla SLSO-anställd personal kontinuerligt underrättad vid driftstörningar.

Avtal mellan SSL-IT, CSTC och ProfDoc Care AB har tagits fram som tydligare beskriver de överenskomna leveranserna och tjänsterna. Uppföljning av att leveranser och tjänster motsvarar avtalade nivåer stäms av vid regelbundna månadsmöten med parterna. Utgångspunkten har varit att driften ska hålla högsta möjliga säkerhetsklass vad gäller sekretess, tillgänglighet och riktighet.

ProfDoc Care AB har CE-certifierat TakeCare enligt kraven i Europaparlamentets medicintekniska direktiv 2007/47/EG [3]

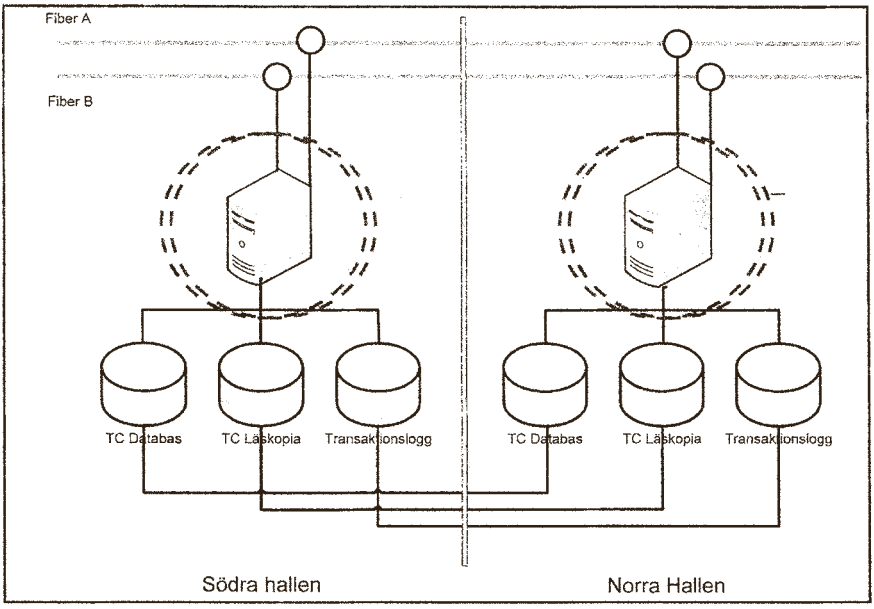
Kompetensen i IT-organisationen har förstärkts och kommer att vidareutvecklas. Till hjälp i detta utvecklingsarbete kommer man att använda sig av de brittiska men internationellt erkända rekommendationerna ”Information Technology Infrastructure Library” (ITIL) för organisation, service och support [10]. IT-organisationen ska öka kunskapen om medicintekniska produkter och dess olika regelverk samt om behovet av riskbedömningar och testningar som behöver utföras innan ett IT-system kan implementeras eller en förändring införs. I övrigt ska kompetens i kvalitetssystem och kvalitetsstyrning generellt ökas men framför allt i IT-system. Det betyder bland annat att kompetensen att göra tydliga och utförliga kravspecifikationer vid upphandlingar ska ökas och att rutiner för regelbundna uppföljningar kommer att införas.

Tekniska åtgärder

En ny driftplattform för TakeCare har tagits i bruk. Den består av två lika delar – server, databas, läskopia och transaktionslogg – placerade i södra respektive norra datahallen. Databas, läskopia och transaktionslogg är placerade i lagringssystem SAN. Vid ett oplanerat avbrott under 2010 fick

man tillfälle att testa funktionaliteten i återläsningen av transaktionsloggen i ett ”skarpt läge” och man kunde konstatera att resultat var gott.

Den nya plattformen TC 2010 – schematiskt



Figur 1: Schematisk bild av den nya plattformen

Risken för problem beroende på att TakeCare delade lagringsutrymme med andra system har eliminerats genom att TakeCare nu har ett eget lagringsutrymme i SAN:et. Övervakningen av lagringssystemet för bland annat TakeCare har förbättrats och en funktion, Journaling, provas för att reducera eller eliminera risken för trasiga filer i databasen.

En uppdaterad driftsdokumentation avseende TakeCare har överlämnats till SLL-IT. Val av standards för den tekniska utformningen av systemet har skötts av ProfDoc Care AB.

Funktionen att skapa en läskopia har som ovan nämnts införts. Det hade man inte tidigare eftersom man vid en tidigare utförd analys av konsekvenserna vid ett längre driftstopp dragit slutsatsen att den funktionen inte var nödvändig. Istället fanns rutinen med den så kallade Läkemedelsbackupen. Detta visade sig dock inte fungera på alla enheter. Det var en tidskrävande och relativt komplicerad procedur och inte alltid det som prioriterades högst av personalen på sjukvårdsenheterna.

En läskopia görs automatiskt fyra gånger per dygn och innehållet är en högst sex timmar gammal kopia av databasen. Emellertid säkrar denna funktion endast att det finns en aktuell kopia av TakeCares data i ett redundant lagringssystem. Om nätverket går ner nära servern för läskopian är den inte läsbar ute i verksamheten. Om nätverket bryts på något annat ställe längre ifrån servern kan man dock nå läskopian via en annan väg. Det ska således finnas viss redundans i nätverket.

Den gamla funktionen Läkemedelsbackup med lokal dator finns kvar. Ansvaret för förvaltningen av denna ligger hos respektive vårdgivare. Man har gjort på olika sätt för att förbättra säkerheten. På SLSO-nivå finns en särskild IT-tjänst som kan ge stöd i hur man lokalt bäst ska upprätthålla en säker läkemedelsbackup.

Fungerande nätverk är en förutsättning för att kommunikation till, från och inom TakeCare ska fungera. Idag är nätverket en svag länk eftersom ingen fullständig redundans, det vill säga inget fullständigt reservnätverk, finns som kan användas om det ordinarie nätverket inte går att använda. SSL-IT undersöker olika möjligheter att skapa ett redundant nätverk, men någon tidsplan är inte fastställd. När SLSO:s intranät förnyas kommer Verva:s (Verket för förvaltningsutveckling)[10] riktlinjer gällande krisinformation på webbplatser att följas.

Haveri i serverhall på Länssjukhuset i Kalmar län

Planering av långsiktiga åtgärder

Det redan påbörjade arbetet inom samtliga sjukvårdsförvaltningar att upprätta handlingsplaner för större driftsavbrott med hjälp av risk- och sårbarhetsanalyser intensifierades efter den aktuella händelsen. Arbetet handlade bland annat om att hitta fungerande informationsvägar inom och mellan förvaltningarna.

Kris- och katastrofberedskapsplan

Landstingets kris- och katastrofplan håller på att revideras. I denna införs åtgärdsplaner för hur allvarliga avbrott i IT-systemen ska hanteras. TiB:s uppgifter vid IT-haverier förtydligas. På IT-förvaltningen har man upprättat checklistor att följa vid bortfall av IT-system. Huvuddelen av detta arbete leds av risk- och sårbarhetsgruppen inom hälso- och sjukvårdsförvaltningen.

I landstingets kriskommunikationsplan framhålls att organisationen bör utse en talesman i olika krislägen. I det nu aktuella fallet hade någon av landstingets chefsläkare varit en lämplig talesman.

Organisation, procedurer och rutiner

Befintliga rutiner för massmediekontakter ska även användas vid allvarliga IT-haverier. Ytterligare utbildning i massmediekontakter, till exempel inom IT-förvaltningen, kommer att genomföras.

Strukturen och kvaliteten i landstingets IT-tjänster ska förbättras. IT-systemen ska prioriteras så att driftansvariga vet vilka system som i första hand ska hållas i drift när störningar inträffar.

Inom landstingets IT-förvaltning tillämpar man nu pm3 förvaltningsmodell [11] för att organisera och styra landstingets alla gemensamma IT-system. Dessutom används ITIL [10] för att utbilda och skapa en driftsäker IT-verksamhet. Vidare följer man standarderna SS-ISO/IEC 27000 [7] och SS-EN 9000-serien [12] i tillämpliga delar för att bygga upp, styra och kontinuerligt utvärdera IT-verksamheten.

Tekniska åtgärder

Efter driftavbrottet 2008 inrättades en ny tillfällig serverhall i Kalmar (hall 19). När det var klart 2009 fanns därför två hallar i Kalmar. Den last som tidigare funnits i hall 18 fördelades på dessa två varvid problemet med att inte kunna bli av med den värme som alstrades, tillfälligt var åtgärdat.

Till hösten 2011 kommer landstinget i Kalmar Län att förfoga över tre moderna datahallar: två i Kalmar och en i Västervik. Det kommer bli möjligt att uppfylla kraven på redundans och säker drift i den omfattning man har behov av. Alla tre hallarna uppfyller kraven som ställs på informationssäkerhet (BITS)[11] [13] enligt MSB:s basnivå. Kraven på redundans och driftsäkerhet uppfylls även för försörjningen av hallarna med kyla, kraftförsörjning och nätanslutningar. En revision för att verifiera allt detta kommer att genomföras under ledning av MSB.

Inom televäxeln startade ett arbete för att säkerställa att allanrop via snabbtelefonsystemet har hundraprocentig täckning inom sjukhusen. När det gäller telefonkösystemet TeleQ ska det klargöras hur mottagningarna ska agera när TeleQ inte fungerar och vilken information som ska lämnas till allmänheten. En inventering av faxar och mobiltelefoner påbörjades för att ha som utgångspunkt för uppdateringar av olika larmlistor. Eftersom man inte kunde komma åt den ”digitala telefonkatalogen” när intranätet inte fungerade planerar man att distribuera den på cd-skivor.

Läskopior av journalsystemet Cosmic är installerade igen på alla tre sjukhusen. Under sista kvartalet 2011 kommer Cosmic att vara redundant fullt ut.

---

[10] Verva upphörde från och med 31 december 2008. Dess verksamheter övertogs av andra myndigheter.

Bildhanteringssystem i landstinget i Uppsala län

Planering av långsiktiga åtgärder

Bytet av bildsystem och den planerade integrationen med patientjournalsystemet Cosmic var en flerårig process. Den långsiktiga åtgärdsplanen var formulerad redan i det första beslutet i landstingsledningen i juni 2004. På grund av komplikationer vid upphandlingen och de senare tillstötta tekniska svårigheterna att få det nya bildsystemet att fungera var det nödvändigt att justera de ursprungliga åtgärdsplanerna. .

Regional katastrofplan- och beredskapsplan

Den regionala katastrof- och beredskapsplanen från 2005 för Landstinget i Uppsala län håller på att revideras. Den beräknas bli färdig under 2011. I den kommer planer för hur man ska hantera störningar i olika försörjningssystem, såsom el, vatten, IT, tele med mera att finnas.

Organisation, procedurer och rutiner

Gränsdragning och ansvarsfördelning mellan landstingets IT-direktör, landstingets förvaltningar, systemägare och Medicinsk informatik och teknik (MIT) har fastställts 2008. MIT är en landstingsgemensam enhet som tillhandahåller drift, underhåll och teknikkompetens i hela landstinget. MIT är uppdelad i tre avdelningar: medicinsk teknik, IT-system (mjukvara) och IT-teknik (hårdvara). För styrning av IT-verksamheten och samverkan med landstingets alla kunder har man inrättat olika råds- och dialoggrupper. I dessa grupper behandlas frågor om IT-policy, infrastruktur, systemägarskap samt MIT:s uppdrag, ansvar, tjänster och hur MIT uppnår sina resultat. Dokumentet beskriver inte uttryckligen hur stora driftstörningar i IT-systemen ska hanteras. Som grund för denna samverkan med kunderna har man använt pm[3]förvaltningsmodell [11].

MIT, som har uppdraget att medverka i upphandlingar av IT-system, ska i fortsättningen genomarbeta kravspecifikationer bättre så att problem av de slag som visade sig under införandet av bildsystemet inte ska återkomma. Vid införande av nya IT-system ska det finnas en organisation och ett ledningssystem utformat för att klara en komplicerad implementering. Rutinerna för avvikelser ska vara ändamålsenliga och tydliga. Alternativa rutiner ska vara fastlagda och kända. Tillräcklig tid, ekonomi och kompetens måste finnas för att projektet ska kunna genomföras. Externa konsulter ska kunna tas in vid behov.

---

[11] Utgavs av den tidigare Krisberedskapsmyndigheten som nu uppgått i Myndigheten för samhällsskydd och beredskap

För att minska riskerna för att patientskador ska inträffa vid oförutsedda negativa händelser med bildhanteringssystemet har man bestämt att verksamhetschefen vid Bild- och funktionscentrum BFC och chefläkaren ska gå ut med information direkt till verksamhetscheferna på de mest berörda enheterna och att informationen även ska publiceras på sjukvårdens interna hemsida.

Tekniska åtgärder

När den tekniska orsaken till haveriet var klarlagd inleddes planeringen för åtgärder omgående. I den nya konstruktionen kompletterades *heart beat*-mekanismen med *I/O-fencing* vilket är en mekanism där indikatorer används i databasen. Med denna konstruktion kan systemet alltid avgöra vilken server som senast använde databasen och vilka transaktioner som nyss genomfördes eller pågick. I händelse av att den server som senast hanterade databasen slutar fungera eller *heart-beat* uteblir kan den server som tar över slutföra föregående transaktion. I och med det kan *split brain* inte inträffa.

Den beslutade funktionen att kunna nå alla bilder via Cosmic hade vid slutet av 2010 ännu inte kunnat genomföras. Detta berodde huvudsakligen på att tillverkaren av journalsystemet Cambio Healthcare System AB inte genomfört de förändringar i programmet som gör funktionen möjlig.

Diskussion

Inledning

Socialstyrelsen har under årens lopp mottagit många anmälningar om problem med databaserade patientjournalsystem. Anledningen till att sjukvården anmält dessa händelser till tillsynsmyndigheten har oftast varit att man förlorat patientdata därför att säkerhetskopieringen inte har fungerat. Det finns emellertid anledning att anta att Socialstyrelsen endast har sett en liten del av alla de problem som sjukvården brottas med när det gäller IT-system.

Tre av de redovisade fallen i denna Kamedorapport har anmälts till Socialstyrelsen enligt lex Maria [14]. I det fjärde fallet (införande av nytt bildsystem i Uppsala) konsulterades Socialstyrelsen under tiden som problemen förekom. Socialstyrelsen har gjort egna utredningar av de enligt lex Maria anmälda händelserna och bedömt vissa av fallen som mycket allvarliga. I Socialstyrelsens beslut finns krav på att organisationerna återrapporterar till myndigheten att de föreslagna åtgärderna har genomförts inom de angivna tidsramarna och att de har avsedd effekt.

I samtliga fall fanns risker för patientsäkerheten och händelserna medförde betydande extra kostnader. Det är sannolikt att några av händelserna kunde förhindrats om risk- och sårbarhetsanalyser gjorts och adekvata åtgärder vidtagits i tid. Kostnaderna som nu uppstod för att återställa driften efter de oplanerade och plötsliga avbrotten i IT-systemen har inte beräknats men har drabbat sjukvården, patienterna och samhället i övrigt.

Patientsäkerheten kan ha satts åsido när information om en enskild patient inte funnits tillgänglig och det medfört att undersökningar fått göras om eller operationer fått ställas in. Långvariga störningar i informationssystemen kan leda till att viktiga medicinska åtgärder försenas eller att allvarliga tillstånd inte uppmärksammas i tid. Individens integritet kan också påverkas vid informationsbortfall, vilket bedöms som en allvarlig incident i sig.

De samhällsekonomiska konsekvenserna kan bli stora om undersökningar och behandlingar får göras om eller kompletteras, sjukskrivningar kan behöva förlängas och personal saknas i organisationen och måste ersättas. Vård och omsorg är en mycket stor produktionsapparat och varje störning får stora konsekvenser – speciellt om man omsätter detta i ekonomiska

termer. I de redovisade fallen har inga beräkningar gjorts av de kostnader som orsakats av driftsavbrotten – vilket i sig är ett observandum. Det är emellertid troligt att kostnaderna hade kunnat minskas om tidiga varningstecken på svagheter i tekniken, uteblivna eller ofullständiga uppdateringar av säkerhetssystem hade observerats och adekvata åtgärder vidtagits.

Övriga aspekter som bör noteras är att tilltron till samhällsviktiga funktioner naggas i kanten när krånglande IT-system medför stora problem i sjukvården; befolkningen kan börja tvivla på att samhället i stort kommer att fungera i händelse av en katastrof.

Många utredningar och artiklar har ägnats åt informationssäkerhet och IT-säkerhet. En nationell IT-strategi för vård och omsorg har tagits fram på Socialdepartementet [2] och Socialstyrelsen har lagt fram en slutrapport om nationell informationsstruktur [15].

Ett närmare samarbete mellan MSB och Socialstyrelsen kan skapa en djupare insikt om risker och sårbarheter och i förlängningen ge förutsättningar för att minska antalet incidenter.

Ledningsfrågor

Ledningens engagemang och ansvar

Det kan tyckas som om ledningsansvariga i de aktuella organisationerna inte varit helt medvetna om den typ av problem som kan uppstå i en verksamhet som är så kritiskt beroende av databaserad informationsteknik. I de fall som beskrivs i denna rapport finns likartade förhållanden som kan vara orsak till de uppkomna problemen. Man kan anta att om organisationerna fullt ut hade följt gällande regelverk och standarder så borde inte IT-problemen ha uppkommit. Gemensamma vårdinformationssystem måste betraktas som samhällskritiska eftersom många patienter och sjukvårdens produktionskapacitet är beroende av dessa. Befolkningens förtroende för systemen beror på om systemen fungerar oklanderligt vid alla tider på dygnet 365 dagar om året.

Efter e-virusangreppet i Region Skåne 2009 begärde regiondirektören i Region Skåne att Socialstyrelsen skulle ta initiativ till ett arbete med att eliminera eller begränsa fenomenet e-virus samt att tydliggöra ansvaret för att skydda sig mot detta. I svaret från Socialstyrelsen [16] påpekas att nu gällande regelverk och tillhörande vägledningar och handböcker torde vara tillräckliga och att det i nuläget inte finns något behov av ett sådant initiativ. Hantering av informations- och IT-säkerheten, och därmed skyddet mot e-virus, är frågor som faller inom ramen för vårdgivarens ansvar.

I Socialstyrelsens författningssamling finns tre föreskrifter som indirekt eller direkt berör arbetet med IT-säkerhet. Först ska nämnas Socialsty-

relsens föreskrifter om ledningssystem (SOSFS 2005:12) [17] för kvalitet och patientsäkerhet i hälso- och sjukvården som kräver att vårdgivaren säkerställer att det finns ledningssystem för kvalitet och patientsäkerhet och tydliggör ansvarsrollerna i organisationen. När det gäller specifik användning och hantering av medicintekniska produkter anges i 3 kap. 6 § 3p i Socialstyrelsens föreskrifter (SOSFS2008:1) [9] om användning av medicintekniska produkter i hälso- och sjukvården att verksamhetschefen ska, efter uppdrag från vårdgivaren, ansvara för att de medicintekniska produkterna och anslutna informationssystemen är kontrollerade och korrekt installerade innan de används på patienter.

Slutligen finns Socialstyrelsens föreskrifter (SOSFS 2008:14) [18 och 19] om informationshantering och journalföring i hälso- och sjukvården tydlig när det gäller vårdgivarens ansvar för att det i verksamhetens ledningssystem finns en dokumenterad informationssäkerhetspolicy. Denna ska säkerställa att patientuppgifter är åtkomliga och användbara för den som är behörig, att uppgifterna är oförvanskade, att obehöriga inte ska kunna ta del av uppgifterna och att det är möjligt att spåra vem som har tagit del av en patientjournal. Vidare sägs att vårdgivaren ska utse person som ska ansvara för informationssäkerhetsarbetet. Denne eller dessa personer ska minst en gång om året rapportera till vårdgivaren vilka granskningar och skyddsåtgärder som har vidtagits.

Det finns ett flertal standarder för IT-drift som kan användas. De viktigaste torde vara SS-ISO/IEC 20000 [20] om informationsteknik – ledningssystem för tjänster och en handledning, samt SS-ISO/IEC 27000-serien [7] om ledningssystem för informationssäkerhet. Den nya standarden IEC/80001-1 [21] om riskhantering i nätverk som innehåller medicintekniska produkter bör också användas.

Sammanfattningsvis har ledningen ansvar för att det finns ett komplett kvalitetsledningssystem för IT-säkerhet. Detta ska omfatta risk- och sårbarhetsanalyser, kvalificeringstester vid förändrade förutsättningar, återkommande interna och externa granskningar samt regelbundna övningar med berörd personal. Vidare måste ledningssystemets organisation och handlingsplaner för krishantering vara tydliga och väl kända av all personal. Med hänvisning till de beskrivna händelserna i denna rapport är det inte troligt en fungerande kvalitetsledning skulle tillåta att kritiska IT-system placerades i samma serverhall eller att dokumentationsloggar för återställning av ett IT-system lagrades i samma lagringssystem som originalsystemet.

Katastrofplaner

Enligt lagen [22] om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap ska landstinget minska sårbarheten i sin verksamhet och ha en god förmåga att hantera krissituationer i fred. Med extraordinär händelse avses i denna lag en sådan händelse som avviker från det normala, innebär en allvarlig störning eller överhängande risk för en allvarlig störning i viktiga samhällsfunktioner och kräver skyndsamma insatser av en kommun eller ett landsting.

I analysen av händelserna i denna rapport kan man konstatera att vårdgivarnas katastrof- och beredskapsplaner endast marginellt innehöll instruktioner om hur man ska hantera allvarliga störningar i databaserade informationssystem. Sjukvården har blivit allt mer beroende av komplicerade tekniska system vilket innebär att kvaliteten snabbt kan försämras om tekniken upphör att fungera..

Allvarliga störningar i IT-system bör alltid innebära att beredskapsnivån höjs till minst stabsläge. Detta är viktigt eftersom någon med helhetssyn måste ta det funktionella ansvaret för både den direkta patientvården och tekniken. Om det i ett senare skede visar sig att incidenten inte är så allvarlig kan beredskapsnivån sänkas och ordinarie underhållsfunktioner åtgärda störningen.

Beredskapsplanering bör bygga på risk- och sårbarhetsanalyser, det framgår av Socialstyrelsens föreskrift [23] om fredstida katastrofmedicinsk beredskap och planläggning inför höjd beredskap. I föreskriften nämns att landstingen särskilt bör uppmärksamma situationer som allvarligt påverkar sjukvårdens funktionsförmåga eller tillgången på nödvändiga sjukvårdsresurser. Vidare nämns att vid planeringen av organisationen för den katastrofmedicinska beredskapen så bör tekniska och serviceinriktade funktioner ingå. Detta innebär bland annat att företrädare för IT- och MT-funktionerna bör medverka vid upprättande av katastrofplaner. Det bör också leda till att företrädare för dessa funktioner ingår i katastroforganisationen då krisen involverar dessa verksamheter.

I fallet med serverhallen i Kalmar hade en ”talesman” för händelsen behövt utses, påpekas det i landstingets egen utredning. Detta är en observation som bör uppmärksammas. När driftstörningar i komplicerade tekniska system inträffar bör en sakkunnig person finnas till hands som kan förklara problemen för massmedia och ge trovärdig information om när systemen åter förväntas fungera.

Beredskap i övrigt

Personalen i den sjukvårdande verksamheten måste vara utbildad och trä-

nad i att hantera situationer då IT- system inte fungerar. I redovisningen från en av de granskade händelserna framhålls att alla nyckelpersoner i den direkta patientvården måste få tillräcklig och adekvat information så fort som möjligt för att kunna fatta beslut om rätt åtgärder – antingen vänta på att IT-systemen åter fungerar eller övergå till reservrutiner. Här ska framhållas att det är olämpligt att ange nyckelpersoner eftersom sådana tenderar att vara frånvarande av olika skäl när de behövs. Istället ska nyckelfunktioner anges, det vill säga ansvarig befattning för berörd enhet. Av handlingarna framgår att man inom alla organisationer som drabbades av IT-avbrott hade reservrutiner att övergå till. Svårigheten var att veta när det skulle göras. Förutsättningen för att ta ställning till det var att få trovärdig information om när det ordinarie IT-systemet åter skulle kunna vara i drift igen.

IT-funktionen måste ha en beredskap att åtgärda problem i IT-systemen med den inställelsetid som den sjukvårdande verksamheten kräver. Inställelsetid och kompetens hos servicepersonal måste grundas på risk och sårbarhetsanalyser utgående från de krav som sjukvården ställer på IT-systemen. Motsvarande krav måste även gälla för den medicintekniska funktionen eftersom allt fler undersökningar och behandlingar görs med avancerad medicinteknisk utrustning, vilken dessutom kan vara ansluten till lokala eller gemensamma nätverk.

När IT-funktionen nås av larm om allvarlig driftstörning i IT-systemen måste alla systemägare omgående informeras så att alternativa metoder eller reservrutiner kan tillämpas. Om full redundans i vårdinformationssystemen inte kan skapas på grund av risker för att systemen kan skadas måste IT-ansvariga ha beredskap att snabbt utföra erforderliga kontroller innan funktionen läggs över på reservsystemen. Detta åtagande måste vara inskrivet i avtal mellan systemägare, leverantörer och användare.

IT- och MT-verksamheterna

Kravet på samverkan mellan IT- och MT-funktionerna i hälso- och sjukvården kan inte nog betonas eftersom de båda teknikområdena successivt integreras i delar som har avgörande betydelse för patientsäkerheten. Då den tekniska utvecklingen satte fart inom sjukvården på 1960-talet uppstod ett behov av medicintekniker i sjukvården för att biträda vårdpersonalen med sitt tekniska kunnande och för underhåll av den växande apparatparken. Ungefär vid den tiden kom också de första mindre datorerna som kunde användas för vissa beräkningar av medicinska uppgifter, till exempel på laboratorier. På 1980-talet blev persondatorerna också mer vanliga

i sjukvården, framförallt för administrativa uppgifter. Alla dessa datorer var ägnade åt specifika uppgifter och hade inte någon koppling till andra datorer eller system.

Interna datanätverk på sjukhusen och senare för hela landstingsområden började skapas under 1980-talet för att i första hand koppla samman datorer och gemensamma datalagringssystem för administrativa ändamål. Ungefär vid denna tid utvecklades digitala bildgivande system för röntgen, datortomografi, ultraljud, strålbehandling med mera. Dessa ställde också krav på stora datalagringssystem.

Under de senaste årtiondena har de medicintekniska utrustningarna mer allmänt försetts med datorfunktioner. Det har inneburit att resultat av provtagningar och andra undersökningar finns i digital form och är lätt att föra vidare i datanätverk. Man har i stor utsträckning använt sig av de befintliga datanätverk som skapats för administrativa ändamål istället för att bygga upp parallella medicinska nätverk. Patientjournaler, som numera bara förs i digital form, är tillgängliga för alla (behöriga) via nätverk.

Eftersom de två teknikområdena medicinsk teknik och informationsteknik således har uppstått vid olika tider och ur olika behov har företrädare för dessa områden format sina organisationer oberoende av varandra. På sjukhusen bildades medicintekniska enheter med lite olika placering i sjukhusens organisation, ibland ingående i en fastighets- eller försörjningsavdelning men också direkt underställda sjukhusledningen. Den medicintekniska verksamheten har alltid varit nära knuten till vård- och behandling av patienter. Medicinteknisk personal är därför ibland direkt anställd på kliniker med tekniskt avancerad utrustning. En egen MT-förvaltning på landstingsnivå finns endast på några få ställen i landet. IT-verksamhet har som regel alltid funnits centralt placerade på landstingsnivå även om det funnits sjukhusanknutna IT-enheter för den lokala servicen. Den utveckling som skett på det digitala området inom medicintekniken som visar att MT- och IT-organisationerna har gemensamma uppgifter för att patientsäkerheten ska upprätthållas.

En faktor att ta hänsyn till är den särskilda lagstiftning [8] som gäller för medicintekniska produkter. Tillverkaren har ansvar för produktens funktion så länge den används och underhålls i enlighet med tillverkarens anvisningar. Användaren får inte vidta några åtgärder på produkten utan tillverkarens godkännande. Uppgraderingar av program och uppdateringar med säkerhetspatchar får endast göras av tillverkaren om inte annat har avtalats mellan tillverkaren och användaren. Detta innebär att en IT-funktion som har ansvar för ett sjukhus/landstings intranät inte kan uppgradera program eller installera säkerhetspatchar i medicinteknisk utrustning på samma direkta sätt som i andra datorer i nätverket. Därtill krävs överens-

kommelser med berörda tillverkare. Vid ett e-virusangrepp i ett IT-system med många klienter krävs ett mycket snabbt och kraftfullt agerande styrt av en IT- och MT-gemensam handlingsplan. Detta kan emellertid försvåras om inte tydliga avtal finns med tillverkarna för de anslutna medicintekniska produkterna .

IT- och MT-organisationerna måste således samverka och formulera gemensamma krav vid upphandling av medicintekniska produkter med datorfunktion och hur produkterna under sin livstid ska skyddas mot farlig kod i form av till exempel e-virusangrepp. Samverkan måste också ske vid störningar i IT-systemen så att ansvaret för att vidta avhjälpande åtgärder är tydligt för IT, MT och externa leverantörer. Exempel på sådan tydlighet är gemensamma larmlistor med angivande av arbets- och ansvarsområden.

Kompetens och utbildning

Det förefaller som om kompetensen hos vårdgivarna att driva eller implementera komplexa och stora IT-system inte varit tillräckligt god. Den interna kunskapen måste höjas eller så måste vårdgivarna ha tillgång till erforderlig kompetens från externt håll. Det bör dock påpekas att om vårdgivaren avtalar med en extern leverantör att leverera dessa tjänster innebär det att kompetens också måste finnas inom organisationen så att man kan precisera vid upphandlingen vad man önskar. Vidare måste man kunna fortlöpande utvärdera och granska leveransen så att man får vad man upphandlat och att ansvaret som åligger respektive part är klarlagt.

Hos upphandlande enheter bör kompetensen att formulera avtal förbättras så att kravspecifikationer innehåller krav och villkor som speglar de ansvarsförhållanden mellan säljare och köpare som regleras i direktiv och författningar för medicintekniska produkter. Det innebär samtidigt att köparen måste ha en klar intern organisation med definierade ansvarsområden för informationsteknik, medicinsk teknik, fastighetsteknik (eller motsvarande) och för användarna i den direkta vården. Den upphandlande enheten bör också förvissa sig om att kravspecifikationerna motsvarar de behov som hälso- och sjukvården har för att kunna ge en god och säker vård.

Information och kommunikation

Ansvaret för spridning av information om allvarliga driftstörningar i IT-system eller andra försörjningssystem måste vara tydligt och välkänt för alla ansvariga på olika nivåer i landstinget. Respektive förvaltning/enhet måste bedöma vilka kanaler (t.ex. allanrop, sms, gruppfax, mobiltelefon) som är mest adekvata. Det kan till och med vara nödvändigt att förbereda

för att sprida intern information med personliga kurirer om allvarliga störningar inträffar (till exempel bortfall av el, intranät och telefon). Dock är det viktigt att säkerställa att det är budskap med samma innehåll som sänds ut. Det bör stämmas av med den regionala katastrofledningen, lokala krisberedskapsledningar eller motsvarande krisorganisationer.

Den regionala katastrofledningen fattar beslut om vilken information som bör ges till massmedierna. I ett krisläge på grund av allvarliga interna driftstörningar bör ledningen snabbt gå ut med information – annars gör andra det. Bland annat är det viktigt att informera allmänheten om telefonkösystem slutar fungera.

Vid planerade större förändringar eller installationer av IT-system och andra försörjningssystem som påverkar flera enheter bör en kommunikationsplan upprättas innan åtgärderna påbörjas.

Driftfrågor

Teknik

Den IT-verksamhet som ansvarar för stora organisationers IT-system har ett omfattande uppdrag. Det innebär bland annat att hålla nätverket inklusive lagringssystem, alla anslutna enheter och program uppdaterade med säkerhetspatchar. Vidare måste IT-verksamheten ha full kontroll över vilka datorer, minnesenheter eller apparater som ansluts till nätverket. Ett strikt regelsystem för detta måste finnas som respekteras och följs av alla som har tillgång till nätverket. När man rensade ut e-viruset som tagit sig in i Region Skånes nätverk fann man att många datorer, som var anslutna till nätverket, inte var kända av den ansvariga IT-verksamheten i regionen. Det var datorer som tillhörde enskilda forskare på universitetets medicinska institutioner och datorer som ingick i medicintekniska system för vård och behandling. De regler som då fanns var antingen inte tillräckligt tydliga när det gäller vad som fick anslutas till nätverket eller så var de inte kända eller respekterade av alla.

Tekniska förändringar i landsting eller på sjukhus initieras vanligen på verksamhetsnivå; ofta är det ny medicinsk teknik som behövs för att förbättra vård och behandling. I sådana situationer finns det inledningsvis minst tre parter, nämligen köparen/kliniken, säljaren/tillverkaren och upphandlingsfunktionen. Den sistnämnda sköter det formella, ofta i samarbete med en intern medicinteknisk enhet. Ytterligare intressenter tillkommer när det löpande underhållet ska bestämmas och definieras i avtal, antingen det ska skötas av en intern enhet på sjukhuset eller av en extern serviceorganisation. Om den nya tekniken ska anslutas till ett datanätverk måste även IT-verksamheten involveras i planeringen. För att detta ska fungera

inom hela organisationen måste verksamhetsansvariga på alla nivåer känna till regelsystemen, dels för medicintekniska produkter, dels för anslutning till befintliga IT-system.

Varje förändring av verksamheten måste föregås av en risk- och sårbarhetsanalys med syftet att upprätthålla patientsäkerheten. När riskanalyser görs inför upphandling av komplexa tekniska system som omfattar både medicinsk teknik och informationsteknik måste företrädare för både MT och IT delta. Det ska också framhållas att när program i medicintekniska produkter uppgraderas eller uppdateras måste tillverkaren göra en fullständig kontroll av produktens funktion och prestanda.

Dataprogram kan vara medicinteknisk produkt

I direktiv 2007/47/EG från Europaparlamentet [3] har klargjorts att programvara i sig själv är en medicinteknisk produkt när den av tillverkaren särskilt är avsedd att användas för ett eller flera medicinska syften som anges i definitionen av en medicinteknisk produkt.

Läkemedelsverket har i samarbete med Socialstyrelsen, Sveriges Standardiseringsinstitut SIS och branschorganisationer diskuterat frågan om programmerbara system för hantering av patientinformation [5]. Från vårdens sida finns uppfattningen att fristående programvaror och system som direkt eller indirekt påverkar diagnos, vård och behandling av patienter ska regleras under ett produktsäkerhetsregelverk. Arbetsgruppen har funnit att det mest lämpliga för närvarande är det medicintekniska regelverket, det vill säga lagen om medicintekniska produkter [8], samt Läkemedelsverkets [4] och Socialstyrelsens föreskrifter [9]. Arbetsgruppen menar att en programvara för medicinskt bruk måste betraktas som en ”produkt” och att begrepp som ”projekt”, ”tjänst” och liknande ska undvikas för att beskriva ett medicinskt informationssystem. Konkret innebär detta att det medicintekniska regelverket ska tillämpas för de programvaror och system som uppfyller definitionen av en medicinteknisk produkt. Reglerna om riskbedömning, verifiering och validering av enskild produkt och system, användande av tillämpliga standarder och bestämning av produktklass ska då göras. Dessutom påpekar arbetsgruppen att vårdgivarna konsekvent måste kräva CE-märkning för sådana system som bör betraktas som medicintekniska produkter.

Det förekommer inom sjukvården att dataprogram/programvara utvecklas för speciella ändamål av datakunniga medarbetare. Eftersom ett dataprogram under förutsättningarna ovan kan definieras som en medicinteknisk produkt gäller följaktligen Socialstyrelsens föreskrifter [9] om medicintekniska produkter som bland annat beskriver kraven på egentillverkning. Ett sådant ”hemmagjort” program ska genomgå den procedur

som beskrivs i föreskriftens 5 kap. om egentillverkning och godkännas av verksamhetschefen innan den används. Proceduren för egentillverkning följer de krav som ställs i EU-direktiv och Läkemedelsverkets föreskrifter [4] för medicintekniska produkter och har som syfte att garantera optimal patientsäkerhet. En egentillverkad produkt ska dock inte CE-märkas. Verksamhetschefen har alltid ansvar för att lämpliga och ändamålsenliga produkter används i patientvården och har genom CE-märkningen på kommersiellt tillverkade produkter en slags garanti för att produkten är lämplig när den används på det sätt som tillverkaren avsett. Om det ”hemmagjorda” dataprogrammet används utan att proceduren om egentillverkning följs tar verksamhetschefen en stor risk och har ensam det fulla ansvaret om fel skulle uppstå. När en egentillverkad medicinteknisk produkt konstrueras är det viktigt att följa standarderna SS-EN ISO 14971:2009 [24] om riskhantering för medicintekniska produkter och SS-EN 60601-1 [25] om säkerhet och väsentliga prestanda för elektrisk utrustning för medicinskt bruk.

Omgivande faktorer

Skadlig kod finns av olika slag och med olika verkan på datorer och nätverk. Gemensamt för alla är att de kommer in i nätverk eller enskilda datorer utan att användaren uppmärksammar att eller när intrånget görs. Det kan ske på olika sätt. Driftsäkerhet och tillgänglighet i IT-system är helt beroende av att datorer och servrar är skyddade och att programtillverkarnas senaste säkerhetspatchar är installerade. Vidare måste datanätverk vara skyddade med brandväggar, behörighetskoder och andra barriärer. Detta räcker dock inte om inte användare följer de strikta regler som måste gälla för att ansluta datorer, externa minnen och annan utrustning till nätverk eller till redan nätverksanslutna enheter. Här kan således talesättet att ”en kedja inte är starkare än dess svagaste länk” vara relevant.

I Region Skåne kom e-viruset W32/Downadup.CM in i intranätet och orsakade stor skada. Detta e-virus var ”intelligent skrivet” och kunde förändra sig själv så att installerade antivirusprogram inte upptäckte det. Det hade också förmågan att spärra installerade antivirusprogram så att de inte kunde hämta nya mönsterfiler. E-viruset hade därför kunnat ta sig förbi de barriärer och skydd som fanns och därmed kommit in i vissa av Region Skånes servrar, datorer och medicintekniska utrustning. I den efterföljande utredningen lyckades man hitta och isolera e-viruset i ett USB-minne, men man kunde också konstatera att det fanns flera luckor i barriärerna och skydden i det stora IT-system som utgjordes av cirka 35 000 enheter (administrativa och medicintekniska datorer, servrar/kluster, nätverksenheter, lagringssystem, skrivare med mera).

Medicintekniske chefen i Region Skåne fick information från Västra Götaland om att man där hittat e-virus på en av sina leverantörers USB-minne. Denna leverantör hade använt USB-minnet på Skånes Universitetssjukhus i Malmö dagarna innan e-virusangreppet i Region Skåne. Västra Götalands antivirusprogram identifierade detta virus som Conflicker 2009-01-08 och detta är en tidigare eller samma variant av det e-virus Region Skåne drabbades av. Detta visar att externa serviceföretag och leverantörer av medicinteknisk utrustning måste hålla samma säkerhetsnivå som krävs av sjukvården. Region Skåne har i sin ”Handlingsplan e-virus” systematiskt gått igenom alla de organisatoriska och tekniska förhållanden som IT-säkerheten är beroende av. Tydliga avtal mellan sjukvården och leverantörer vid anskaffning av medicinteknisk utrustning måste skrivas. Ansvar för uppdatering av antivirusprogram, installation av säkerhetspatchar, anslutning till nätverk och annan utrustning måste preciseras.

I detta sammanhang kan det vara intressant att reflektera över den skriftväxling som några år tidigare skedde mellan MTC-RS och Socialstyrelsen och Läkemedelsverket. I ett brev 2004 [26] till dessa myndigheter begär MTC-RS klarläggande, dels om tillverkarnas ansvar för att skydda levererade produkter mot e-virus, dels vad vårdgivarnas ansvar enligt gällande föreskrifter för användningen innebär.

Ett gemensamt svar inkom 2005 från Socialstyrelsen och Läkemedelsverket [27]. Enligt myndigheternas uppfattning har tillverkaren alltid fullt ansvar för säkerhet och funktion hos sin produkt då den används i den miljö och på det sätt som tillverkaren avsett. Detta gäller hela produkten inklusive eventuell programvara. Om tillverkaren har valt att använda programvaror från annan tillverkare (t.ex. Microsoft) i sin medicintekniska produkt ska tillverkaren ta ansvar för hela produkten inklusive av honom licensierad programvara.

Socialstyrelsen påpekar att det framgår av myndighetens föreskrifter (SOSFS 1996:24)[12] om kvalitetssystem i hälso- och sjukvården att systemen ska innehålla rutiner för inköp av varor och tjänster som påverkar kvaliteten i verksamheten och som säkerställer att lämpliga krav inklusive eventuella avtal om ansvar ställs så att kvalitets- och resultatmål i verksamheten uppnås. Vidare framgår enligt 3 § i Socialstyrelsens föreskrifter och allmänna råd (SOSFS 2001:12)[13] om användning och egentillverkning av medicintekniska produkter i hälso- och sjukvården att vårdgivaren har ansvaret för att bestämmelserna i 9 § i lagen om medicintekniska produkter [8] efterlevs. Detta betyder att endast de produkter som uppfyller kraven i lagen och Läkemedelsverkets författningar på området får tas i bruk. Myndigheterna menar därför att denna sak redan bör vara beaktad i samband med upphandlingen av medicintekniska produkter.

I svaret från myndigheterna sägs också att det normalt inte bör vara användaren som skall sköta uppdatering av programvaror i den medicintekniska produkten eftersom dessa ingrepp kan påverka funktionen hos den medicintekniska produkten. Det är vidare självklart att tillverkaren inte kan ta fullt ansvar för funktion och säkerhet hos sin produkt om nya, samverkande, programvaror ändras/installeras av användaren utan dennes vetskap.

I en artikel ”Datavirus och driftavbrott i datanätverk hotar patientsäkerheten”[28] i Läkartidningen 2007 beskriver Ulf Boström ett antal händelser i sjukvården då e-virus har orsakat problem med medicintekniska produkter anslutna till datanätverk.

Ett sätt att hålla sig informerad om aktuella problem och nya e-virus är att regelbundet besöka hemsidan www.cert.se eller att prenumerera på deras nyhetsbrev. CERT-SE är Sveriges nationella Computer Emergency Response Team med uppgift att stödja samhället i arbetet med att hantera och förebygga IT-incidenter. Verksamheten bedrivs vid Myndigheten för samhällsskydd och beredskap (MSB).

[12] Föreskriften är ersatt av Socialstyrelsens föreskrifter (SOSFS 2005:12) Ledningssystem för kvalitet och patientsäkerhet i hälso- och sjukvården [15].

Referenser

1. IT och sårbarhet - kritiska beroendeförhållanden i den nationella IT-infrastrukturen, KBMs temaserie, 2003:5
2. Nationell IT-strategi för vård och omsorg, Socialdepartementet, S2006:007 samt senare lägesrapporter
3. Europaparlamentets och rådets direktiv 2007/47/EG, Medicintekniska direktivet (MDD)
4. LVFS 2003:11 Läkemedelsverkets föreskrifter om medicintekniska produkter.
5. Förslag till vägledning för klassificering av vårdens mjukvarubaserade informationssystem. Läkemedelsverkets arbetsgrupp om Medicinska informationssystem. Projektredovisning, 2 juni 2009
6. Socialstyrelsen. Beslut 2010-07-16 i Lex Maria-ärende diarienummer 6393/2010. Angående ablationsbehandling som avbröts då datorn togs över via fjärrkontroll
7. SS-ISO/IEC 27000 serien, Informationsteknik - Säkerhetstekniker - Ledningssystem för informationssäkerhet
8. Lag (1993:584) om medicintekniska produkter
9. SOSFS 2008:1 Socialstyrelsens föreskrift om användningen av medicintekniska produkter i hälso- och sjukvården
10. Information Technology Infrastructure Library, ITIL, ITIL Foundation, www.itilfoundation.org.
11. Förvaltningsmodell pm3 från På i Stockholm AB. www.pais.se
12. SS-EN 9001: 2008 Ledningssystem för kvalitet
13. Basnivå för informationssäkerhet (BITS) KBM rekommenderar 2006:1
14. SOSFS 2005:28 Socialstyrelsens föreskrift och allmänna råd om anmälningsskyldighet enligt Lex Maria
15. Nationell Informationsstruktur – Slutrapport, Socialstyrelsen, 2009-12-27
16. Resare, P. Region Skånes begäran om Nationellt initiativ för bättre IT-säkerhet. Socialstyrelsen 2009-11-17

[13] Föreskriften är ersatt av Socialstyrelsens föreskrifter (SOSFS 2008:1) om användning av medicintekniska produkter i hälso- och sjukvården [12].

17. SOSFS 2005:12 Socialstyrelsens föreskrift om ledningssystem för kvalitet och patientsäkerhet i hälso- och sjukvården
18. SOSFS 2008:14 Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården
19. Handbok för tillämpning av SOSFS 2008:14
20. SS-ISO/IEC 20000-1/2:2007 Informationsteknik - Ledningssystem för tjänster - Del 1: Krav och Del 2: Vägledning
21. IEC/ISO 80001-1 Application of risk management for IT-networks incorporating medical devices. Part 1: Roles, responsibilitites and activities.
22. Lag (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap
23. SOSFS 2005:13 Socialstyrelsens föreskrifter och allmänna råd om fredstida katastrofmedicinsk beredskap och planläggning inför höjd beredskap; Socialstyrelsen 2005
24. SS-EN ISO 14971:2009, Medicintekniska produkter - Tillämpning av ett system för riskhantering för medicintekniska produkter
25. SS-EN 60601-1, Elektrisk utrustning för medicinskt bruk - Säkerhet och väsentliga prestanda
26. Holmer NG. Avvikelser på grund av e-virus som angriper programvara i medicintekniska produkter, MTP. Brev till Socialstyrelsen och Läkemedelsverket, 2004-08-11. Socialstyrelsens diarienummer 50 7399/2004.
27. Philipsson, L och Soop, M. Avvikelser på grund av e-virus som angriper programvara i medicintekniska produkter. Svar på brev från Holmer, NG. Läkemedelsverket och Socialstyrelsen 2005-04-28
28. Boström, U.: Datavirus och driftavbrott i datanätverk hotar patientsäkerheten, Läkartidningen nr 28-29 vol. 104: 2082-2086, 2007

Förteckning över Kamedo-rapporter

Nr	Titel	Utgivningsår
1	Katastrofmedicinska studier i USA. Beredskap mot naturkatastrofer	1966
2	Studiebesök i USA: American Medical Association's konferens om katastrofsjukvård i Chicago	1966
3	Katastrofmedicinska studier i Turkiet: Jordbävningskatastrof i Varto-området, augusti 1966	1967
4	Erfarenheter från naturkatastrof kongress i Skopje 25–30 oktober 1966	1967
5	Katastrofmedicinsk dokumentation: "Människor i katastrof". Genomgång av psykologisk och psykiatrisk litteratur av katastrofmedicinskt intresse	1968
6	Ej utgiven	
7	Katastrofmedicinska studier i Israel: Studier av krigssjukvården	1967
8	Katastrofmedicinska studier i Turkiet: Jordbävning i Debar 1967-11-30–12-02	1968
9	Katastrofmedicinska studier i Italien: Jordbävningskatastrofen på Sicilien, januari 1968	1968
10	Ej utgiven	
11	Katastrofmedicinsk organisation i Öst-Pakistan: Rapport från studieresa maj 1968	1969
12	Katastrofmedicinska studier i Indonesien: Vulkanen Merapis utbrott januari 1969	1969
13	Symposium om katastrofmedicin (utgiven som specialnummer av tidskriften Försvarsmakten)	1969
14	Katastrofmedicinska studier i Göteborg: Stormen "Ada"1969-09-21–22	1970
15	Katastrofmedicinska studier i Jugoslavien: Jordbävningen i Banja Luka 1969-10-26–27	1970
16	Katastrofmedicinska studier i Västtyskland: Smittkoppsepidemien i Meschede, Westfalen 1970	1970
17	Katastrofmedicinska studier i Turkiet: Jordbävningen i Kütahya-området mars 1970	1971
18	Katastrofmedicinska studier i Peru: Jordbävningskatastrofen 1970-05-31	1971
19	Katastrofmedicinska studier i Jugoslavien: Tågbrand i Wranduktunneln 1971-02-14	1971
20	Katastrofmedicinska studier i Jordanien: Redogörelse för arbetet vid Svenska Röda Korsets operationslag oktober 1970	1971
21	Studier i USA, september–oktober 1970: Utvecklingstendenser inom medicinsk utbildning och katastrofberedskap	1971
22	Katastrofmedicinska studier i Västtyskland: Järnvägskatastrof i Rheinweiler 1971-07-21	1972
23	Katastrofmedicinska studier i Glasgow: Gasexplosion i Clarkston 1971-10-21	1972
24	Katastrofmedicinska studier i Frankrike: Gasexplosion i Argenteuil 1971-12-21	1972
25	Katastrofmedicinska studier i Danmark: Fenolkatastrofen i Simmersted och Syd-Jylland den 20–23 januari 1972	1972
26	Katastrofmedicinska studier i Japan: Järnvägskatastrofen mellan Nagoya och Osaka den 25 oktober 1971	1973
27	Amerikansk krigskirurgi i Sydostasien: Erfarenheter i sam band med katastrofmedicinska studier 1972	1973

Nr	Titel	Utgivningsår
28	Katastrofmedicinska studier i Glasgow: Katastrof i Ibrox park fotbollsstadion den 2 januari 1971	1973
29	Katastrofmedicinska studier på Rhodos: Restaurangbranden 1972-09-23 Flygevakueringsoperationen	1973
30	Katastrofmedicinska studier i England: Seriekollisioner på motorväg M6 väster om Manchester 1971-09-31	1974
31	Katastrofmedicinska studier i Israel oktober 1973	1974
32	Katastrofmedicinska studier i Italien: Koleraepidemin i Syd-Italien 1973	1975
33	Katastrofövning på Sturup	1976
34	Katastrofmedicinska studier i Nord-Italien: Luftutsläppet av organiska klorföreningar i Seveso, Milano-provinsen 1976-07-10	1977
35	Totalhaveriet av tankfartyget ”Monte Urquio” vid La Coruna Spanien, maj 1976	1977
36	Katastrofmedicinska studier på Teneriffa: Flygplansolyckan på Los Rodeos-flygplatsen den 27 mars 1977	1977
37	Katastrofmedicinska studier i Tuve: Skredet den 30 november 1977	1978
38	Katastrofmedicinska studier: Psykiska reaktioner vid katastrofer	1979
39	Katastrofmedicinska studier i Borås: Hotellbranden 10 juni 1978	1979
40	Katastrofmedicinska studier i Spanien: Gasolyckan i Los Alfaques 11 juli 1978	1979
41	Katastrofmedicinska studier i Östersund: Järnvägsolyckan vid Lugnvik 10 augusti 1978	1979
42	Katastrofmedicinska studier i Mississauga, Kanada: Järnvägs olycka 10 november 1979 med åtföljande brand, klorutsläpp och behov av evakuering	1980
43	Katastrofmedicinska studier: Barn under krigs- och katastrof förhållanden. Deras upplevelser, beteenden och psykiska svårigheter	1981
44	Katastrofmedicinska studier i Nordsjön: Förlisningen av bostadsplattformen Alexander L. Kielland den 27 mars 1980	1981
45	Katastrofmedicinska studier i samband med två svenska järnvägsolyckor 1980: Tågkollisionen i Storsund 1980-06-02. Tågurspårningen i Upplands Väsby 1980-08-24	1981
46	Katastrofmedicinska studier i Bologna: Sprängattentatet på centralstationen den 2 augusti 1980	1981
47	Katastrofmedicinska studier i Nevada: Branden på MGM Grand Hotel i Las Vegas den 21 november 1980	1982
48	Katastrofmedicinska studier: Brännskadebehandling	1982
49	Katastrofmedicinska studier i Libanon: Beirut 82	1983
50	Katastrofmedicin – Kemiska olyckor	1984
51	Katastrofmedicinska studier i Mexico: Explosions och brandkatastrofen i San Juanico Ixhuatepec den 19 november 1984	1986
52	Katastrofmedicin – Kärnvapenkrig	1986
53	Katastrofmedicinska studier i Indien: Giftgasolyckan i Bhopal, december 1984	1987
54	Katastrofmedicinska studier i Hessen, Västtyskland: Tankbilsolyckan i Herborn 7 juli 1987	1988
55	SoS-rapport 1989:17 Färjeolyckan vid Zeebrügge den 6 mars 1987	1989
56	SoS-rapport 1990:30 Branden i tunnelbanestationen King’s Cross den 18 november 1987	1990
57	SoS-rapport 1990:31 Olyckan vid flyguppvisningen vid Ramsteinbasen den 28 augusti 1988	1990

Nr	Titel	Utgivningsår
58	SoS-rapport 1991:14 Flygplansbranden i Manchester den 22 augusti 1985	1991
59	SoS-rapport 1992:4 Kärnkraftsolyckan i Tjernobyl den 26 april 1986	1992
60	SoS-rapport 1993:3 Branden på passagerarfärjan Scandinavian Star den 7 april 1990	1993
61	SoS-rapport 1993:19 Branden på Huddinge sjukhus den 9 november 1991	1993
62	SoS-rapport 1994:2 Spårvagnsolyckan i Göteborg den 12 mars 1992	1994
63	SoS-rapport 1994:15 Flyghaveriet vid Gottröra den 27 december 1991	1994
64	SoS-rapport 1994:16 Jumbojetkatastrofen i Amsterdam den 4 oktober 1992	1994
65	SoS-rapport 1996:11 Rökgranatolyckan i Uppsala den 25 augusti 1993 och Klorgasolyckan vid Vanadisbadet i Stockholm den 2 augusti 1993	1996
66	SoS-rapport 1996:12 Jordbävningen i Kobe, Japan tisdagen den 17 januari 1995	1996
67	SoS-rapport 1996:20 Explosionen vid World Trade Center i New York den 26 februari 1993	1996
68	SoS-rapport 1997:15 Estoniakatastrofen M/S Estonias förlisning i Östersjön den 28 september 1994	1997
69	SoS-rapport 1997:20 Ebolaepidemin i Zaire 1995	1997
70	SoS-rapport 1998:14 Den tyska katastrofberedskapen belyst genom tre stora olyckor under 1996–97	1998
71	SoS-rapport 1998:20 Terroristattacken med sarin i Tokyo den 20 mars 1995	1998
72	SoS-rapport 1998:21 Bombattentaten i Jerusalem, Ashkelon och Tel-Aviv, våren 1996	1998
73	SoS-rapport 1999:4 Katastrofmedicinska studier under 35 år	1999
74	SoS-rapport 2000:9 Isstormen i östra Kanada januari 1998	2000
75	Brandkatastrofen i Göteborg natten 29–30 oktober 1998	2001
76	Översvämningar i Polen 1997 och i Sverige 2000	2001
77	MS Sleipners förlisning 26 november 1999	2003
78	Den kärntekniska olyckan i Japan 1999	2003
79	Tågolyckan i Tyskland 1998	2004
80	Tågolyckan i Storbritannien 1999	2004
81	Flygolyckan i Taiwan 2000	2004
82	Explosionen i fyrverkerilagret i Nederländerna 2000	2004
83	EU-toppmötet i Göteborg 2001	2004
84	Terrorattackerna mot World Trade Center 11 september 2001	2004
85	Husraset vid bröllopsfesten i Jerusalem 2001	2005
86	Explosionen i konstgödselfabriken i Frankrike 2001	2005
87	Bombattentatet i köpcentrumet i Finland 2002	2005
88	Översvämningarna i Tjeckien och östra Tyskland 2002	2006
89	Terrorattacken på Bali 2002	2006
90	Terrorattackerna i Madrid i Spanien 2004	2006
91	Flodvågskatastrofen i Asien 2004	2007
92	Evakueringen av svenskar från Libanon 2006 - Observatörsstudier i samband med kriget i Libanon sommaren 2006	2007
93	Strömavbrottet på Karolinska Universitetssjukhuset, Huddinge den 7 april 2007	2008
94	Stora busskrascher i Sverige 1997–2007	2010
95	SNAM-insatsen i samband med terroristattentatet i Bombay 2008	2011

Hälso- och sjukvården är i hög grad beroende av en fungerande informationsteknik. Störningar och avbrott påverkar ekonomin men framförallt patientsäkerheten negativt. Samtidigt har sektorn drabbats av ett ökande antal IT-haverier. I denna rapport redovisas fyra olika typer av haverier som inträffat i svensk sjukvård under perioden 2008- 2009: Ett e-virusangrepp i Region Skåne, ett journalsystemsbortfall inom Stockholms läns landsting, ett haveri i en serverhall på Länssjukhuset i Kalmar och införandet av bildsystem i landstinget i Uppsala län. Tre av haverierna har anmälts till Socialstyrelsen enligt lex Maria. De fyra typhändelserna illustrerar väl vad som kan hända, konsekvenser och möjliga åtgärder som minskar risken för upprepning. Rapporten presenterar lärdomar och erfarenheter av de fyra typhändelserna.

IT-haverier i vården
(artikelnr 2011-12-24) kan beställas från
Socialstyrelsens beställningsservice, 120 88 Stockholm
www.socialstyrelsen.se/publikationer
E-post: socialstyrelsen@strd.se
Fax: 08-779 96 67

Publikationen kan också laddas ner på
www.socialstyrelsen.se

Socialstyrelsen