Datavirus och driftavbrott i datanätverk hotar patientsäkerheten

Avvikelserapport eller Lex Maria-anmälan krävs vid risk för patientskada

ULF BOSTRÖM, överingenjör, teknologie licentiat, certifierad medicinsk civilingenjör, Medicinsk teknik Östergötland, Universitetssjukhuset i Linköping; sekreterare, standardiseringskommittén TK62 »Elektrisk utrustning för medicinskt bruk« inom Svenska Elektriska Kommissionen (SEK)
Ulf.Bostrom@lio.se

Sjukvårdens datanätverk med anslutna medicintekniska utrustningar är sårbara system, som kan äventyra patientsäkerheten och förorsaka stora kostnader om de inte konstrueras, integreras och övervakas på rätt sätt. Nya internationella standarder ställer krav på såväl nätverkens som de medicintekniska apparaternas säkerhet. Dessutom pekar dessa standarder på sjukvårdens ansvar för systemintegrationen. Det största hotet torde vara sabotage som nätverken kontinuerligt utsätts för i form av skadliga datorprogram, s k e-virus (e-virus är en generell term för olika typer av skadliga program såsom virus, maskar och trojaner). Även andra typer av driftavbrott i nätverk kan äventyra patientsäkerheten.

Ursprungligen installerades nätverk på sjukhus för administrativ databehandling. Därefter började man överföra laboratoriedata på dem. Idag överförs stora mängder data för olika medicinska ändamål i sjukvårdens nätverk. I synnerhet medicinska bilder från olika typer av diagnostiska utrustningar, t ex datortomografer och digitala röntgenapparater, genererar ofantliga mängder data som fordrar snabba nätverk.

Sjukvården driver på utvecklingen och kräver alltmer avancerade tillämpningar, t ex fjärrstyrda operationsrobotar så att en kirurg på ett sjukhus kan styra en robot i en operationssal på ett annat sjukhus. Det är självklart att man då måste ställa stora krav på säkerhet hos såväl utrustning som nätverk.

Idag integreras medicinska informationssystem, t ex patientjournaler, med medicintekniska produkter på ett sådant sätt att gränserna blir oklara. Detta skapar problem med tanke på säkerhets- och ansvarsfrågor.

För medicintekniska produkter gäller särskild lagstiftning (enligt Läkemedelsverkets föreskrifter om medicintekniska produkter, LVFS 2003:11), vilken kräver att tillverkare genomför riskanalyser, garanterar säkerheten och förser dem med CE-märkning. Det vore önskvärt att detta eller liknande regelverk införs för medicinska informationssystem.

Utvecklingen medför att sjukvården måste utveckla nya former för samarbete mellan medicintekniska avdelningar, som har kompetens vad gäller medicintekniska produkter, och IT-enheterna, som har kompetens vad gäller medicinska informationssystem och nätverk.

Svensk förening för medicinsk teknik och fysik, MTF, har tagit upp ovanstående problem och startat ett projekt kallat MIDS (Medicintekniska instrumentdatasystem) för att klargöra ansvarsområden, föreslå kompetenskrav och ge riktlinjer för samarbete mellan medicintekniska avdelningar och IT-enheter. Projektet beskrivs på MTFs webbplats ‹www.mtf.nu›, där också resultaten kommer att redovisas.

Grundläggande säkerhetskrav för medicintekniska apparater

International Electrotechnical Commission, IEC, specificerar i tredje utgåvan av den internationella standarden IEC 60601-1 [1] grundläggande säkerhetskrav och väsentliga prestanda för medicinteknisk utrustning. Enligt avsnitt 14.13 i denna utgåva skall tillverkaren i den tekniska beskrivningen specificera vilka egenskaper ett nätverk måste ha för att den medicintekniska apparaten skall kunna fungera i detta utan att säkerheten äventyras. Tillverkaren skall också ange risker som kan uppstå vid fel i nätverket. Vidare skall följande anvisningar till vårdgivaren finnas i den tekniska beskrivningen:

- Att anslutning via ett nätverk kan ge upphov till tidigare oidentifierade risker.
- Att vårdgivaren bör identifiera, analysera, värdera och kontrollera dessa risker.
- Att förändringar i nätverks-/datakopplingen, dvs anslutning och borttagning av objekt eller uppgradering av programvara, kan ge upphov till ytterligare risker som kräver förnyad analys.

Vissa medicintekniska apparater har konstruerats för att arbeta tillsammans med andra apparater via nätverk. Om användare inom sjukvården vill koppla in även annan utrustning måste vårdgivaren ta på sig tillverkaransvaret för det totala systemet och göra en riskanalys för att kunna garantera säkerheten med systemet.

Standarden IEC 60601-1 [1] konstaterar att någon måste ta ansvaret för det integrerade systemet och introducerar termen systemintegratör. Detta måste vara en enskild individ eller en särskild organisation. Ansvaret kan inte delas mellan olika tillverkare. Tillverkarens ansvar är att tillhandahålla nödvändiga specifikationer för en säker systemintegration. Standarden nämner som exempel att en vårdgivare kan träffa

SAMMANFATTAT

Vårdgivaren har enligt SOSFS 2005:12 ansvar för systemintegration av nätverk och medicinteknisk utrustning.
Tillverkaren har ansvaret för säkerheten med medicinteknisk utrustning inklusive dess programvara och inbäddade standardprogram, s k OTS-program.
Nätverksansluten medicinteknisk utrustning måste säkras mot e-virus och driftavbrott.
Angrepp av e-virus och problem vid driftavbrott skall utredas och dokumenteras samt rapporteras som avvikelse och eventuellt som Lex Maria-ärende.
Tydliga systemkrav måste anges vid upphandlingar av medicinteknisk utrustning som skall nätverksanslutas.

»Det är nödvändigt att sjukvården satsar på hög säkerhet i sina datanätverk.«

avtal med ett externt företag om att ta på sig ansvaret som systemintegratör.

En systemintegratör behöver känna till

- hur det integrerade systemet är tänkt att användas
- erforderliga prestanda för det integrerade systemet
- den tänkta konfigurationen av systemet
- begränsningar i möjligheten att utvidga systemet
- specifikationer och prestanda för all utrustning som skall integreras
- informationsflödet inne i och runt systemet.

En systemintegratör måste otvetydigt ha hög kompetens och stora befogenheter. Som typiska arbetsuppgifter anges följande:

- Att planera integration av medicinteknisk och annan utrustning med nätverket.
- Att genomföra riskanalys av det integrerade systemet och åtgärda upptäckta risker.
- Att till vårdgivaren vidarebefordra tillverkarnas instruktioner för säker drift av det integrerade systemet och varningar för risker som kan uppstå om konfigurationen ändras.

För att genomföra riskanalyser enligt ovan kan den internationella standarden ISO 14971 »Application of risk management to medical devices« [2] användas. Nyligen fattades beslut inom IEC att ta fram en mer specifik standard: IEC 80001 »Application of risk management for IT-networks incorporating medical devices«. Denna kommer att bli ett viktigt hjälpmedel för systemintegratörer.

Om en vårdgivare ansluter en medicinteknisk apparat till ett nätverk trots att tillverkaren inte uttryckligen angivit att detta är tillåtet tar vårdgivaren på sig ett tillverkaransvar enligt SOSFS 2001:12. Att vårdgivaren också är ansvarig för systemintegrationen följer av kravet på riskhantering i 4 kap 5 § SOSFS 2005:12.

Säkra programvaror

Det finns ingen kungsväg till säkra programvaror. Det finns nästan alltid fel, s k buggar, i dem. Den som utvecklar ett datorprogram förväntas testa detta. Men hur länge man än testar kan man inte garantera att alla buggar har hittats, och då man rättar till buggar finns alltid en risk att skapa nya fel.

Genom att utveckla programvaror för medicintekniska utrustningar efter den nya internationella standarden IEC 62304 »Medical device software – software life cycle processes« [3] bör man ha säkerställt att eventuella kvarvarande buggar inte medför några oacceptabla risker. Standarden kräver en systematisk utveckling av programvaran där man måste följa vissa regler. Det sista steget innebär en validering, dvs en kontroll av att programvaran kan göra det den är avsedd att göra på ett säkert sätt.

Eventuella kvarvarande buggar, som kan behöva rättas till, brukar upptäckas efter en tids användning. Leverantören kanske också av andra skäl vill modifiera programmet till en ny version. I så fall måste denna nya version valideras innan den installeras i utrustningar som redan är i bruk. I många fall vill tillverkaren göra snabbkorrigeringar av ett program genom att skicka ut en programfix. Det är då viktigt att även programfixarna är validerade.

När medicinteknisk utrustning kopplas in i nätverk kan nya säkerhetsrisker uppstå, t ex genom påverkan av programvaror på nätet eller i andra nätverksanslutna apparater. Det kanske allvarligaste hotet mot patientsäkerheten är e-virus som tar sig in i nätverket. Tillverkare måste gardera sig mot sådana hot. Särskilt problematiskt blir det när antivirusprogram installeras och regelbundet uppdateras, eftersom tillverkaren måste validera att utrustningen även klarar dessa uppdateringar.

Ofta använder sig programutvecklare av på marknaden befintliga standardprogramvaror. Sådana kallas på engelska »off-the-shelf (OTS) software«. Ansvaret för säkerheten med OTS-program ligger då hos tillverkaren av den medicintekniska apparaten.

Center for Devices and Radiological Health, CDRH, vid den amerikanska myndigheten Food and Drug Administration, FDA, har behandlat säkerhetsfrågor med nätverksansluten medicinteknisk utrustning i dokumentet »Guidance for industry – cybersecurity for networked medical devices containing off-the-shelf (OTS) software« [4]. Myndigheten anger tydligt att det är tillverkaren av medicinteknisk utrustning som har hela ansvaret även för OTS-program som används i medicinteknisk utrustning. I detta ansvar ingår också att validera varje programändring före installation på nya eller redan levererade utrustningar.

Alan Kusinitz, som representerar en tillverkare av medicintekniska produkter, behandlar samma frågeställningar i en artikel [5] och konstaterar: »We cannot rely on the assumption that Microsoft or the users of the Internet will protect the public health. That is not their job and they are not equipped to do it. It is our job as medical device manufacturers and if we can't do it then our devices should not be connected to networks.«

Konsekvenser av angrepp från e-virus

Alla nätverksanslutna apparater kan drabbas av e-virus. Den vanligaste effekten torde vara att nätverket överbelastas så att datakommunikation omöjliggörs. E-virus kan också skada utrustningen, t ex i form av hårddiskhaveri. Då medicinteknisk utrustning drabbas skulle även patienter kunna skadas. Några officiella rapporter om patientskador tycks dock inte finnas, trots att äldre utrustningar sannolikt inte är skyddade mot påverkan av annan programvara.

Scott Bolte, product security program manager vid GE Healthcare i USA, hävdar att urskillningslös tillämpning av IT-säkerhetsåtgärder i nätverk utan samråd med tillverkare kan hota patientsäkerheten på följande sätt [6]:

- Automatisk uppdatering och programkorrigering har medfört felfunktioner hos medicintekniska utrustningar.
- Test av nätverkets sårbarhet och antivirusprogram kan störa klinisk verksamhet, som kräver snabba svarstider i sina program.
- Feltolkning av kliniska data som datavirus kan störa pågående klinisk verksamhet.
- Vid upptäckt av fel måste behörighetskontrollen fortsätta att släppa in användare.

Exempel på virusattacker

Privat e-post smittade hela nätverket. En till sjukhusets nätverk ansluten ultraljudsapparat hade inbäddade Microsoft-program, som inte var säkerhetsuppdaterade. Leverantörens serviceingenjör använde i strid mot reglerna en bärbar dator även privat. När han öppnade en bilaga till ett e-postmeddelande smittades datorn av Melissa-viruset. När datorn sedan an-

vändes vid service på ultraljudsapparaten blev också denna smittad, liksom hela nätverket.

Anställds misstag ledde till allmänna råd. Den engelska myndigheten Medicines and Healthcare Products Regulatory Agency, MHRA, publicerade 2001 en riskrapport, SN2001(29), med rubriken »Breach of IT security in radiology PACS« med anledning av att ett sjukhus rapporterat e-virus i sitt bildhanteringssystem, ett s k PACS (picture archiving and communications system). Problemen uppstod då en anställd av misstag laddade ner information som innehöll e-virus. Detta spred sig och infekterade PACS-servrarna så att all kommunikation i nätverket blockerades.

Riskrapporten har nyligen ersatts av allmänna råd i dokumentet »Radiology PACS (picture archiving and communications system) – IT security« [7]. MHRA anger i detta nio olika åtgärder för att förhindra attacker av e-virus. Bland annat rekommenderas följande:

- Brandväggar mellan kritiska medicintekniska nätverk och allmänna nätverk.
- En central server för automatisk distribution av programfixar och uppdateringar av datorer.
- Rutiner som garanterar att externa serviceföretag följer sjukhusets krav på IT-säkerhet då man ansluter testutrustning, t ex bärbara datorer, direkt till nätverksansluten apparatur.

Sasser gav fråga till Socialstyrelsen och Läkemedelsverket. De medicintekniska cheferna i Region Skåne begärde 2004 i brev [8] till Läkemedelsverket och Socialstyrelsen klarläggande av hur Lagen om medicintekniska produkter (SFS 1993:584) och Socialstyrelsens föreskrifter och allmänna råd om användning och egentillverkning av medicintekniska produkter (SOSFS 2001:12) skall tillämpas avseende tillverkarens skydd mot e-virus.

Frågan ställdes med tanke på att det inom IT-verksamheten ansetts vara användarens, dvs vårdgivarens, ansvar att skydda sig mot e-virus genom att anskaffa och underhålla brandväggar, antivirusprogram och programuppdateringar. I brevet redovisades ett fall då masken Sasser smittade digitala röntgensystem (PACS), en datortomograf, ögonbottenbilder, journaler och dylikt. Vid tidigare attacker hade hjärtövervakningsanläggningar och ultraljudsapparater fått problem.

Läkemedelsverket och Socialstyrelsen svarade de medicintekniska cheferna i Region Skåne genom brev [9] att frågan om skydd mot e-virus och inkoppling av medicinteknisk utrustning till nätverk skall vara beaktad redan i samband med upphandling av produkterna. Myndigheterna ansåg att det normalt skall vara leverantören som sköter uppdatering av programvaror. Om vårdgivare väljer att själva sköta uppdateringar skall reglerna för egentillverkning enligt SOSFS 2001:12 tillämpas, vilket innebär att vårdgivaren själv har det fulla ansvaret för den medicintekniska produkten.

Av svaret framgår att anmälningsplikt vid problem med e-virus gäller för såväl vårdgivare som tillverkare. Innehållet i svaret finns tillgängligt på Läkemedelsverkets webbplats i dokumentet »Medicintekniska produkter som kopplas till Internet eller annat datanätverk« [10].

Nimda-masken drabbade Östergötland. Hela IT-nätet inom Landstinget i Östergötland drabbades av Nimda-masken i februari 2002. Den kom in i nätverket via en PC, vars virusskydd inte hade uppdaterats sedan 1998. En anställd öppnade en smittad bilaga i e-posten, varefter spridningen startade. Efter några timmar hade samtliga operativsystem av typ Windows NT och Windows 2000 slagits ut. Att spridningen fick ett aggressivt och snabbt förlopp berodde delvis på att ett stort antal servrar inte hade fullgott virusskydd – de var inte uppdaterade med de senaste programfixarna.

Effekten av angreppet blev att hela nätverket stängdes. All dataverksamhet inom landstinget drabbades, allt från tandvårdskliniker och vårdcentraler till större enheter som Universitetssjukhuset i Linköping. Det tog 8 dygn innan alla system fungerade fullt ut igen. Då hade 295 servrar och 5 250 persondatorer rensats från smittade filer och uppdaterats med fullgott virusskydd.

Operativsystemet Unix klarade sig, varför PACS-systemet på Universitetssjukhusets röntgenavdelning kunde användas. De patientadministrativa systemen Conrad och Kundrad var däremot inte tillgängliga under 1 dygn, varför det ibland saknades information om hur patienter skulle röntgas. I några fall fick patienter ligga kvar ett extra dygn i väntan på akut röntgenundersökning eller på grund av inställda operationer.

Förlossningsjournalen Obstetrix var inte tillgänglig under 2 dygn i Motala och Linköping samt under 3 dygn i Norrköping.

Journalsystemen i primärvården kunde inte användas under 1–2 dygn.

Strålbehandlingsmaskinerna på Universitetssjukhusets onkologiska klinik låg på ett eget nätverk och drabbades därför inte.

På Laboratoriemedicin fungerade inte systemet för inställning av läkemedlet warfarin för blodförtunning under 1 dygn.

Landstingsfastigheter fick fyra servrar så nedsmittade att styr- och regleröverövakningen på Universitetssjukhuset slogs ut. Viktiga driftfunktioner som övervakning av larm från centralgassystem, ventilation och hissar fungerade inte utan fick övervakas manuellt.

Landstingets kostnader på grund av virusattacken uppskattades till 1 800 000 kronor. Inga direkta patientskador uppstod vid virusangreppet, men risken för sådana måste bedömas som stor – i varje fall indirekt genom avsaknad av patientuppgifter.

Två bildplattesystem virusinfekterade i Göteborg. Två nyinstallerade röntgensystem i Göteborg, ett på Sahlgrenska Universitetssjukhuset/Östra och ett på Mölndals lasarett, drabbades våren 2005 av e-virus. På grund av oklarheter i upphandlingen hade leverantören inte installerat virusskydd. Apparaterna använde operativsystemet Windows XP, men det gick inte att surfa på Internet, läsa e-post eller ansluta externa CD-skivor eller USB-minnen till systemen. Ändå drabbades de av e-virus som sedan smittade ner andra objekt tills det inte längre gick att skicka digitala röntgenbilder.

Cirka 30 minuter efter angreppets början hade den centrala IT-enheten genom övervakning av nätet upptäckt att dessa två objekt var smittade. Nätverksanslutningarna drogs ur och rensning av systemen påbörjades. Leverantören accepterade sedan att sjukhusens normala antivirusprogram installerades, och dessutom installerades brandväggar. Övriga digitala röntgenapparater hade det äldre operativsystemet Windows NT4, som inte angreps av den aktuella masken.

MSBlast-masken smittade ultraljudsapparat. I avvikelsedatabasen reidarMTP (Rikstäckande elektronisk informationsdatabas för avvikelser rörande medicintekniska produk-

»Därför bör landsting och kommuner samarbeta så att man på ett enhetligt sätt utreder, dokumenterar, utvärderar och rapporterar säkerhetsbrister och nya hot mot datasäkerheten …«

ter), ‹http://www.reidar.se›, finns en rapport (diarienummer 581) från 2005 om att MSBlast-masken smittat en ultraljudsapparat. Apparaten hade några år tidigare skaffats till mammografiavdelningen för att anslutas till det befintliga PACS-systemet. Operativsystemet Windows 2000 ingick i utrustningen, men inga säkerhetsuppdateringar var gjorda och inget antivirusprogram fanns. Enligt leverantören skulle ett sådant ta för mycket datakraft i anspråk.

Genom övervakning av nätverket upptäckte IT-enheten att apparaten på ett onormalt sätt skickade datapaket via port 135. Porten stängdes, vilket medförde att det inte gick att registrera patienter och inte heller att lagra bilder i PACS-systemet. Problemet löstes genom att apparaten isolerades från nätverket med en brandvägg.

E-virusangrepp på Karolinska Universitetssjukhuset. I september 2006 rapporterade Svenska Dagbladet [11] att e-virus hade slagit ut flera datorer på Karolinska Universitetssjukhusets röntgenavdelning i Solna. Angrepp av flera olika typer av e-virus pågick den 11–31 augusti 2006 på bildplattesystem som använde operativsystemet Windows NT4 och antivirusprogrammet McAfee.

Vid upphandlingen tre år tidigare hade leverantören inte haft några specifika krav på nätverksanslutningen, utan accepterat det generella nätverket. Sjukhuset krävde att leverantören skulle sköta uppdateringen med Microsofts programfixar och acceptera sjukhusets antivirusprogram efter validering. Dessvärre hade Microsoft slutat med sin support av NT4 några år tidigare, och någon formell validering av att utrustningarna fungerade tillsammans med antivirusprogrammet gjordes aldrig. Sjukhuset hade inte heller ställt några specifika krav för nätverksanslutningen och hade ingen annan nätverkslösning att erbjuda.

Angreppet av e-virus började mycket diffust och slog till med full kraft efter två veckor då sju bildplattesystem på röntgenavdelningen slogs ut. Angreppet verkar ha haft flera faser och bestod av flera olika varianter av masken W32/Sdbot.

Att angreppet blev så omfattande och var svårt att komma till rätta med berodde på flera omständigheter, bl a att operativsystemet saknade programfixar. Det dök upp nya versioner av masken i så hög takt att man inte lyckades rensa med sjukhusets antivirusprogram. Det blev till och med nödvändigt att hämta en av antivirusleverantörens främsta experter från utlandet.

Medicintekniker, IT-tekniker liksom leverantörerna av både röntgenutrustning och antivirusprogram var inblandade i felsökning och rensningsförsök. Efter krismöten med divisionsledning och sjukhusledning gav man upp tanken på fortsatt drift med det aktuella bildplattesystemet och beslöt byta till ett annat fabrikat. Leverans och installation inklusive personalutbildning genomfördes på bara tre dagar.

Vid felsökningen fann man att flera ställen än röntgenavdelningen hade drabbats, bl a kemiska laboratoriet, som tvingades byta från Windows NT4 till XP på 180 datorer.

De direkta kostnaderna på grund av attacken uppskattades till 8 miljoner kronor. Om även indirekta kostnader medräknades blev summan 14 miljoner kronor. Därtill kan läggas andra mer svårbedömda kostnader såsom sjukhusets försämrade goodwill och samhällsekonomiska kostnader i form av patienternas omak och oro. En betydande del av de faktiska kostnaderna var en följd av besparingskrav på IT-sidan, vilket medfört att nödvändiga säkerhetsåtgärder inte genomförts tidigare.

Driftavbrott i datanät. En rapport från 1999 (diarienummer

»För att säkerheten i sådana system skall fungera krävs en tydlig ansvarsfördelning, skärpta behörighetsregler och ett aktivt säkerhetsarbete genom sektionering av nätverken, brandväggar, antivirusprogram och övervakning av nätverksfunktionerna.«

EXTERN8 i olycksdatabasen Reidar ‹http://www.reidar.se›) gällde en ögonbottenkamera, som förlorade bilder vid avbrott i nätverket. Efter genomförd ögonbottenangiografi skulle bilderna lagras på en CD-skiva via flera mellanlagringsstationer i nätverket. Bilderna förlorades vid avbrottet innan de hunnit till den slutliga lagringsstationen och kunde sedan inte återfinnas. Systemet var inte tillräckligt säkert mot avbrott i nätverket.

Nätverksåtgärd gav funktionsstörning i röntgensystem. I början av 2006 rapporterade ett sjukhus om problem med ett bildplattesystem för digitala röntgenbilder. Vid upphandlingen hade man krävt av leverantören att uppdatering med programfixar och obligatoriskt virusskydd skulle fungera. Trots detta förlorades kontakten med bildplatteläsaren. Problemet visade sig bero på att IT-avdelningen lagt med systemet i ett slags övergripande brandväggsdomän som tog över de inställningar som leverantören gjort i sin brandvägg. Kommunikationerna mellan leverantör, medicinteknisk avdelning och IT-avdelning hade inte fungerat tillräckligt bra.

Driftavbrott på »säkert« nätverk på universitetssjukhus. Ett universitetssjukhus rapporterade till reidarMTP under 2003 två likartade driftavbrott i nätverket som slog ut patientövervakningsutrustning. Den första rapporten föranledde en Lex Maria-anmälan till Socialstyrelsen med bedömningen »ett stort antal patienter utsatta för risk« på grund av driftavbrottet.

Sjukhuset trodde sig ha ett säkert system, eftersom övervakningsutrustningen var skild från nätverket. Den kommunicerade via ett virtuellt nätverk i sjukhusnätet med en övervakningsserver placerad i en datahall. Dessutom användes principen för redundanta system, vilket innebar att systemet kunde reparera sig självt vid felfunktion. I sjukhusnätverket fanns reservvägar som kunde användas vid felfunktion, men som inte fick vara öppna samtidigt som de ordinarie vägarna. Vid driftstörningarna i nätverket hade emellertid systemets intelligens satts ur spel så att parallella vägar var öppna. Isoleringen från nätverket hade upphört att fungera.

Vid den första driftstörningen rapporterades att övervakningscentraler och monitorer på intensivvårdsavdelningarna inte fungerade genom att kurvorna försvann eller att monitorerna startades om flera gånger. Totalt var 53 patienter på olika avdelningar utan övervakning i upp till 20 minuter.

Vid den andra driftstörningen slocknade monitorerna för övervakningen, och patientdatasystemet QS upphörde att fungera. Information om patienters cirkulation, andning, neurologiska status, laboratoriedata och omvårdnadsdokumentation under det senaste dygnet gick inte att komma åt. Problemet med övervakningen började samtidigt som sjukhusets nätverk drabbades av ett totalavbrott som varade i två timmar. Genom att koppla ur nätverksanslutningarna till monitorerna och göra omstart kunde övervakning startas vid patientplatserna, men utan tillgång till tidigare data.

Driftstörningarna visade att efter ett avbrott i nätverket kunde monitorerna inte återgå till normal funktion. Man beslöt att utreda lämpligheten av att använda virtuella nätverk för pati-

entövervakningsutrustning och stängde tills vidare av den redundanta kopplingsfunktionen i nätverket.

Nätverks komplexitet kräver aktivt säkerhetsarbete

Vid utredning av attackerna på Östergötlands läns landsting och Karolinska Universitetssjukhuset fann man att datanätverken är så stora och innehåller så många olika system att det är svårt att få en total överblick över alla anslutna enheter.

För att säkerheten i sådana system skall fungera krävs en tydlig ansvarsfördelning, skärpta behörighetsregler och ett aktivt säkerhetsarbete genom sektionering av nätverken, brandväggar, antivirusprogram och övervakning av nätverksfunktionerna.

Organisationen måste vara genomsyrad av en god säkerhetskultur, och personalen måste vara välutbildad och motiverad.

Rapporteringsskyldighet enligt föreskrifter

Trots att massmedier rapporterat om många virusangrepp på sjukhusnätverk har det inte gjorts några Lex Maria-anmälningar eller rapporter till Läkemedelsverket om virusangrepp. En förklaring till detta kan vara att datanätverk inte betraktas som en medicinteknisk produkt och att det därmed inte skulle falla under rapporteringsskyldigheten till Läkemedelsverket.

Även om ingen patientskada skett skall anmälan enligt SOSFS 2005:28 »Anmälningsskyldighet enligt Lex Maria« göras då risk för patientskador förelegat. I författningen nämns uttryckligen att felaktig användning eller felaktigt underhåll av medicintekniska produkter eller annan utrustning som tekniska försörjningssystem, nödkraftaggregat och informationssystem bör föranleda en anmälan.

En 6 § SOSFS 2001:12 skall olyckor med medicintekniska produkter också anmälas till berörd tillverkare eller dennes representant och till Läkemedelsverket.

Landstingen måste skärpa kraven i upphandlingar

Ett problem för tillverkarna är att vårdgivarna använder olika antivirusprogram och olika brandväggar. Det skulle underlätta om det fanns en branschstandard för sådana program. I avsaknad av detta måste landstingen skärpa kraven i upphandlingar och tydligt ange villkoren för att apparater skall få kopplas in på nätverk.

Landstinget i Östergötland kräver nu att leverantörer skall ge landstingets IT-enhet i uppdrag att installera det antivirusprogram som används inom landstinget. Vidare skall IT-enheten eller medicintekniker sköta uppdateringar av antivirusprogram och programfixar från Microsoft på leverantörens uppdrag.

Om leverantören inte accepterar detta skall han ange hur han vill sköta uppdateringar av antivirusprogram och programfixar. Ett av landstingets villkor är att kritiska säkerhetsrelaterade uppdateringar av operativsystem eller underliggande program skall implementeras omedelbart, medan icke-säkerhetskritiska uppdateringar skall införas senast tre månader efter det att de släppts.

Ett stort problem för leverantören torde vara att livslängden för operativsystem är betydligt kortare än för medicinteknisk utrustning. Så länge utrustningen används måste operativsystem och andra programvaror underhållas och uppdateras. Även denna fråga bör beaktas vid upphandling.

Nya säkerhetslösningar

Vissa tillverkare hävdar nu att de efter genomförd riskhantering låst operativsystemen så att antivirusprogram inte behövs. Det är viktigt att tillverkaren i sådana fall validerar att denna lösning fungerar även i aktuella nätverk.

Ett alternativ till konventionella antivirusprogram kan vara s k tillståndsbaserade e-virusskydd som arbetar med applikationscertifikat, vilket innebär att man endast tillåter åtgärder som är uttryckligen godkända. Alla andra processer är förbjudna. Program som arbetar med applikationscertifikat kräver en organisation för hantering av godkända program och utdelande av digitala certifikat. Sådana program måste också godkännas och valideras av tillverkaren.

Säkerheten i framtiden

Hittills verkar attacker av e-virus ha motiverats av en önskan att visa upp teknisk virtuositet genom förmågan att sabotera nätverk. På senare tid har e-virusen även blivit mer sofistikerade och svårare att upptäcka. Genom att de inte överbelastar näten tar det längre tid att upptäcka dem, och skadorna kan därmed bli större. Hotbilden har också förändrats från sabotage till kriminella handlingar såsom identitetsstöld, utpressning och misskreditering av andra leverantörer eller sjukhus. Sjukvården måste också skydda sig mot hackare som försöker komma åt sekretessbelagda patientuppgifter.

Det är nödvändigt att sjukvården satsar på hög säkerhet i sina datanätverk. Därför bör landsting och kommuner samarbeta så att man på ett enhetligt sätt utreder, dokumenterar, utvärderar och rapporterar säkerhetsbrister och nya hot mot datasäkerheten samt testar och utvärderar nya säkerhetslösningar. Det krävs också en strikt disciplin vid anslutning av utrustningar till nätverk och ett nära samarbete mellan IT-enheter, medicintekniska avdelningar, verksamhetschefer och leverantörer av såväl utrustningar som programvaror.

Potentiella bindningar eller jävsförhållanden: Inga uppgivna.

REFERENSER

1. International Electrotechnical Commission. IEC 60601-1:2005 Medical electrical equipment. Part 1: General requirements for basic safety and essential performance. 3rd ed. Geneva: International Electrotechnical Commission; 2005.
2. International Organization for Standardization. ISO 14971:2007 Medical devices – application of risk management to medical devices. Geneva: International Organization for Standardization; 2000.
3. International Electrotechnical Commission. IEC 62304:2006 Medical device software – software life cycle processes. Geneva: International Electrotechnical Commission; 2006.
4. Center for Devices and Radiological Health, CDRH. Guidance for industry – cybersecurity for networked medical devices containing off-the-shelf (OTS) software. 2005 Jan 14. http://www.fda.gov/cdrh/comp/guidance/1553.html
5. Kusinitz A. Making the software connection. Biomed Instrum Technol. 2005;39(3):248.
6. Bolte S. Cybersecurity for medical devices: Three threads intertwined. Presented to MedSun audio conference »Cybersecurity of Medical Devices«. 2005 April 12. http://www.medsun.net/participants/Uploads/ScottBolteGE.ppt
7. MHRA. Radiology PACS (picture archiving and communications system) – IT security. http://www.mhra.gov.uk/home/idcplg?IdcService=SS_GET_PAGE&useSecondary=true&ssDocName=CON2024755
8. Holmer NG. Avvikelser på grund av e-virus som angriper programvara i medicintekniska produkter, MTP. Brev till Socialstyrelsen och Läkemedelsverket, 2004 08 11. Dnr SOS: 50 7399/2004.
9. Philipson L, Soop M. Avvikelser på grund av e-virus som angriper programvara i medicintekniska produkter. Brev från Läkemedelsverket och Socialstyrelsen till NG Holmer, MTC Region Skåne. 2005 04 28. Dnr LV: 481:2004/45946.
10. Läkemedelsverket. Medicintekniska produkter som kopplas till Internet eller annat datanätverk. http://www.lakemedelsverket.se/Tpl/NormalPage____1586.aspx
11. Bondesson M. Datavirus slog ut sjukhusröntgen. Svenska Dagbladet. 2006-09-25. http://www.svd.se/dynamiskt/inrikes/did_13734112.asp