Säker IT-drift inom hälso- och sjukvården (HSN/1297/2021)

Bakgrund

I dag är verksamheter i hela samhället beroende av IT-baserade informationssystem. Detta gäller allt från kreditkortsbetalningar till trafikövervakning och patientjournaler. Samhällsviktiga funktioner som el- och vattenförsörjning är alltmer beroende av att kommunikation inom tele- och dataområdet fungerar. Med de senaste decenniernas snabba tekniska utveckling följer också sårbarheter vid dataintrång, spridning av skadlig kod eller om exempelvis nätförbindelsen bryts eller en programvara slutar fungera.

Enligt regionens Ledningssystem för informationssäkerhet (LIS) är informationssäkerhets-incident definierad som enskild eller flera oönskade eller oväntade händelser som har negativa konsekvenser för verksamheten och dess informationssäkerhet. Vid en informationssäkerhetsincident upprättas en incidentrapport för att möjliggöra uppföljning av säkerhetsincidenter och för att initiera förbättringsarbete/åtgärdsförslag.

Regionen har historiskt sett haft relativt få oplanerade IT-avbrott, men har under hösten drabbats av två större incidenter.

Den 1 september inträffade en driftsstörning klockan 05:06. En automatisk uppgradering av regionens interna brandvägg misslyckades, vilket fick till följd att ingen kunde logga in i regionens citrix-miljö. Inloggning i citrix-miljön är en förutsättning för åtkomst till en stor del av regionens verksamhetssystem. Klockan 09:00 var felet åtgärdat och IT-miljön fungerade som vanligt. Avbrottet medförde bl a att planerad vård fick ställas in eller senareläggas under samma dag. Händelsen klassificerades som 2 på en skala 1-4. Incident klass 2 är ”Mindre allvarlig”, vilket innebär t ex försök till dataintrång, misslyckade attacker eller missbruk av IT-resurser samt längre driftavbrott (<0,5 dagar) för verksamhetskritiska system.

Den 10 oktober inträffade ytterligare en driftsstörning ca kl 18. Sammanställning av incidentanalys pågår, så i dagsläget finns ingen rapport över händelseförloppet och orsaken till avbrottet. En felande komponent i regionens serverfarm är identifierad, men det utreds fortfarande varför omfattningen av störningen blev stor trots att arkitekturen är robust byggd och komponenten är redundant i flera led.

Hälso- och sjukvårdsnämnden beslutade 2021-09-23 att Regiondirektören får i uppdrag att till hälso- och sjukvårdsnämnden i november inkomma med redovisning över hur Regionen arbetar med att säkerställa en patientsäker verksamhet vid IT-störningar.

Arbetet med att säkerställa en patientsäker verksamhet vid IT-störningar kan delas in i tre olika perspektiv:

- Teknik, system och processer för att förutse och förebygga IT-störningar
- Reservlösningar och redundans när störningar och avbrott inträffar
- Manuella reservrutiner vid planerade och oplanerade avbrott.

Förutse och förebygga IT-störningar

För att förutse och förebygga IT-störningar krävs både övervakning av IT-miljön, skydd mot attacker och intrång samt systematiska och kvalitetssäkrade processer och rutiner.

En genomlysning av IT-funktionen har genomförts i syfte att etablera en bild av nuläget och de utvecklings- och förändringsbehov som finns inom IT-funktionen. Genomlysningen har bl a resulterat i en ny sourcingstrategi med indelning av IT-leveranser i tjänstekomponenter som upphandlats av externa parter och en etablering av regionens Helpdesk i egen regi. Den nya sourcingstrategin innebär även att uppgifter av strategisk karaktär, som idag ligger hos driftsleverantören, övertas av regionens personal. Under året har tjänsteansvariga för server och IT-arbetsplats, datanätverk samt Helpdesk rekryterats.

Regionen har tidigare köpt verktyg och IT-lösningar för övervakning och ärendehantering från externa part, som en del av IT-drift och Helpdesk. För att ge förutsättningar för leverantörsberoende och förbättrad kontroll, kommer regionen i fortsättningen att äga dessa verktyg samt faciliteter och hårdvara.

Vårdsystemet COSMIC är verksamhetskritiskt för informationsförsörjning och processtöd inom hälso- och sjukvården. För att säkerställa kontinuitet och höja regionens kompetens inom COSMIC teknik, har systemets applikationsdrift och teknikteam etablerats med regionanställd personal. Under 2022 kommer regionen även att förstärkas med resurser inom informatik och arkitektur.

En IT-säkerhetsplan för 2022-2024 har upprättas under september månad. Syftet är att systematiskt planera för IT-säkerhetshöjande åtgärder, såväl tekniska som organisatoriska samt att tydliggöra arbetet för övriga organisationen. Planen sträcker sig över tre år och baseras på återkommande självskattning mot CIS Cybersäkerhetskontroller. Regionens arbete med förbättrad IT-säkerhet följs upp inom ett antal olika aktivitetsgrupper. För att möta hoten från omvärlden kommer även SOC (security operations center) att upphandlas, för extern kontroll av regionens IT-säkerhet.

ITIL processer och roller för hantering av IT-tjänster håller på införas. Syftet är att säkerställa kvalitet, kontroll och styrning av IT-leveransen, såväl med externa parter som i regionens egen verksamhet. Utbildning av medarbetare samt dokumentation av rutiner pågår i samarbete med nya driftsleverantörer.

Reservlösningar och redundans

Reservlösningar kan bestå av en parallell IT-miljö, alternativa accessvägar, andra plattformar etc. Det finns dock inte en reservlösning som täcker alla typer av störningar, utan det beror helt på vad som orsakat avbrottet.

Regionen har genom åren byggt upp en relativt robust infrastruktur med flera datahallar som har redundant kraftförsörjning och diselkraft, redundant kylning och brandsläckning samt dubblerade serverar och datalagring. Regionen har även leverantörsavtal med hög servicenivå för olika infrastrukturkomponenter.

Manuella reservrutiner vid planerade och oplanerade avbrott

Checklista Reservrutin används vid planerade längre driftstopp i vårdsystemet COSMIC och den mobila plattformen NOVA. Journaler och övrig vårddokumentation finns tillgänglig i läskopia, i vilken även diktering av nya anteckningar kan göras. En pärm för Reservrutin driftstopp COSMIC ska finnas på varje enhet. Den ska förvaras på överenskommen plats och vara känd av samtliga medarbetare.

Reservrutiner för laboratorier och röntgen baseras på pappersremisser och speciella rutiner för hur svaren ska hanteras. Svar hämtas in till COSMIC automatiskt efter driftstart. Receptblanketter används vid för skrivning av läkemedel.

Det finns ingen generell rutin för oplanerade avbrott i vårdsystemet COSMIC. Samma rutiner vid oplanerade som vid planerade driftsstopp ska användas, men beroende på vad som orsakat avbrottet kan läskopia eller mobil plattform finnas tillgänglig. Om Citrix fungerar, men inte Cosmic eller läskopian är tillgänglig, ska särskild filarea användas för tillfällig lagring av diktat, enligt särskild rutin.

Reservrutiner vid bortfall av IT-system, finns för samtliga områden. Innehållet kan variera men oftast innehåller det telefonlista reservtelefoni och hjärtlarm.

Planerade avbrott i COSMIC

Den digitala utvecklingen går fort och COSMIC utvecklas ständigt för att bli ett bättre arbetsverktyg för alla i vården. Region Jämtland Härjedalen ingår i ett kundgrupps-samarbete som gemensamt har beslutat om en extrasatsning på 500 mkr, för att utveckla systemet över de närmsta åren. I nuläget släpps tre-fyra COSMIC versioner per år, där rekommendation från leverantör är att driftsätta åtminstonde tre av dessa versioner.

En ny version innehåller en rad förändringar. Dels är det ny funktionalitet, men också rättningar av felärenden och prestandaoptimeringar. Beroende på verksamhet sluten-, öppen- eller primärvård, kan de förändringar som introduceras vara av både större och mindre karaktär.

Inför varje ny leverans av COSMIC testas versionen i regionens interna testmiljöer. Tester utförs för att säkerställa att versionen fungerar bra och att det inte introduceras några fel i och med leveransen. Förutom COSMIC testas även de integrationer som finns till andra system t ex lab, röntgen, nationella e-tjänster.

I dagsläget kräver installationen av ny version ett driftstopp. Alla planerade uppgraderingar förankras och beslutas i COSMIC styrgrupp, som består av områdes-/ verksamhetschefer. Det har tidigare tagits beslut att driftstopp i största möjliga mån ska utföras under natten mellan torsdag och fredag, men när det inte är möjligt utförs arbetet under lördagar. De kan ske en rad olika aktiviteter under ett driftstopp. Dels installeras en ny version av systemet, men ibland kan det också behövas uppgraderingar/förändringar i någon övrig del av COSMIC infrastruktur. Beroende på vilka förändringar som introduceras kan det också krävas att konfiguration utförs under driftstoppet. Det utförs även testning i produktionsmiljön under ett driftstopp för att säkerställa att allt fungerar innan systemet blir tillgängligt för alla användare igen.

Eftersom det är många olika parametrar som påverkar skiljer sig tiden för hur lång tid ett driftstopp tar. Någon vecka innan planerat driftstopp utförs en generalrepetition i testmiljö och utifrån det kan driftstoppets längd uppskattas. Dock skiljer sig regionens test- och produktionsmiljö åt, så det är inte möjligt att uppskatta exakt hur lång tid driftstoppet kommer att ta.

Behov av ytterligare åtgärder för att säkerställa patientsäkerhet vid IT-störningar

Det är i första hand för vårdsystemet COSMIC som behovet av reservlösning är som störst. Sannolikhet och konsekvenser av IT-störning eller avbrott måste dock alltid vägas mot kostnaden för att bygga upp reservlösningar. Ett antal olika störningsscenarios som rör COSMIC har analyserats och förslag till rutiner samt teknik för att minska konsekvenser vid störningar har utformats.

Åtkomst till COSMIC kompletteras med flera tänkbara vägar, idag finns åtkomst via Citrix (COSMIC) och Ipad (NOVA). Åtkomstmöjligheterna kompletteras med att PC-klienter köps in och placeras på utvalda avdelningar, där behovet är som störst. En extra läskopia sätts upp i en separat databas på separata servrar i en egen datahall, befintlig reservhall eller externt. Den extra läskopian uppdateras mer sällan än den befintliga, 1-2 ggr per dygn. Det ger ett skydd mot eventuella fel som hinner skrivas över till den befintliga läskopian, som uppdateras var 15e minut.

PC-klienter i kombination med en extra läskopia skyddar mot bortfall av Citrix och ett osannolikt scenario att de två primära datahallarna slutar fungera, men reservhallen fungerar (extra läskopian). Lösningen förutsätter dock att datakommunikationen fungerar. En inventering behöver genomföras som underlag för beslut om vilka avdelningar som kan vara aktuella och hur många PC-klienter som behöver köpas in. Kostnaden är ca 10 000:- per PC-klient och skärm samt kostnad för ny servermiljö ca 200 000:-.

Vid bortfall av datakommunikation utreds ett förslag för att lindra konsekvenserna för verksamheten, som bygger på att det skapas ett ”COSMIC akutrum” i lokaler på sjukhuset dit det dras en egen fiber direkt från nuvarande reservdatahall, som är oberoende av befintligt nät. Det innebär att vid ett avbrott i datakommunikationen, så kan vårdsystemet nås via PC-klient med fysisk placering i ”COSMIC akutrum”. Rummet kan bemannas av personal från COSMIC förvaltningsorganisation, med uppgift att skriva ut information efter telefonbeställning från verksamheten.

Det trådlösa nätets täckning och prestanda behöver förbättras och en kostnadsuppskattning av detta är beställd av Regiondirektören