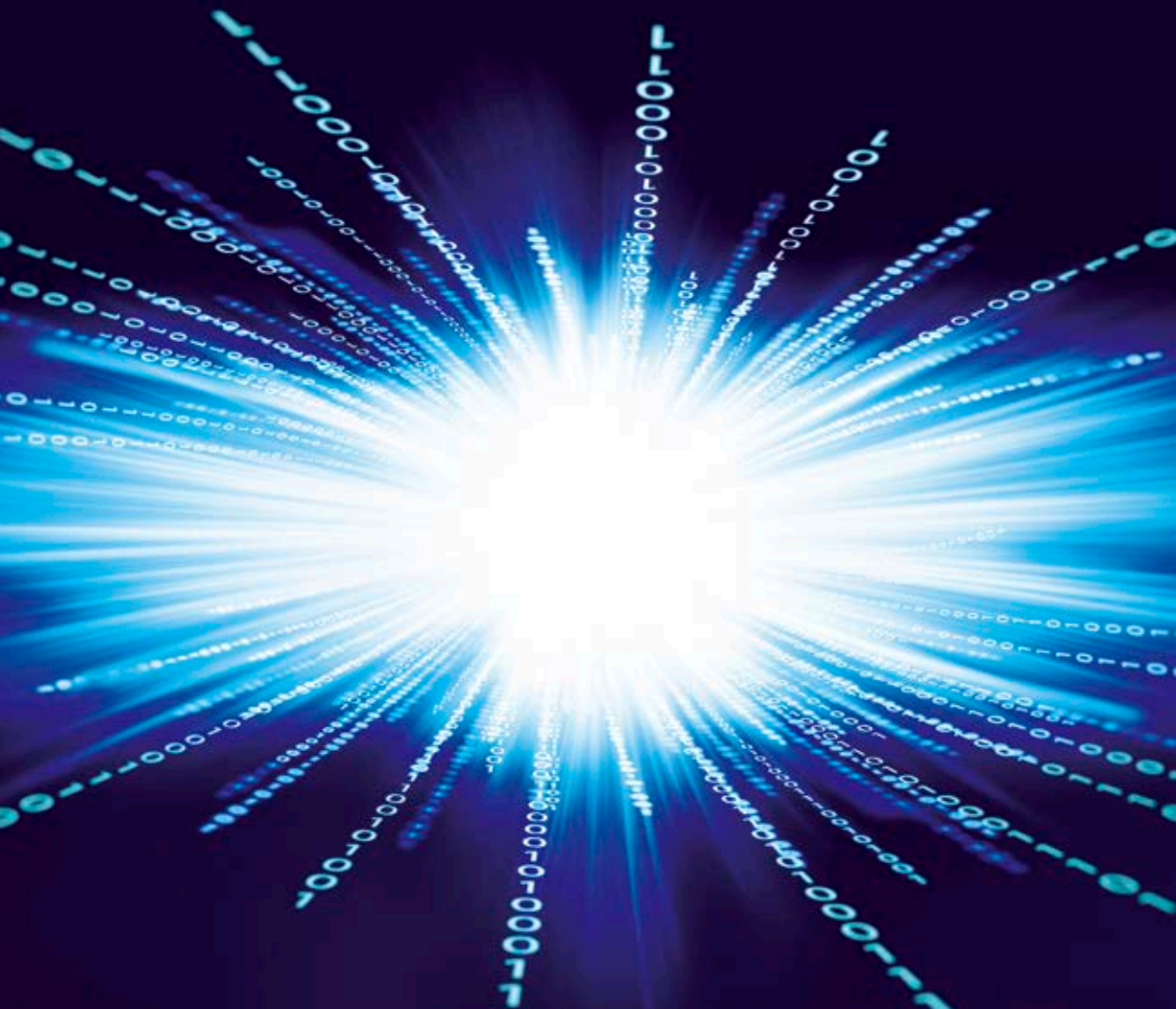
Myndigheten för samhällsskydd och beredskap

It- och informationssäkerhet i Sverige

Erfarenheter och reflektioner från några större it-incidenter under 2012–2014



It- och informationssäkerhet i Sverige

Erfarenheter och reflektioner från några större it-incidenter under 2012–2014

It- och informationssäkerhet i Sverige
Erfarenheter och reflektioner från några större it-incidenter under 2012–2014

Myndigheten för samhällsskydd och beredskap (MSB)

MSB:s kontaktpersoner:
Verksamheten för samhällets informations- och cybersäkerhet

Layout: Advant Produktionsbyrå
Tryck: DanagårdLiTHO

Publ.nr: MSB721 - januari 2015
ISBN: 978-91-7383-465-0

Innehållsförteckning

Förord **9**

Sammanfattning **11**

Inledning **15**

Om rapporten *15*

1. Exempel på inträffade incidenter 2012–2014 ..... **17**

1.1 Exempel på incidenter på informationssäkerhetsområdet 17

1.2 Överbelastningsattackerna i södra Sverige september 2013 17

1.2.1 Åtgärder och erfarenheter *19*

1.3 Skadlig kod Västra Götalandsregionen 2012 20

1.3.1 Åtgärder och erfarenheter *22*

1.4 Följdeffekterna av telestörning hos TDC i april 2013 23

1.4.1 Åtgärder och erfarenheter *24*

1.5 Nätverksbortfall och avbrotten i TakeCare i juni 2013 24

1.5.1 Åtgärder och erfarenheter *26*

1.6 Brand hos it-leverantören EVRY nyår 2013–2014 29

1.6.1 Åtgärder och erfarenheter *32*

2. Erfarenheter från händelserna **39**

2.1 Överbelastningsattacker 39

2.2 Skadlig kod 40

2.3 Följdeffekter av telestörning 40

2.4 Fel i operativsystem 41

2.5 Incident hos it-leverantör 41

3. Förmågan att förebygga **45**

3.1 Riskhantering och informationsklassning 45

3.2 Övningens betydelse för hanteringen 46

3.3 Relationen mellan kund och leverantör 46

4. Förmågan att hantera incidenter **51**

4.1 Kontinuitetshantering 51

4.2 Kommunikationens betydelse i incidenthanteringen 53

5. Övriga reflektioner **57**

5.1 Kostnadsaspekten 57

5.2 Återställningsprioritet 59

5.3 Timing och tur 60

6. Hur stärker vi då förmågan ytterligare? **63**

6.1 Ledningens engagemang måste öka 63

6.2 Förmågan att styra och prioritera måste stärkas 64

6.3 Förutsättningarna för lägesbild måste stärkas 65

6.4 Satsa på riskhantering och informationsklassning 66

6.5 Förmåga till kommunikation vid kris måste öka 66

6.6 Satsa på övning och kompetens 67

Bilagor **69**

Källor och underlag från intervjuer 69

Generellt underlag *69*

Överbelastningsattacker *70*

Skadlig kod samt intrång VGR *70*

Störning hos tele/nätoperatör *71*

Nätverksbortfall och fel i operativsystem *71*

Brand i datahall hos leverantör *72*

Kriskommunikation *73*

Skadlig kod – några lärdomar i korthet 74

Namn, akronymer och begrepp 75

Förord

Förord

Förmågan att upprätthålla samhällets funktionalitet är idag i mångt och mycket beroende av olika it-lösningar. Sverige har under de senaste åren drabbats av en rad stora it-incidenter som i olika grad har lett till konsekvenser för samhället. I november 2011 så drabbades it-driftleverantören Tieto av ett tekniskt fel, vilket kom att få direkta konsekvenser för cirka 50 av företagets kunder inom såväl privat som offentlig sektor. Sedan dess har ett flertal händelser, som på olika sätt har påverkat samhället skett. För att beskriva bredden på de konsekvenser som en it-incident kan ge upphov till har MSB nu analyserat ytterligare fem större incidenter som inträffade under perioden 2012–2014 där samhällets informationshantering påverkades kraftigt.

Denna rapport redovisar ett antal lärdomar och erfarenheter av krishantering vid dessa it-incidenter, både ur organisationens perspektiv men också som reflektioner ur ett samhällsperspektiv. Dessa lärdomar och erfarenheter kan förhoppningsvis användas för att stärka olika aktörers, och därmed samhällets, förmåga att förebygga och hantera it-incidenter. Därmed kan samhällets förmåga att motstå och återhämta sig från it-incidenter stärkas.

Stockholm 2015-01-20

Richard Oehme
Chef Verksamheten för samhällets informations- och cybersäkerhet
Myndigheten för samhällsskydd och beredskap (MSB)

Sammanfattning

Sammanfattning

Hur starkt står dagens samhälle mot de större it-incidenter som inträffar? Den tekniska utvecklingen – och även vårt ökande beroende av den – går svindlande snabbt. De starka beroenden mellan verksamhet och informationshantering som uppstått gör det ännu tydligare att ingen kedja är starkare än sin svagaste länk. En liten incident kan få oanade och ibland extrema konsekvenser. Medborgarna ställer krav på att verksamhet och tjänster ska kunna upprätthållas oavsett om it-systemen är tillgängliga eller ej, vilket gör att det krävs mycket planering och investeringar för att kunna erbjuda likhet i verksamheten under i stort sett alla förhållanden. Närhetsprincipen sätts på prov när den som äger data inte längre hanterar den, utan leverantören kanske befinner sig ett halvt jordklot bort.

I denna situation finns ett antal utmaningar. MSB kunde redan i analysen av Tieto-händelsen, som inträffade 2011, identifiera några centrala frågeställningar som är av vikt för att stärka informationssäkerheten. Några sådana var till exempel betydelsen av tydliga ansvarsförhållanden inom organisationer men även mellan organisationer som deltar i samma informationshanteringsprocesser.[1] Ytterligare slutsatser som lyftes i MSB:s Tietorapport 2011 var behovet av fungerande kontinuitetshantering och förmåga att bygga en nationell lägesbild vid större it-incidenter. Flera av dessa erfarenheter återkommer i denna rapport, vilket visar att arbetet med att stärka informationssäkerheten måste fortsätta.

Rapporten beskriver fem fall av incidenter, som inträffat på informationssäkerhetsområdet, i Sverige under perioden 2012–2014. Exemplen omfattar en tillgänglighetsattack, ett incident med skadlig kod, en telestörning, ett driftsstopp i ett system och en brand hos en it-leverantör. Fallen är valda för att visa på bredden av händelser som kan påverka informationssäkerheten.

Utifrån erfarenheterna från de beskrivna händelserna finns det ett antal åtgärder som bör vidtas om samhällets informationssäkerhet ska stärkas. Någon måste ta ansvar, sätter en kravställning och följa upp. **Ledningens engagemang vad avser informationssäkerhetsfrågor måste därför öka.**

1. Det kan gälla kommersiella relationer i form av outsourcing (utkontraktering) eller då myndigheter samarbetar kring olika typer av informationshanteringslösningar.

Aktörer, privata som offentliga, bör vidare **satsa på riskanalys och informationsklassning.** Ett systematiskt informationssäkerhetsarbete är förutsättningen både för fungerande kontinuitetshantering och för inkludera rätt krav på informationssäkerhet vid upphandlingar. I båda dessa aktiviteter är informationsklassning ett centralt stöd liksom tydlighet i rollfördelning mellan interna och externa parter.

En allt större del av den informationshantering som stödjer samhällsviktig verksamhet är idag utkontrakterad eller ombesörjs i gemensamma tjänster. I och med detta blir det av stor betydelse att de avtal som sluts mellan offentliga och privata aktörer kring informationshantering innehåller tydliga kravställningar kring informationssäkerhet och att ansvarsförhållandena regleras.

Vidare bör aktörernas **förmåga till kommunikation vid en kris öka.** Lyckas man hantera kommunikationen så ökar också möjligheterna att påverka hanteringen av krisen. Samhällets aktörer bör även **satsa mer på övning och utbildning** för att bättre klara incidenter på informationssäkerhetsområdet.

Erfarenheterna visar att samhällets **förutsättningar för en lägesbild fortsatt måste stärkas, liksom förmågan att styra och prioritera.** På en övergripande samhällsnivå finns, liksom vid Tietohändelsen 2011, fortsatt svårigheten att snabbt kunna skapa en lägesbild vid en större it-incident. Vidare finns det idag inga möjligheter för staten att vid en incident begära av en leverantör att samhällsviktig verksamhet ska prioriteras t.ex. vid uppstart.

Ansvarsförhållandena är viktiga i hela krishanteringssystemet och så bör de även vara när det gäller informationssäkerhet och it-säkerhet. De senaste åren har it-system byggts ut och beroendet av olika leverantörer av tjänster på it-området har ökat. Komplexiteten och hastigheten i förändringarna har tyvärr medfört att ansvarsförhållande mellan informationsägare och system/tjänsteägare ibland blivit otydlig vilket är till stor nackdel för informationssäkerheten.

Rapporten belyser även ett antal, tidigare inte belysta faktorer som påverkar informationssäkerheten och arbetet med den. Dessa aspekter inkluderar kostnader, återställningsprioritet och faktorn timing och tur. Flera av incidenterna i denna rapport har medfört stora kostnader. Trots det tvekar många aktörer att satsa på redundans t.ex. i form av dubblerad datalagring. Att få ner kostnaderna för it-hantering är idag en mycket starkt pådrivande faktor för

att t.ex. välja en extern it-leverantör, men flera av de intervjuade anser att utkontraktering lika mycket är ett måste p.g.a. höga krav från användarna på flexibilitet och utvecklingskrav på den tekniska miljön.

Vid en akut incident måste it-leverantörerna prioritera vilken kund alternativt vilka system som ska prioriteras vid hanteringen. Leverantörerna uppgav vid intervjuer att prioriteringen huvudsakligen skedde efter vad leverantören uppfattade som samhällsviktigt, hur kundens avtal var formulerat och hur kundens egen hårdvara var konfigurerad och där nyare utrustning prioriterades.

Samhällets funktionalitet är idag beroende av att enskilda aktörer tar sitt ansvar för att säkra informationssäkerheten. För att få en genomgående god informationssäkerhet krävs att alla aktörer arbetar aktivt med systematisk informationssäkerhet. Samtliga aktörer i samhället måste ta ett ansvar för att se till att it- och informationssäkerheten stärks. Vi är alla beroende av varandra i det nya högteknologiska samhället.

Inledning

Inledning

Samhällets funktionalitet bygger idag mycket på att vi kan lita på att de it-system vi använder fungerar som de ska. För att skydda samhällets funktionalitet är det av stor vikt att it-system har förmåga till kontinuitet även under svåra förhållanden och att vi kan skydda information enligt aspekterna riktighet, konfidentialitet, spårbarhet och tillgänglighet.

Den här rapporten kan förhoppningsvis bidra till att öka förståelsen för vikten av att arbeta med informationssäkerhet och hur man kan gå vidare i arbetet, både inom enskilda organisationer och på samhällsnivå.

Om rapporten

Rapporten följer MSB:s inriktning för området samhällskydd och beredskap. I första kapitlet beskrivs ett urval informationssäkerhetsincidenter som förekommit under perioden 2012–2014. I de följande kapitlen beskrivs därefter erfarenheter utifrån olika perspektiv. I kapitel 2 beskrivs de generella lärdomar som kan dras från respektive typfall. Därefter görs i kapitel 3 och 4 en genomgång av vilka förmågor som aktörerna bör stärka för att klara it-incidenter bättre. Avsnittet om förmågeuppbyggandet har, för att förenkla för läsaren, delats in i två kapitel; ett med fokus på förebyggande arbete respektive ett på hantering när väl incidenten inträffat. I ett avslutande kapitel görs sedan några reflektioner utifrån ämnen som kom upp under de intervjuer som gjordes som underlag för rapporten.

Underlaget till rapporten består främst av intervjuer med, de i rapporten presenterade incidenterna, berörda aktörer, men även av incident- och granskningsrapporter samt material från media. I förekommande fall har CIO/informationssäkerhets- och/eller säkerhetsfunktioner intervjuats. Även verksamhetsägare och incidentmanager/driftansvariga och Business continuity managers har intervjuats.

Målgruppen för denna rapport är främst aktörer med ansvar för kontinuitet och riskhantering i olika typer av samhällsviktig verksamhet. Rapporten kan även vara av intresse för andra aktörer i samhället, som vill stärka sin kontinuitetshantering.

Vi vill tacka samtliga aktörer som bidragit till denna rapport. Denna rapport hade inte kunna göras utan att ni delat med er av era erfarenheter!

Exempel på inträffade incidenter 2012–2014

1. Exempel på inträffade incidenter 2012–2014

1.1 Exempel på incidenter på informationssäkerhetsområdet

Det är många typer av händelser som kan hota it- och informationssäkerheten.

För att exemplifiera de problem som kan uppstå som en effekt av en incident så beskrivs här fem typer av incidenter, som inträffat på informationssäkerhetsområdet, i Sverige under perioden 2012–2014. Fallen har valts för att visa på bredden av händelser som kan påverka informationssäkerheten hos en organisation.

De fem exemplen omfattar

- en tillgänglighetsattack mot södra Sverige i september 2013
- skadlig kod som drabbade Västra Götalandsregionen i december 2012
- en mindre telestörning hos telebolaget TDC i april 2013
- ett driftstopp i systemet TakeCare utlöst av ett fel i operativsystemet i juni 2013
- en brand hos it-tjänsteföretaget EVRY i december 2013.

Varje fall inleds med en kort beskrivning av själva incidenten och de huvudsakliga konsekvenser. Därefter redogörs översiktligt för de åtgärder som berörda aktörer vidtog eller övervägde under och efter händelsen.

1.2 Överbelastningsattackerna i södra Sverige september 2013

Under september 2013 utsattes flera sydsvenska kommuner och trafikföretag för överbelastningsattacker[2]. De började mot Skånetrafiken måndagen 16 september. Under tisdagen drabbades även Region Skåne, Jönköpings kommun och Admax (ett webbhotell) av korta överbelastningsattacker. Onsdagen 18 september utsattes SJ AB:s leverantör för en kort överbelastningsattack. Problemen fortsatte under torsdagen då även Helsingborgs kommun och Malmö stad drabbades.

2. Överbelastningsattacker innebär i regel att system eller nätverksresurser blir otillgängliga på grund av att stora datamängder riktas mot en aktörs datasystem.

Skånetrafiken

De konsekvenser som Skånetrafiken upplevde var främst relaterade till deras biljettförsäljning, men de fick även störningar i reseplaneraren via http://www.reseplaneraren.skanetrafiken.se. Skånetrafiken gick dock att nå via telefon. För att minska trycket mot sina system valde Skånetrafiken att temporärt stoppa utländsk trafik till sina datasystem. Detta gav dock till följd att vissa kortbetalningar inte kunde utföras. Vidare störtes företagets bokningssystem för anropsstyrd trafik, en funktion som Skånetrafiken själv anser vara ”samhällskritisk verksamhet”[3].

Region Skåne

Region Skåne utsattes för tre attacker. Attackerna påverkade tillgängligheten till deras externa internetkoppling (e-post, hemsida, distansinloggning) samt Region Skånes koppling till Sjunet[4] med tjänster som e-recept och 1177 Rådgivningsstöd[5]. När det gäller sjukvårdsrådgivningen omfördelades trafik så att andra landsting tog över frågor från Region Skånes upptagningsområde. Generellt så fungerade den interna verksamheten och informationstillgången bra. De hade dock problem med system som hade kontakt med spärrlistor till behörighetskontroll via internet, vilket innebar att man inte kunde upprätthålla stark autentisering i systemen och i vissa fall att det inte var möjligt att logga in.

Överföringen av EKG-värden från ambulanser fungerade inte, men risken för patientsäkerheten var begränsad eftersom manuella reservrutiner kunde tillämpas.

Övriga drabbade aktörer

De kommuner som använde IP-telefoni fick problem, likaså de som i sin telefonväxel använde tjänster som var beroende av internet. Kävlinge kommuns hemsida var inte nåbar under några timmar.[6]

Eftersom flera aktörer som blev utsatta för överbelastningsattacken använde samma it-leverantör, så uppstod som följdeffekt att problem även drabbade andra kunder som initialt inte varit utsatta för attacken. Till exempel drabbades Systembolagets hemsida av tillgänglighetsproblem till följd av leverantörens felsökning.

3. Anropsstyrd trafik är trafik som endast utförs om någon i förväg begärt att få resa. Den mest omfattande anropsstyrda trafiken är resor i färdtjänst och sjukresor.
4. Nätet ska ha garanterad tillgänglighet. Nätet används idag för över 100 olika tjänster, bl.a. e-recept och överföring av patientjournaler.
5. Region Skåne definierade det som system med kopplingar och beroenden till skane.se.
6. Kommunen satte själva attacken i samband med de överbelastningsattacker som ägde rum ett halvår tidigare (6–8 februari 2013).

Vidare låg SJ AB:s bokningssystem via webb och mobil nere under flera timmar av samma orsak. Vissa interna system hos SJ påverkades även eftersom de var ihopkopplade med det externa nätet.

1.2.1 Åtgärder och erfarenheter

På kort sikt – under hanteringsfasen

SJ, Skånetrafiken och Region Skåne valde att filtrera bort utländsk trafik under några dagar. Transportföretagen fick under tiden övergå till manuella rutiner. Resenärer som inte kunnat köpa biljetter på grund av de utslagna betalningsfunktionerna kunde dock ändå fullfölja sin resa.

Vissa av SJ AB:s kunder hade inte svensk uppkoppling (svenska ip-adresser) och kunde därmed inte köpa biljetter. Några av dessa kunder valde då att gå över till en temporär lösning i form av 3G-donglar[7], som gjorde det möjligt för dem att använda svenska telenätet.

SJ AB uppger att det tog lång tid innan de fick besked av leverantören om att det var en överbelastningsattack de var utsatta för. Leverantören letade nätverksproblem vilket var den indikator som de såg. SJ hade vid denna tidpunkt enbart ett mycket rudimentärt skydd mot överbelastningsattacker och inga egna övervakningsverktyg, vilket gjorde dem beroende av leverantörens bedömning. SJ AB:s erfarenhet är att en bra incidenthanteringsrutin är av mycket stor vikt.

Region Skåne styrde om sitt telefonsystem så att andra landsting gick in och stöttade sjukvårdsrådgivningen 1177.

Kävlinge kommun hade efter tidigare attacker sett till att försöka skydda sin verksamhet mot överbelastningsattacker men detta gav dock inte tillräckligt skydd för den massiva attack som kom i september.

Efter händelsen

SJ AB hade återverkningar i cirka två veckor efter överbelastningsattacken. Efter att ha utsatts för ett antal incidenter valde SJ att ta fram ett överbelastningsskydd tillsammans med sin internetleverantör. SJ har idag satsat på skydd genom bl.a. protokollfiltrering. Bolagets slutsats är att det enda sättet att skydda sig är att sätta upp en lösning tillsammans med internetleverantören.

7. En form av externt trådlöst modem, ofta i form av en USB-sticka.

Samma lösning har även SkåneTrafiken och Region Skåne implementerat. De har utökade protokollfilter och även bevakning på sin nättrafik för att få en tidig varning om något håller på att hända.

1.3 Skadlig kod Västra Götalandsregionen 2012

Måndagen 17 december 2012 får Västra Götalandsregionens it-system, VGR IT, tillgänglighetsproblem med Sjunet[8]. VGR:s it-funktion har initialt svårt att hitta en förklaring till problemen men åtgärdade ändå tillgänglighetsproblemen.

Allt från läkemedelsautomater till sjukvårdsrådgivningen drabbas

Därefter inträffar händelser som först inte uppfattas höra ihop med de rapporterade problemen i Sjunet. En lokal enhet till Sjukhusapoteket i Borås rapporterar att deras inloggningsbild till Sjunet ser annorlunda ut. Vid Södra Älvsborgs sjukhus undrar man också om datorn som styr läkemedelsautomaterna[9] har förändrats utan att det meddelats. Senare framkommer att styrdatorn till läkemedelsautomaterna har ett testanvändarkonto med ett mycket svagt lösenord. Genom att utnyttja detta svaga lösenord försöker nu en smittad dator infektera styrdatorn, men hindras av ett uppdaterat virusskydd.

Under tisdagen får också VGR e-post från ett amerikanskt universitet, som uppger att en ip-adress tillhörande VGR används för att attackera universitetet. Ip-numret visar sig tillhöra en dator som styr larm för bl.a. vatten och värme vid Mölndals sjukhus, som ingår i samma sjukhusgrupp som Sahlgrenska universitetssjukhuset. Det som händer är att ett mycket litet antal av VGR:s 45 000 datorer används för att leta efter andra datorer att infektera och att fjärrstyra. De infekterade datorerna söker både inom och utanför VGR:s eget nätverk. Det förekommer även falska (spoofade) ip-adresser, vilket gör arbetet att spåra de infekterade datorerna svårt.

Som en följd av detta belastas VGR:s nätverk så hårt att flera funktioner slås ut eller får omfattande problem. Liknelsen kan göras med att Västra Götalandsregionen utsätts för en intern form av överbelastningsattack, eventuellt i syfte att utgöra attackplattform för någon annan. Fortsatt är det dock problemen med åtkomst till Sjunet som ställer till störst problem.

8. För beskrivning av Sjunet se bilaga 3.
9. Läkemedelsautomater är en elektroniskt styrd lagerplats för läkemedel.

VGR IT arbetar dygnet runt under flera dagar med att få bukt med incidenten, trots att endast ett fåtal datorer infekterats. Även om stora arbetsinsatser görs så går det inte att spåra källan till viruset, eftersom loggningsverktyg på VGR:s datorer inte installerats eller är otillräckligt konfigurerade.

Belastningen på VGR:s nätverk skapade störningar bl.a. i tillgången till e-recept och det regionsgemensamma e-journalsystemet för ambulanssjukvården, men även till webbaserade tjänster för samtalshantering, som t.ex. sjukvårdsrådgivningen 1177 och tjänster för fastighetsstyrning. Även internetförbindelsen och funktioner i regionens it-miljö sattes ur spel.

På Skaraborgs sjukhus drabbades ett system som används för att göra bedömningar på hjärtpatienter med hjälp av specialister från Sahlgrenska sjukhuset[10], och på Södra Älvsborgs sjukhus drabbades, som tidigare nämnts, de läkemedelsautomater där man hämtar ut mediciner till patienterna.

Övriga drabbade aktörer

Vidare bedöms en monitor för vädertjänst på Säve flygplats ha infekterats, vilket gör att förmågan för Säve ambulanshelikopter att avläsa väder påverkas. Ett digitalt styrsystem vid sjukvårdens tvätteri måste också tas ur drift vilket kunde ha påverkat verksamheten genom att orsaka brist på rena kläder till sjukvården (så skedde dock inte). Även vissa inpasseringssystem påverkas, bl.a. vid Göteborgsoperan och i Västfastigheter.

Fyra dagar efter den inledande incidenten upptäcks fler infekterade datorer. Passagesystem för en datahall och ytterligare medicinteknik upplever störningar. VGR får nu information från en leverantör om att deras nätverk kan nås i stort sett direkt från internet[11]. Detta visar sig ha möjliggjorts genom en förändring som utfördes av den egna it-personalen i inledningen av incidenten och korrigeras snabbt. När läkemedelsautomaterna som fått tas ur drift[12] ska återinstalleras stöter man på problem och oron är stor att problemet inte ska vara åtgärdat innan julledigheterna.

10. Avser ett system där operationer kan övervakas i realtid på distans (ger t.ex. en specialist på annan ort möjlighet att delta med råd). Här var det framför allt tidskoordinationen som påverkades.
11. I detta fall via Remote Desktop Protocol, en fjärrskrivbordsapplikation som kan ansluta sig via internet till en dator om en bestämd TCP-port har lämnats öppen.
12. Automaterna var inte virusangripna men beslut togs ändå att ta dem ur drift, eftersom skadlig kod tagit sig in. Malwaren hade dock inte lyckats installera någon illasinnad kod.

Även en infekterad dator (server) som hanterar larm från hissar, gas, VVS, fläktsystem m.m. måste tas ur drift, vilket gör att personal under tio dagar måste kallas in för att manuellt rondera på Uddevalla sjukhus.

Sammantaget var en del system (tjänster) inte åtkomliga under två veckor och andra tjänster upplevde stora störningar. Eftersom systematisk loggning inte förekom fanns det ingen möjlighet att klarlägga om konfidentiella uppgifter röjts, förändrats eller lyfts ur systemet.

1.3.1 Åtgärder och erfarenheter

VGR uppger att de efter händelsen arbetat intensivt med att förbättra både den systematiska informationssäkerheten och den tekniska säkerheten. VGR: s datanät var vid tidpunkten för incidenten inte segmenterat. Det fanns flera hundra accesspunkter in i nätverket och nätverkskontakt mellan dessa. Idag låser VGR sitt nätverk mycket hårdare. Kombinationen av brist på segmentering, kontroll av uppkopplade datorer samt svaga lösenord gjorde it-systemen mycket känsliga för ett virusangrepp. Bristen på loggningsförfaranden gjorde det också svårt att utreda vad som hade hänt.

Vid tillfället för incidenten fanns rutiner och planer för krishantering utifrån en it-relaterad incident. Det fanns en it-incidentplan och en utsedd it-incidentchef med dygnet runt jour. Det fanns även en krishanteringsplan för hela VGR. Vad som dock inte fanns var verktyg samt en central punkt där it-systemen kunde övervakas i syfte att effektivt kunna bedöma och tidigt kunna motverka incidenter. Vidare fanns inga definierade SLA:er[13] med externa leverantörer, som kunde appliceras på incidenten. Det saknades dessutom lokalt intrångs- och detekteringsskydd på de infekterade datorerna i nätverket, vilka inte heller var uppdaterade för tredjepartsprogram.

I samband med att VGR drabbades av skadlig kod i december 2012 så gjorde regionen en mångfald erfarenheter. Några av dem återges i korthet i bilaga 2. VGR: s erfarenheter av datavirusattacken 2012 samt ett antal andra it-incidenter har gjort att regionen nu kraftsamlar kring informationssäkerhetsarbetet.

13. För terminologi se bilaga 3.

1.4 Följdeffekterna av telestörning hos TDC i april 2013

Den 3 april 2013 kl. 13:15 inträffade en telestörning i teleoperatören TDC:s stamnät i Sverige. TDC är en nordisk teleoperatör som enbart riktar sig mot företagskunder och agerar på den nordiska marknaden. Störningen drabbade stora delar av företagets nordiska nät. Till de som drabbades hörde Skatteverket, som tappade sin kommunikation med lokalkontor i hela landet. Telestörningar uppträdde hos alla TDC:s kunder, såsom taxibolag, kommuner, vårdcentraler och landsting. Nätstörningen påverkade också flera mediekoncerner och orsakade problem i produktionssystemen för bl.a. Göteborgs-Posten.

Den ursprungliga felorsaken, ett routingproblem i nätverket, kunde åtgärdas redan efter en kort stund genom en återrullning av system till tidigare stabilt drifttillstånd. I samband med detta fick ett stort antal utrustningar startas om. Efter några timmar kunde större delen av nätet återställas. Vissa geografiskt spridda utrustningar i nätet tog dock ytterligare tid i anspråk. Runt kl. 18.00 återgick TDC till normal driftsituation.

Följdeffekterna bland några av operatörens kunder visade sig vara relativt omfattande. Till de drabbade hörde företaget Inera, som driver en rad sjukvårdsgemensamma tjänster, samt kommunikationsnätet Sjunet, som byggts med hjälp av länkförbindelser hos TDC. Vid telestörningen hos TDC slutade kommunikationen i Sjunet till stora delar att fungera, vilket ledde till att sjukhus och vårdinrättningar inte längre kunde komma åt tjänster som central kontroll av inloggningsbehörigheter och ordination av läkemedel. Hade störningen kvarstått till påföljande dag hade den kunnat orsaka stora konsekvenser inom hela vård- och omsorgssektorn i Sverige.

Hos företaget Inera etablerades redan inom någon timme en krisorganisation som fick arbeta under eftermiddagen och kvällen med att återställa de driftstörningar som teleavbrottet förorsakat. Sjunet var åter igång kl. 17.00 samma dag och systemdriften i övriga berörda system var återställd strax före kl. 23.00 samma kväll. Det tillstötte emellertid komplikationer i olika system till följd av systemberoenden. Detta förorsakade problem som varade under flera dygn.

1.4.1 Åtgärder och erfarenheter

De lärdomar Inera gjorde var bland annat att diversitet och redundans, dvs att dela upp hårdvara och satsa på extra förbindelser, inte fungerade i det här fallet eftersom det fanns en punkt där förbindelserna gick samman (s.k. single point of failure). Det var också svårt att följa upp SLA med leverantören och även om Sjunet hade viteskrav med i sina avtal gick det inte att gå vidare på den vägen eftersom loggarna var bristfälliga. Detta är dock viktig kunskap inför förhandlingar vid förnyade upphandlingar.

När det gäller Ineras interna rutiner var en åtgärd som vidtogs att uppdatera återstartsrutinerna, t.ex. prioriteringar för att kunna starta om i rätt ordning – med hänsyn till beroendena mellan systemen. Inera uppges även ha tagit nya designbeslut för att öka nätets robusthet.

1.5 Nätverksbortfall och avbrotten i TakeCare i juni 2013

Under juni 2013 inträffade ett antal it-incidenter vid Stockholms läns landsting, där flera vårdgivares verksamheter påverkades negativt.

Först ut var ett större nätverksbortfall vid Karolinska universitetssjukhuset, som är ett av Europas största sjukhus med över 15 000 anställda. Måndagen 3 juni var nätverket vid Karolinska universitetssjukhuset i Solna utslaget i några timmar då en lokal brandvägg slutade fungera efter ändringar i konfigurationen. Situationen vid sjukhuset bedömdes så allvarlig för verksamheten att de beslutade att gå över i stabsläge vilket bl.a. innebär utökad bemanning.

Journalsystemet TakeCares driftstopp

Sedan drabbades journalsystemet TakeCare av två driftstopp under den aktuella tiden, 11 respektive 18 juni 2013. Systemet är ett av de centrala systemen i vården. De båda stoppen var identiska och hade med största sannolikhet samma ursprung. De uppträdde utan förvarning och innebar att systemet blev onåbart för användarna[14]. Återställningsarbetet, dvs. tiden innan systemen var i full funktion igen, tog sex respektive fem timmar vid stoppen.

TakeCare har sedan det infördes vid KS år 2004 drabbats av flera stora driftavbrott och även varit föremål för flera utredningar.

14. Den bakomliggande orsaken, ett fel (en bugg) i det underliggande operativsystemet AIX, åtgärdades efter det andra driftstoppet genom en rättning i den nya versionen från leverantören.

Idag använder cirka 125 vårdgivare med sammanlagt runt 40 000 anställda inom Stockholms läns landsting (SLL) TakeCare som huvudsakligt journalsystem och informationsstöd för sina vårdprocesser.[15]

Konsekvenser av driftproblemen

Konsekvenserna vid driftproblemen 3 juni blev bl.a. längre väntetider för patienter, att akutpatienter uppmanades att söka andra sjukhus, att manuella rutiner i form av papper och penna fick tas till samt att det inte var möjligt att ringa via telefonist utan bara med direktnummer. En del öppenvårdsbesök ställdes in och ett mindre antal selektiva operationer fick skjutas upp. Enligt den Lex Maria-anmälan som sjukhuset gjorde efter incidenten, låg hela nätet vid Karolinska universitetssjukhuset nere under 3,5 timmar och ambulanser med prio 2- och prio 3-patienter fick under en dryg timme styras bort från KS.

Vid ett driftstopp 11 juni förlorades data som skrivits in i journaler och uppgifterna fick skrivas in igen manuellt. Enligt SLL IT kunde alla komma åt läskopian[16], men kunde inte lägga in ny information under driftstoppet. Detta var dock en uppfattning som inte delades av alla p.g.a. de långa svarstiderna. Tjänsterna e-recept och digital tidsbokning låg nere. Efter stoppet gick det åt mycket arbete för att manuellt återinföra labbsvar och journalanteckningar i systemet.

Även vid driftstoppet 18 juni förlorades data som skrivits in i journaler. Läskopian fungerade bättre under detta stopp, men störningen varade under större delen av en arbetsdag och orsakade olägenheter och långa väntetider i en stor del av landstinget.

Vid intervju med en vårdgivare framkom konkreta konsekvenser av it-incidenterna. Ett exempel är att operationer fick genomföras utan tillgång till journalerna. Vital information om patienter saknades och det medförde att till exempel operationer och provtagning blev kraftigt försenade. Felmedicinering skulle kunnat ske eftersom läskopian inte var synkroniserad med originalet. Patientkontakt via telefon fungerade inte. Sammantaget var incidentens inverkan på sjukvårdens förmåga mycket stor och betydande negativa konsekvenser kunde ha inträffat.

15. De största vårdgivarna inom SLL är Karolinska Universitetssjukhuset (Solna och Huddinge), Stockholms läns sjukvårdsområde (SLSO), Södersjukhuset, Danderyds sjukhus, Södertälje sjukhus och S:t Eriks ögonsjukhus. Systemet används även av privata vårdgivare och sjukvården i Gotlands län.
16. En läskopia är en kopia av (produktions)servern som kan användas vid ett eventuellt driftstopp.

1.5.1 Åtgärder och erfarenheter

Åtgärder på kort sikt

Verksamheten (vårdgivarna) initierade arbete med läskopian (en statisk kopia av journalerna i TakeCare), men det finns olika uppgifter om hur nåbar den var. Väntetider på uppemot 20 minuter för att komma åt en journal rapporterades. Under det första stoppet 11 juni saknades kapacitet för att hantera de många anrop som gjordes. På flera platser saknades även de uppdateringar som krävdes för att få de nyare versionerna av läskopian att fungera. Dessa problem var betydligt mindre under det andra stoppet en vecka senare, då den tekniska kapaciteten för läskopian hade utökats.

All dokumentation fick göras med hjälp av manuella rutiner och med analoga hjälpmedel. Det blev ett merarbete att sedan överföra den analoga dokumentationen till det digitala systemet, vilket förorsakade övertidsbeläggning under de närmast följande dagarna.

Driftleverantören startade sedvanligt incidenthanteringsarbete med operativ felsökning och stabsarbete samt kontaktade leverantörer av it-miljön för stöd. SLL hanterade även mediekontakter och informationsspridning externt under de initiala delarna av avbrotten.

Efter händelserna gjordes flera Lex Maria-anmälningar, dels en gemensam från chefläkarna på de tre stora sjukhusen, dels en mer detaljerad om en pågående operation som drabbades av incidenten.

Åtgärder på lång sikt – vårdgivare

Efter händelserna har vårdgivarna arbetat aktivt för att ta tillvara på erfarenheter från händelserna och omsätta dem i handlingsplaner. Ett exempel är att ett större sjukhus bl.a. har gjort ett tillägg till sin katastrofplan och skapat en egen bilaga som redogör för hur en it-incident ska hanteras organisatoriskt och flödesmässigt. En viktig kontaktpunkt är TakeCare-förvaltningen. Vårdgivaren har planerade övningar och ska ha en regional alternativt lokal övning med TakeCare och Stockholms läns landstings IT (SLL IT).

Under det stora stoppet fungerande inga vanliga kontaktvägar eftersom intranät och till viss del även telefonväxeln var utslagen. Som reservrutin har nu chefläkarna möjlighet att skicka ut massmeddelanden till personal runt om i organisationen. De har även en särskild sida på intranätet där manuella rutiner och dito underlag (t.ex. journalmallar) finns samlade. Det ska också finnas förberedda pärmar med utskrivet material på strategiska ställen. På några

avdelningar har även intervallen mellan uppdateringar av läskopian förtätats mellan olika instanser.

Åtgärder – förvaltning
Förvaltningen för TakeCare har ansvaret för kontinuitetsplaneringen och för de övningar av denna som genomförs. Det identifierade potentiella problemet kring oklarhet vad gäller arbetsuppgifter, ansvar och roller är också en fråga som hanteras av förvaltningen. Andra viktiga frågor man utrett vidare är avtal med leverantörer.

Åtgärder på lång sikt – driftleverantör
SLL initierade flera utredningar kring händelserna och genomförde flera konsultgenomlysningar av informationssäkerhet inom SLL samt tillsatte en specifik analyskommission som leddes av chefen för SLL IT.

En av de mest centrala åtgärder som beslutats är att skapa en testmiljö för TakeCare i egen (landstingets) regi för att inte längre behöva förlita sig på leverantören. Integrationstester och versionstester kommer då underlättas. I dagsläget har mycket underhållsarbete genomförts i produktionssystem under pågående drift.

Återstartstider var även det ett återkommande tema tillsammans med rutiner för hur dessa skulle gå till. Även om leverantören vidtagit en hel del förbättringar här är landstinget inte fullt ut nöjda med systemet ur denna aspekt. För närvarande utreder SLL förutsättningar och möjligheter vad gäller framtidens vårdinformationssystem tillsammans med två landsting. Innan leverantören genomförde förbättringar tog en återstart över ett dygn. Efter att ”warm spare”[17] införts har svarstiderna kortats betydligt, men det finns fortsatt små möjligheter att med nuvarande tekniska lösning nå de två timmar som verksamheten önskar.

Efter olika utredningar beslutades bland annat att inrätta en övergripande funktion med uppgift att stödja landstingets verksamheter med att upptäcka och hantera it-säkerhetsrelaterade hot och incidenter. SLL ska också ställa mer precisa it-säkerhetskrav i beställningar på tekniska plattformar. SLL ska dessutom utreda om en central teknisk lösning ska införas för att upptäcka avvikelser och potentiella hot i landstingets nätverk.

17. ”Warm spare” är en backupmetod där data från huvudsystemet speglas till reservsystemet i intervaller. Detta innebär att huvudsystemet och backupsystemet vid jämna mellanrum inte innehåller exakt samma data.

Övriga erfarenheter

Något som noterades var att det var mycket varierande kvalitet på manuella rutiner och på hur arbetet och verksamheten kunde fortsätta under störningarna. Detta var i huvudsak personberoende, dvs. de som var vana vid en manuell hantering (dvs. hade arbetat innan digitaliseringen) kunde hantera situationen bättre. Förmågan påverkades också av huruvida det fanns nyckelpersoner i tjänst som gjorde att arbetet flöt lättare. Var dessa inte i tjänst blev det mer utmanande att hantera verksamheten.

Vikten av kommunikation, både intern och extern, var också uppe till diskussion. Hur får man rätt information anpassad till alla målgrupper vid en it-incident? Det är många som vill ha och behöver information vid en it-händelse, och de som vet mest är ofta hårt uppknutna i det operativa hanterandet av själva händelsen. Här bör avlastning vara planerad.

Att hantera bilden av krisen istället för själva incidenten kan bli resurskrävande. En önskan från arbetsgivaren var att enbart ett fåtal personer skulle uttala sig i medierna, så att det av misstag inte gavs en alltför splittrad bild av incidenten, vilket i förlängningen skulle kunna leda till förtroendeproblem. En erfarenhet var att det finns behov av information/utbildning om kriskommunikation till alla anställda som kan bli föremål för intresse från medier.

En annan erfarenhet var att när personal som inte har övat på oförutsedda driftstopp plötsligt ska dokumentera och kommunicera vårdprocesser genom att improvisera blir informationsöverföringar och ansvarsfördelningar oklara och riskabla. Vikten av övning och att ha en krisplan som är ordentligt testad kom upp, inte minst för att minska ledtider – vem ska kontakta vem och i vilken ordning?

Inom en sektor som sjukvården med dess stora behov av information uppstår även problem med att se till att all patientinformation blir korrekt, trots att personalen inte har tillgång till it-systemen. Det fanns behov av att kunna hantera skyddsvärd information och sekretess säkert, vilka måste tillgodoses även vid ett it-avbrott.

Tidpunkten på dagen kan också ha betydelse för i vilken omfattning en incident får genomslag. Vid den första störningen, när hela nätverket på KS slogs ut, var det eftermiddag, vilket störde verksamheten mindre än TakeCare-stoppen som inträffade på morgon och förmiddag.

1.6 Brand hos it-leverantören EVRY nyår 2013–2014

Den 30 december 2013 inträffar en brand i anslutning till en datahall hos it-driftleverantören EVRY. I datahallen finns produktionssystem för och data från ett flertal kunder, bl.a. en av Sveriges största arbetsgivare. Branden kunde dock släckas utan produktionspåverkan.

Natten därpå, nyårsnatten, inträffar en ny brand i samband med att en kondensator i en UPS[18] i datahallen exploderar. Denna gång försvåras släckningsarbetet av att aggregaten med inergen tömts kvällen innan men inte hunnit bli påfyllda igen[19].

Branden orsakar en kraftig ljusbåge som skadar flera komponenter i närheten. Som konsekvens av detta påverkas strömtillförseln till servrarna. De strömspikar som blir resultatet av ljusbågen skapar ett avbrott i elförsörjningen, vilket gör att flera system stängs ner automatiskt och två SAN (datalager) låser sig varav det ena inte direkt går att starta upp igen, enligt uppgift p.g.a. felaktighet i samband med programvara[20 21].

Värst drabbade blir de kunder som fanns på det låsta SAN:et, som inte gick att starta upp igen. Sammanlagt drabbas 19 kunder. Cirka 900 system behövde genomgå revision för att verifieras så att de inte hade några okända beroenden, och över 700 system drabbades i olika grader av tillgänglighetsproblem.

I fallet med branden hos EVRY var ett stort antal aktörer från olika sektorer drabbade. Till de värst drabbade kunderna hörde, enligt media SJ, SL, CSN och PostNord. Även Systembolaget, Green Cargo, Skatteverket, Forex, fackförbundet Kommunal (hemsida och a-kassetjänst), fackförbundet Unionen, e-tjänsten ListOn (kundloggning för vårdsektorn) och en tidningstjänst drabbades[22]. Nedan beskrivs kort en del av de effekter som blev konsekvensen av branden.

18. Uninterruptible power supply, UPS, är en elektrisk apparat som tillhandahåller ström om strömavbrott eller annan störning inträffar. Används för att stabilisera strömtillförsel oberoende av strömkälla.
19. Insatsrapport Storstockholms brandförsvar, nr 2014166161, 2014-01-01. Inga funktionsbrister avseende släckutrustningen i datahallen kunde påvisas. EVRY uppger att händelsen inte hade någon påverkan på händelseförloppet samt att det enbart innebar en marginell tidsförskjutning att släcksystemet var tomt.
20. EVRY lyckas efter 18 timmar få upp det mindre av de två SAN-lagren, men en säkerhetsfunktion som låst/skadat en indexeringstabell gjorde att informationen lagrad på den andra SAN-disken förblir oåtkomlig.
21. För den som vill veta mer om hur man fysiskt kan skydda (sin information i) datahallar rekommenderas Vägledning för fysisk informationssäkerhet i it-utrymmen, MSB 2014.
22. Media uppger även felaktigt att Apoteket drabbats.

Transportsektorn

SL-trafiken fortsatte att rulla eftersom trafikstyrningssystemen driftas av en annan leverantör, men trafikinformationssystem och betalsystem fungerade otillfredsställande i två dygn. Mest kritiskt för SL var dock att ekonomisystemen låg nere när arbetet med årsredovisningen skulle inledas.

Även ett annat bolag med koppling till transporter påverkades i hög grad av EVRY-incidenten i januari 2014. Bolaget hade huvuddelen av sin drift hos EVRY. Vid incidenten påverkades nära 200 av bolagets system, bl.a. flera produktionssystem och hela bolagets försäljningssystem. Deras hemsida gick ner och därmed försvann biljettbokningen på nätet under nära två dygn[23]. Vidare påverkades även biljettautomater och utskick av sms-biljetter under ett dygn.

Bolaget såg konsekvenser av EVRY-incidenten upp till en månad efter händelsen. Flera stödjande system fungerade otillfredsställande tre–fyra dygn efter incidenten. Mest långvariga var störningarna för bolagets test- och utvecklingsmiljöer, vilket resulterade i försenade releaser och extra kostnader.

Vid incidenten förlorade företaget även vissa data ur försäljningssystem. Vid dialogen med EVRY framkom att det internt hos aktören fanns osäkerhet kring vad som beställts avseende backup. Det saknades underliggande dokument hur resonemanget gått i samband med att kontraktet skrevs några år tidigare, vilket försvårade tolkningen av avtalets innehåll vid en dialog med leverantören[24].

Distribution av post

PostNord blev tidigt uppmärksammade på att något inte stod rätt till med deras it-system genom att en kund inte kom åt sina system. EVRY är den enskilt största leverantören till logistikföretaget, där de främst har produktionssystem för brev och paket.

PostNord upplevde effekter av incidenten upp till cirka 12–14 dagar efter händelsen. Den långa återhämtningstiden berodde enligt företagets bedömning på en kombination av leverantörens agerande, att systemtester tog tid och att stora mängder data tog tid att återläsa (48 timmar). Till detta kom att misstag gjordes där fel data lästes in vid ett tillfälle. PostNord uppger dock att de inte förlorat några data.

23. Bolaget har nära sex miljoner besök på sina digitala kanaler under december månad, varav drygt 4 miljoner via sin hemsida.
24. Bolaget har idag en modell med backuper på olika platser (redundans i form av alternativa system och kontinuitetsplaner). De har dock börjat fundera kring ny modell för redundans. Den tolkning som företaget gör idag är att det tidigare tagits ett medvetet beslut om att inte kravställa för hårt kring backup och sedan ta det ekonomiskt mest fördelaktiga budet.

I korthet drabbades PostNords verksamhet på ett flertal sätt. Deras hemsida gick ner, vilket bl.a. gjorde att vissa beställningstjänster inte gick att nå. Vissa produkter gick inte att producera maskinellt utan fick produceras manuellt, vilket skapade förseningar[25]. Postavier gick inte ut under några dagar, vilket gjorde att det inte gick att hämta ut levererade brev. Varubrev försenades med upp till tre dagar och även postförskott drabbades av vissa förseningar. Förseningarna skapade även kostnader genom att extra transporter fick hyras in för att klara leveranser (hyra in flyg, sätta in extra tåg, bilar etc.). Hanteringen blev dessutom mycket resurskrävande.

Vidare kunde inte rekommenderade brev, som kräver fullmakt eller behörighetshandling, lämnas ut eftersom it-incidenten omöjliggjorde kontroll[26]. Företagets bemanningsverktyg slogs ut (planeringsverktyg), vilket skapade problem för personalplaneringen. Vidare fungerade inte tjänsten med spårning av brev och paket, vilket gjorde att produkter inte gick att spåra. Manuell hantering fick sättas in, vilket var mycket kostnadskrävande.

PostNord bedömer att incidenten inte påverkade någon samhällsviktig funktion som t.ex. större medicinleveranser. När det gäller större försändelser så finns det möjlighet att hantera detta manuellt. Varje kundansvarig säljare vet vilka de större kunderna är och vilka deras viktiga försändelser är.

Medierna rapporterade mycket få fall där aktörer påverkades negativt av förseningarna i postleveranser och inget av de rapporterade fallen kan bedömas som samhällskritiskt. Ett konkret exempel på de praktiska problem som uppstod av incidenten var att företaget Samres, som har hand om upphandlingen av färdtjänst och sjukresor på Gotland, tvingades förlänga anbudstiden inför en ny avtalsperiod eftersom flera anbudsgivares rekommenderade brev inte kunnat hämtas ut i tid.

Posthantering är en viktig service i samhället som många aktörer är beroende av. Störningar i verksamheten och dess påverkan på samhällsviktig verksamhet är dock fortfarande inte genomlyst. Post- och telestyrelsen skriver 2013 i en rapport om risker och sårbarheter i postsektorn att de har för avsikt att genomföra ett projekt där samhällsviktiga verksamheters beroenden av förmedling av postförsändelser kartläggs[27].

25. Förseningarna skapade vidare merproblem genom att extra transporter fick hyras in för att klara leveranser.
26. REK till privat mottagare kunde dock lämnas ut mot legitimering.
27. PTS rapport Risk- och sårbarhetsanalys postsektorn 2013, dnr 12-10536-14, s. 11.

Andra samhällsfunktioner

Även myndigheter drabbades och därmed också enskilda personer. En myndighet som påverkades av it-avbrottet fick i stort sett hela sin verksamhet utslagen, vilket kraftigt kunde ha påverkat utbetalningar till de privatpersoner, som är beroende av myndigheten för sin försörjning[28].

På grund av kundkrav så är nära nog all hantering vid denna myndighet idag automatiserad och verksamheten är idag i stort sett helt förlagd till den virtuella världen. Till detta kommer att myndigheten inte äger någon infrastruktur själv utan leasar all digital utrustning. Branden hos EVRY slog ut myndighetens e-tjänster, som Mina sidor och Mina tjänster, men även myndighetens e-posttrafik samt intranät. En konsekvens av incidenten var vidare att handläggningen av nya ärenden inte kunde påbörjas. Myndighetens möjligheter att göra behörighetskontroller upphörde eftersom uppkopplingen mot andra leverantörer även påverkades. Sammantaget var hela verksamheten otillgänglig i två dygn och delar av verksamheten i fyra dygn. Under denna period kunde inga utbetalningar ske.

Även mediesektorn drabbades. Distributionen av dagstidningar i Hälsingland påverkades eftersom Tidningstjänst, som distribuerar tidningar inom Mitt-Media, drabbades. Företaget fick stora förseningar eftersom de var tvungna att arbeta manuellt med sådant som vanligtvis sköts per automatik.

Fackförbundet Kommunals hemsida kommunal.se var okontaktbar under en vecka, men Kommunal menar att det största problemet var att data har förlorats och ”inte tycks kunna återskapas”. Förutom den externa hemsidan drabbades även intranätet Komin, förbundets ekonomisystem och medarbetarnas filkataloger.

1.6.1 Åtgärder och erfarenheter

Leverantörens åtgärder

EVRY aktiverade sin interna organisation för it-incidenthantering så fort händelsen inträffat. De arbetade under flera dygn för att försöka åtgärda det SAN[29] som krånglade, men började redan efter några timmar parallellt att agera utifrån sin alternativplan, en full återläsning av data för samtliga kunder.

28. Detta kunde undvikas då incidenten inte inträffade vid ett transfereringstillfälle.
29. Storage Area Network (SAN) är nätverk vars enda uppgift är att distribuera och lagra data.

För att få tillgång till datalagringsytan igen var EVRY beroende av leverantören till lagringsskåpet, vilket ytterligare fördröjde en lösning. EVRY uppger att de hade sammanlagt runt 150 personer som arbetade långa arbetspass och treskift för att återställa tillgång på data[30]. Specialister flögs också in från utlandet för att skynda på arbetet. Leverantören prognostiserade att driftstörningarna skulle vara borta till sista januari, men samtliga system och tjänster var, enligt uppgift, i full funktion 20 januari.

EVRY skapade s.k. kundteam med olika kompetenser runt varje kund. En dialog kunde därmed inledas omgående med varje kund avseende vilka system som kunden ville prioritera uppstart på samt att åtgärderna kunde skräddarsys för kundens behov. EVRY uppger att de hade en god lägesbild relativt omgående, bl.a. kunde incidentledningen i realtid följa hur många system som låg nere.

På fråga uppger EVRY att de prioriterade återställning av de system/applikationer som hade någon form av ”samhällsviktig funktion”. På frågan hur de definierar samhällsviktig uppger EVRY att detta skedde i dialog med kunderna och med hänsyn till samhällseffekterna. EVRY ansåg att det var enkelt att identifiera de system och aktörer som skulle prioriteras, men går inte vidare och förklarar hur de gick till väga. I en artikel uppges EVRY ha sagt att *”Det är en stor gråskala för vad som är samhällskritiskt”*[31]. EVRY förtydligar uttalandet via e-post: *”Gråskalan om vad som är samhällskritiskt är att det inte finns en definition att luta sig mot utan en tolkning i många fall av de system som idag inte är definierade som samhällskritiska men som har påverkan på samhället.”* I rapporten Handlingsplan för skydd av samhällsviktig verksamhet går MSB igenom och förklarar ett antal termer med koppling till samhällsviktig verksamhet. I Vägledning för samhällsviktig verksamhet[32] förklaras vilka verksamheter som är att betecknas som samhällsviktiga. Syftet med vägledningen är att underlätta identifiering av samhällsviktig verksamhet.

Vidare anser EVRY att det har betydelse för återställningstakten hur aktiv kunden är: *”En del kunder är mer på och för andra kunder har vi gemensamt lagt det åt sidan för att prioritera annat arbete och inte hållit listorna och prioriteringen på rätt nivå.”*[33]

30. EVRY uppger vid ett möte att insatsen uppgick till 300–400 personer sammanlagt.
31. Computer Sweden, Låst skåp blev EVRYs fall, 140131, http://computersweden.idg.se/2.2683/1.544785/last-skap-blev-EVRYs-fall/sida/2/nu-kommer-den-praktiska-processen.
32. https://www.msb.se/sv/Om-MSB/Nyheter-och-press/Nyheter/Nyheter-fran-MSB/Vagledning-for-samhallsviktig-verksamhet/ Se även Ett fungerande samhälle i en föränderlig värld (Nationell strategi för skydd av samhällsviktig verksamhet), MSB 2011.
33. Artikel Computer Sweden: Låst skåp blev EVRYs fall. Publicerad 2014-01-31 http://computersweden.idg.se/2.2683/1.544785/last-skap-blev-EVRYs-fall.

EVRY har uppgett att de vidtog ett antal åtgärder efter incidenten. Bl.a. förändringar i infrastrukturen (kapacitetsökningar i backupcentralen och i backbonenätet) och nya serverplattformar för virtualisering för att ersätta de som havererat.

Leverantörens erfarenheter

EVRY:s erfarenhet är att hur kunderna formulerat sina krav och på vilken nivå de prioriterat vissa system varierade och att bra förarbete hade sparat tid.

Vidare anser EVRY att det har betydelse hur kundernas it-system ser ut; de anser att det är en fördel om de har god kunskap om systemen, om de är rätt konfigurerade och om systemen är nya. Flera av installationerna krävde manuell hantering eftersom kundernas system var gamla, vilket var mycket resurskrävande.

Intressant nog så uppger EVRY att en del av deras kunder inte drabbades alls av incidenten eftersom de hade en annan typ av kravställning med högre redundans. Här gör EVRY bedömningen att dessa kunder dessutom ofta har en högre beredskap för it-incidenter och är mer övade.

EVRY uppger att de vidtagit ett flertal tekniska förbättringsåtgärder sedan incidenten, men går inte in i detalj på vilka åtgärder som avses. De uppger även att de kommer öva mer. Antalet övningar ökas från en om året till två, och omfattningen av själva övningarna ska öka. EVRY planerar dessutom att vidta flera andra åtgärder efter incidenten, bland annat får en person ansvar för att på halvtid specifikt arbeta med planer för att motverka incidenter, ett konkret uppdrag för att lyfta frågan om kontinuitetsplanering.

EVRY:s erfarenhet var att kunderna hade mycket olika standard på sin utrustning samt varierande grad av kunskap om sina system, vilket försvårade arbetet. Vidare var det enbart ett fåtal kunder som hade prioriterat vilka system de ansåg verksamhetskritiska och därmed var prioriterade för uppstart.

EVRY uppfattade även att kunskapen hos kunderna var låg om det man avtalat om och att det fanns en övertro på vad avtalen innehöll. EVRY anser att avtalen många gånger enbart styrts av ekonomiska principer (lägst bud), vilket gjorde att en del kunder blev överraskade över att de inte omfattade mer.

EVRY uppger att de drog ett antal tekniska lärdomar av incidenten, bl.a.:

- att de satsat på bättre separation på tjänstenivå, då det minskar konsekvenserna av om det inträffar ett problem
- information lagrad på gamla servrar var mer problematisk att återställa (mycket tidskrävande)
- att generatorerna inte var gjorda för att gå så länge som de gick.

Kundernas åtgärder

För att hantera händelsen aktiverade det tidigare nämnda större transportföretaget sin kontinuitetsplan för it. Sedan tidigare hade bolaget prioriterat vilka system som var mest kritiska för verksamheten (prioriterade system), vilket underlättade i dialogen med leverantören vid incidenten. Övrig verksamhet vid bolaget fick gå över till manuella rutiner.

Efter att den akuta händelsen var hanterad och verksamheten var uppe i normal drift igen, rapporterade bolaget omedelbart händelsen till bolagets riskstyrgrupp som en risk att hantera. Gruppen ansvarar för bolagets riskhanteringsprocess. I denna process, där riskstyrgruppen inventerar och följer upp risker i organisationen, finns även en revisionsgrupp som kan ta upp ämnen med bolagets styrelse[34].

PostNord valde att starta upp sin krisledningsorganisation omedelbart eftersom incidenten bedömdes som omfattande. Fördelarna med att arbeta med en särskild organisation var enligt företaget främst de kortare beslutsvägarna samt enklare resurstillsättning, men även att särskilda kommunikationsinsatser gjordes både på affärsområdesnivå och på koncernnivå samt att personalen fick enklare att fokusera/prioritera.

PostNord upplevde att det var svårt att få tydliga och korrekta uppgifter om omfattningen av incidenten och på grund av detta var det svårt att bedöma vilka konsekvenser den skulle få i ett tidigt skede. Omfattningen av konsekvenserna ökade dessutom snabbt efter hand och detta i kombination med oprecisa besked från leverantören gjorde det svårt att planera arbetsinsatsen.

34. Arbetet omfattar alla former av risker, från it-risker till att en nyckelperson slutar. Risker inventeras i bolaget bl.a. genom regelbundna enkäter till slumpvis utvalda medarbetare. Utöver detta genomför cheferna en gång per kvartal en inventering där de presenterar de risker de hittat i sin verksamhet. Riskstyrgruppen tar sedan upp, vid behov, riskerna med styrelsen och gör även uppföljning.

PostNord hade sedan tidigare prioriterat vilka system de behöver starta upp först och arbetade i nära relation med leverantören för att få upp dessa system. Identifiering av kritiska leveranser har varit det främsta kriteriet för att kunna göra prioriteringar i produktionen. Vidare hade PostNord nyligen övat beredskap där man tagit höjd för den ökade produktionstakten vid jul och i samband med det även övat sin it-organisation.

När företagets hemsidor gick ner startades en tillfällig hemsida där information om incidenthanteringen löpande lades ut samt snabblänkar till de tjänster som fungerade.

Efter incidenten var hanterad har PostNord tagit fram en ”action list” med ett antal punkter som ska åtgärdas. Prioriterat är att skapa ökad förståelse och tydlighet mellan it och produktion. Företaget arbetar löpande med att identifiera vilka system som behöver vara igång för att en viss tjänst ska fungera och ser nu över sitt ramverk för kravställning avseende kontinuitet på leveranser internt. Här vill man säkerställa att produktionsverksamheten kommunicerar sina krav på leveranser till övriga delar av verksamheten. PostNord har även satsat på utbildning för att ytterligare tydliggöra alla de interna beroenden och samspel som måste fungera när en störning uppstår.

Kundernas erfarenheter

I EVRY-fallet var det mest ekonomiska konsekvenser för de drabbade. I många fall gick det dock att dämpa förlusterna, t.ex. genom manuell försäljning. Flera aktörer uppger dock att det var ”tur i oturen” att händelsen inträffade när den skedde och att inte andra funktioner drabbades. Flera aktörer hade för tillfället låg produktion p.g.a. röda dagar.

De fyra dagarna 7–10 januari när kunderna återigen började efterfråga tjänster i större omfattning, men flera av aktörerna inte ännu var riktigt uppe i produktion, var kritiska för flera av aktörerna. Men trots växande synpunkter på utebliven service, så upplevde de drabbade organisationerna att det fanns förståelse hos medborgarna att felet låg utanför aktörernas kontroll.

En annan kund angav att de inte hade ändrat inställning till utkontraktering, men att de nu satsade på att bli bättre kravställare. Detta innebär framför allt att ta ett mer aktivt ansvar med kontroll och uppföljning av leverantören och att se till att löpande säkra att det som avtalats även var det som levererades. Vidare fanns funderingar på att ställa krav på leverantören om en separerad datamiljö.

PostNord ansåg att de vann mycket på att ha en bra fungerande och övad krisledningsorganisation med en tydlig metodik att arbeta utifrån, där det fanns redan utsedda funktioner och tillgång till utrustad lokal. Krisledningsorganisationen hade sedan tidigare övat virusangrepp, vilket bidrog till att arbetet fungerade relativt effektivt. Intressant nog hade dock ingen av de tillfrågade aktörerna funderat över att öva tillsammans med leverantören.

Ett bolag uppger att konsekvenserna hade kunnat bli mycket större än de blev. Eftersom det var en period med låg produktion så hann företaget sätta in de manuella rutinerna till dagen efter, vilket hade varit omöjligt vid normal verksamhet. Bolaget har även reflekterat över att om den andra servern hos EVRY hade gått ner, så hade företaget förlorat kontakt med de system som krävs för att bedriva och planera sin kärnverksamhet. Konsekvensen av detta hade blivit att all verksamhet efter hand hade avstannat.

Kunskapsnivån hos leverantören ansåg en del intervjuade vara en viktig faktor för framtida val av leverantör, liksom om leverantören hade stor genomströmning av personal på kritiska tjänster. Som exempel nämndes problemet med att behålla it-specialister och inte ”tappa” dem till andra positioner i företaget, som t.ex. konsultrådgivning. I intervjuerna framkom vidare att flera kunder ställer sig kritiska till hur leverantören löst det tekniska upplägget och att leverantören valt att lägga flera för samhället viktiga tjänster tillsammans.

En intervjuad lyfte fram det faktum att leverantörerna agerar i en ekonomisk miljö med starka krav på att pressa ner kostnader, vilket kan bidra till ett riskfyllt beteende.

Erfarenheter från händelserna

2. Erfarenheter från händelserna

Samtliga aktörer som intervjuats för denna rapport arbetar idag på något sätt för att stärka sin informationssäkerhet. Förutsättningarna och insatserna varierar dock kraftigt mellan aktörerna oavsett om verksamheten är privat eller offentlig och oavsett storlek på verksamheten eller verksamhetens art. Vissa gemensamma erfarenheter kan dock dras, vilka redovisas nedan.

2.1 Överbelastningsattacker

Överbelastningsattacker blir tyvärr allt vanligare. Generellt sett har dessa attacker dock sällan några mer varaktiga effekter på verksamheten annat än temporära tillgänglighetsproblem. De kan däremot vara både kostsamma och kräva stora arbetsinsatser. Mycket av detta kan dock lindras genom bra förberedelser.

Initialt bör organisationen se över sitt skydd mot överbelastningsattacker. Detta sker enklast genom att inleda en dialog med organisationens leverantör. Flera intervjuade påpekar sedan vikten av att vara förberedd. En bra, väl inövad incidenthanteringsrutin underlättar, liksom en god kontakt med internetleverantören. Viktigt är också att sedan följa de beslutade hanteringsrutinerna även vid en säkerhetsincident som exempelvis vid en överbelastningsattack.

Likaså bör organisationen vara medveten om sina prioriteringar innan en incident och ha identifierat sina prioriterade verksamheter. Vidare bör alternativa kontaktvägar och kommunikationslösningar ses över eftersom en överbelastningsattack i de flesta fall leder till att exempelvis e-post, ip-telefoni och webbplatser inte fungerar.

Även om en aktör anser att risken för att bli utsatt för en överbelastningsattack är låg, så kan man bli påverkad ändå genom sitt beroende till leverantörer, dvs. att den leverantör man anlitar har andra kunder som blir utsatta för en attack. Detta kan leda till att leverantören för att hantera händelsen måste reglera flödet i sina system som helhet, vilket kan påverka även de kunder som inte är det primära målet för attacken.

Överbelastningsattacker faller under Brottsbalkens bestämmelser (4 kap 9c §) och MSB rekommenderar därför att alla som utsätts för en attack gör en polisanmälan. För att stödja i det utredande arbetet bör loggsystem ha installerats på de prioriterade systemen.

2.2 Skadlig kod

Skadlig kod är ett av de mer förrädiska problemen i it-världen, särskilt eftersom den kan göra stor skada utan att det syns på ytan. Som exemplet i denna rapport visar kan man dessutom råka illa ut även om man inte är det huvudsakligt mål för attacken.

Incidenter med skadlig kod visar ofta tydligt hur beroende av varandra it-system kan vara. Verksamheter med till synes helt olika funktioner kan genom sina it-system vara ihopkopplade. En svåröverskådlig arkitektur kan lätt uppstå när en aktör bygger upp sin it-verksamhet över tid. Allt fler funktioner kopplas in och till slut har ingen överblick. Tydlig förvaltning och systemägarskap blir här oerhört viktiga komponenter.

Med ett tekniskt väldefinierat nätverk, uppdaterade programvaror, loggning och tydliga regler som efterlevs kan dock riskerna med skadlig kod minska drastiskt. För fler tips kring hantering av skadlig kod, se bilaga 2.

2.3 Följdeffekter av telestörning

Problem i nätverk är svårt att skydda sig emot. Problemet är inte heller så lätt att komma till rätta med som tidigare eftersom ändutrustningen idag är mer intelligent i jämförelse med tidigare system. Ett kort stopp kan ta lång tid att återställa ifrån på grund av kaskadeffekter[35] i system.

Vikten av tydliga rutiner och att dessa är kända och övade var en annan lärdom som Inera gjorde av händelsen. Eskalering, dvs att skifta fokus vad gäller resursinsatser och hantering, från incident till kris visade sig inte vara lätt, även om goda leverantörskontakter underlättade situationen.

Krisledning och rutiner för det behöver finna sina former och etableras när situationen är i normaldrift och inte lösas under pågående incident/kris.

35. För definition se bilaga 3.

När det gäller extern kommunikation är det bra att ha förberedda underlag och genomtänkta mallar som snabbt kan användas. Man har inte tid att sitta och fundera fram bra formuleringar under tidspress. Se mer under avsnittet om Kommunikation.

2.4 Fel i operativsystem

Fel i operativsystem hittas med jämna mellanrum. Många gånger när felet skapar incidenter så har det skett för att applikationer och konfigurationer i operativsystemet inte provats fullt ut i en testmiljö först, utan belastning har provats först när systemet satts i drift. Resultatet av det kan som exemplet visar få långtgående och i värsta fall ödesdigra konsekvenser. Incidenterna i TakeCare i juni 2013 kunde ha blivit mycket allvarliga sett till patientsäkerheten.

I samband med incidenter av denna typ aktualiseras eventuella oklarheter vad gäller arbetsuppgifter, ansvar och roller vid it-drift och hantering av it-system. Här bör organisationer ha höga krav på tydlighet. Ett sätt att nå dit är att inleda ett genomgripande arbete med standardisering[36]. Vidare bör en genomgång ske av de så kallade Service level agreement, SLA:er som eventuellt finns.[37]

I samband med händelsen identifierades också svårigheter kring ansvarsfrågor och roller för it-drift/-förvaltning/-användning. Även beslutsvägar och frågan kring hur avtalet med leverantören såg ut (framför allt då serviceavtalet, det så kallade SLA:et) aktualiserades under händelserna. I en tidskritisk verksamhet uppstår snabbt stress vid denna typ av händelse. Det innebär även mycket övertidsarbete med att efterdokumentera som i sin tur ökar arbetsbördan.

2.5 Incident hos it-leverantör

Det hör inte till vanligheterna att incidenter i datahallar får de stora konsekvenserna som branden hos EVRY kring årskiftet 2012–2013 fick. Det är dock inte ovanligt att det inträffar olyckor i datahallar. Beställare, men även it-leverantörer måste därför idag arbeta utifrån premisserna att säkra sina kritiska processer mot denna typ av incident.

36. Se här särskilt SIS 27000-serien.
37. En metod för att ange vilken kvalitetsnivå en leverens ska hålla.

Att kravställa på tillräcklig nivå är svårt, särskilt när detta ställs mot det ekonomiskt fördelaktiga, men detta måste vara en prioriterad fråga för verksamhetens ledning. Utöver att kravställa på rätt nivå så behöver beställande aktör dessutom idag vara aktiv som kund och löpande följa upp avtal. Vidare behöver de ha kunskap om sina egna verksamhetsprocesser och noga kartlägga sina interna beroenden samt hur dessa beroende påverkas av it-leverantörens tjänst och rutiner, exempelvis it-incidentrutiner.

Ett hinder för en robust informationshantering kan vara de begränsade servicenivåer som erbjuds av leverantörerna vid utkontraktering. Dessa är ofta mycket svåra att ändra eftersom hela affärsidén ligger i att leverera en generisk tjänst till många. Att ställa krav utanför standardavtal blir därför inte sällan mycket kostsamt.

Det är mycket svårt att skapa fullständig redundans oavsett avtal eller tekniska lösningar. Därför måste aktörer idag fortsatt se till att de har manuella reservrutiner.

Förmågan att förebygga

3. Förmågan att förebygga

I detta avsnitt sammanfattas några generella förmågor som bör stärkas när det gäller att förebygga it-incidenter. Viljan att bära risker varierar med aktör och med verksamhet, och den kan också förändras över tid. Det är nära nog omöjligt att få 100-procentigt skydd mot it-incidenter. Men med ett strukturerat arbete kan många av riskerna hanteras.

3.1 Riskhantering och informationsklassning

För att kunna uppnå god informationssäkerhet och effektivt hantera risker är det centralt att verksamheten identifierar, analyserar och dokumenterar risker. I och med det stora beroendet till informationshanteringen är förmågan att kunna hantera information både i ett normalläge och i ett krisläge central. I den stora undersökningen av statliga myndigheters informationssäkerhet, *En bild av myndigheternas informationssäkerhetsarbete 2014*, framgår det att nära 80 % av myndigheterna har en metod för riskanalys.[38] Flertalet av de för denna rapport intervjuade aktörerna, arbetar också med någon form av riskidentifiering och riskhantering. Skillnaderna var dock stora avseende hur långt man implementerat arbetet i organisationen.

Få av de intervjuade organisationerna i denna rapport använde dock en modell för informationsklassning. I undersökningen av statliga myndigheters informationssäkerhet framgår det att endast två tredjedelar av myndigheterna har en informationsklassningsmodell. MSB:s arbete med andra sektorer pekar tyvärr på att det inte är bättre i dessa.

När det gäller arbete med informationens värde genom aspekterna konfidentialitet, riktighet, spårbarhet och tillgänglighet, så framkommer i intervjuerna att det ofta enbart är den förstnämnda respektive sistnämnda som anges och då med stor övervikt för tillgänglighetsaspekten.

38. Rapport MSB 740. Vidare uppger nära 60 % av myndigheterna att de inte slagit fast när en informationsklassning ska ske.

3.2 Övningens betydelse för hanteringen

En annan aspekt som återkommer är bristen på uthållighet när man kommer till att genomföra värdefulla förebyggande åtgärder. Tyvärr har flera av de tillfrågade aktörerna redovisat svårigheter med att ta till vara de erfarenheter som de erhållit vid en incident och överföra dessa till faktiska åtgärder. Det är många gånger svårt att behålla fokus på det långsiktiga arbetet i en föränderlig värld. Alla de saker som vid händelsen var självklara och prioriterade tenderar att när allt återgår till det normala alltför snart falla i glömska.

Att öva sina avbrotts- eller incidenthanteringsrutiner tillsammans med sin driftleverantör förbättrar beredskapen väsentligt. I en realistisk övning testas inte minst kontaktvägar, vilket är en förutsättning för en välfungerande hantering i ett skarpt läge. Ett logistikföretag uppger att det faktum att företaget övat på en it-incident bara några veckor innan EVRY-incidenten hade stor betydelse för deras möjligheter att hantera händelsen. Rutiner fanns färska i minnet och personalen var samspelad.

De manuella reservrutinerna är helt beroende av användarens vana och rutin. Som ett exempel i denna rapport visar klarade den personal som var van att arbeta utan datastöd ett systembortfall betydligt bättre än de som var ovana och aldrig hade upplevt analog hantering (papper och penna).

3.3 Relationen mellan kund och leverantör

Utkontraktering har många fördelar men kan också leda till svåra situationer, framför allt vid incidenter. Vems är ansvaret för t.ex. dataförlust om en it-incident inträffar när man har utkontrakterat hanteringen av sin information? Vilka problem kan uppstå i relationen mellan kund och leverantör? Och hur ser ansvarsfördelningen ut mellan kund och leverantör?[39]

En central grundförutsättning är att det är beställaren som är informationsägare och därigenom ansvarar för informationen. Rättsliga krav på att hantera information säkert finns i flera lagar och förordningar. När det gäller statliga myndigheter har detta bland annat tydliggjorts i krisberedskapsförordningen.[40]

39. För stöd i upphandling, se Vägledning – informationssäkerhet i upphandling, MSB555.
40. Se 30a§ förordning (2006:942) om krisberedskap och höjd beredskap och myndigheten för samhällsskydds- och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2009:10). Krav på säker informationshantering ställs exempelvis även i 31§ personuppgiftslagen (1998:204).

Det går att identifiera ett flertal beroenden mellan kund och leverantör, vilka kan påverka förutsättningarna för hur väl en it-incident kan hanteras. Utöver att ha en bra dialog med leverantören, så är man som kund beroende av att leverantören håller dig informerad och att informationen är korrekt i den mån det går. Som beställare bör man säkerställa detta genom avtal.

Utöver informationsproblemet så kan det vara svårt som kund att veta vem, och än mindre vilka, man hamnar tillsammans med på servern hos leverantören[41]. Även detta kan avtalas med leverantören. Vidare kan det vara svårt att se om de tekniska förutsättningarna och kraven i avtalet är uppfyllda hos leverantören och den egna kontrollen över den egna it-miljön riskerar därför att minska. Erfarenheten från incidenter visar att man måste vara aktiv som beställare och kund. Det går inte att frånskriva sig ansvaret som informationsägare.

Synpunkter från de intervjuade

Flera intervjuade lyfter också betydelsen av att göra sin egen hemläxa; man ska ha prioriterat vilka system som ska startas upp först vid en incident och kunskap måste finnas i den egna organisationen om hur de olika interna processerna påverkar varandra i en verksamhet.

Flera av de intervjuade upplevde att leverantören tog ett stort ansvar och agerade enligt villkoren i avtalet för att på olika sätt stödja och hjälpa kunden. Att leverantören ska leverera mer än vad som är avtalat är dock inte något kunden kan räkna med utan istället är den rimliga utgångspunkten att det som står i avtalet gäller. I många fall kommer leverantören, när flera kunder drabbas samtidigt, att ha svårt att leva upp till alla kunders avtal, flera incidenter pekar på att leverantören de facto gör en prioritering av vilken kund man hjälper först.

Några intervjuade har reflekterat över kompetensnivån rörande systemadministration hos de leverantörer de anlitar, liksom deras förhållningssätt till kontinuitetsarbete och erfarenhet av krishantering[42]. Förmågan att kunna leverera med kvalitet hänger ihop med kunskapen om att systematiskt arbeta med informationssäkerhet och it-säkerhet och att göra detta kontinuerligt. Liksom

41. Detta kan ha betydelse om det är en aktör som är extra utsatt t.ex. för tillgänglighetsattacker, vilket gör att leverantörens samtliga system kan komma att påverkas. Riskerna är även då större att råka ut för kaskadeffekter, t.ex. vid återuppstart av leverantörens system.
42. Vidare var flera kunder skeptiska till de tekniska lösningar som leverantörerna verkar ha använt, hur de konfigurerat de tekniska lösningarna samt hur de koordinerat aktörernas samvaro i miljön.

kunderna bör ha kunskap om sina beroenden, bör även leverantörerna analysera vilka processer som påverkas i verksamheten och identifiera kritiska leveranser.

Leverantörerna å sin sida upplevde många kunder som okunniga om sina system och att kunderna ofta hade dålig kännedom om förekomsten och innehållet i de avtal som upprättats. Till detta tillkommer att leverantörerna lever i en kommersiell verklighet, där vinstmarginaler löpande ställs mot ansvaret för kundens data.

Även en hög kunskapsnivå rörande system- och nätverksdesign samt support och underhåll av systemen hos leverantören ansåg en del intervjuade vara en viktig faktor för framtida val av leverantör, liksom om leverantören hade stor genomströmning av personal på kritiska tjänster. Även leverantörens tekniska upplägg var en viktig faktor för förtroendet.

I vissa intervjuer framkom en viss frustration kring att det inte finns andra åtgärder än avtalsvägen för kunder med samhällsviktig verksamhet för att säkerställa att leverantören inte lade flera för samhället viktiga tjänster tillsammans i samma servermiljö.

Förmågan att hantera incidenter

4. Förmågan att hantera incidenter

Det hanterande arbetet tar vid där det förebyggande inte går att använda eller inte räcker till, t.ex. i de fall där det bedöms kosta för mycket att förebygga, eller där det inte är tydligt hur händelsen kan förebyggas. Målsättningen är att det ska finnas en förmåga att genom planering och andra förberedelser påbörja, eller medverka i, arbetet för att ***avhjälpa*** *en it-incident, samt i möjligaste mån återställa skadade strukturer eller individer till ett normaltillstånd*

Fokus i det hanterande arbetet är att se till att förutsättningarna blir så bra som möjligt för att kunna göra medvetna val vid en nära förestående eller inträffad incident så att händelsens negativa konsekvenser begränsas.

4.1 Kontinuitetshantering

Kontinuitetshantering är en metod för att på ett strategiskt sätt skapa en förmåga att kunna fortsätta att bedriva sin verksamhet på en tillräcklig nivå, oavsett vilken typ av störning som organisationen utsätts för.[43] I den tidigare nämnda rapporten om den stora it-incidenten som Tieto råkade ut för 2011 framkom betydelsen av fungerande kontinuitetshantering både hos kunden och hos leverantören.

När det gäller kontinuitetshantering så pekar tyvärr allt på att de flesta verksamheter inte gör tillräckligt. I den studie som MSB gjort vad gäller statliga myndigheters informationssäkerhet så uppger 65 % av myndigheterna att det de saknar en kontinuitetsplan. Nära 60 % av myndigheterna uppgav att de inte använder riskanalyser som stöd vid kontinuitetsplanering. Det finns tyvärr inget som pekar på att det är väsentligt annorlunda inom många andra sektorer.

Inom ramen för arbetet med kontinuitetsplanering ingår att skapa en särskild process för it-incidentberedskap. Det finns flera principmodeller för detta. Information Technology Infrastructure Library,

43. För mer om kontinuitetshantering se ISO 22301:2012 Samhällssäkerhet – Ledningssystem för kontinuitet – Krav. MSB kommer under 2014 ta fram en svensk vägledning.

ITIL, är en sådan[44]. CERT-SE[45] vid MSB har också utvecklat en incidenthanteringsprocess, baserad på internationella standarder och Best Practice, vilken beskriver ett arbetssätt från det att incidenten upptäcks tills den åtgärdas och ärendet stängs[46].

När en störning inträffar måste alla involverade i organisationen för it-incidenthantering veta vem som gör vad och när. Roller, ansvar och rutiner internt måste följaktligen vara tydligt definierade och dokumenterade i förväg för att organisationen snabbt ska kunna återgå till ett normaltillstånd igen. Hantering av en it-störning innebär att en mängd åtgärder ska vidtas under förhållanden där tiden för återställande ofta är mycket kort innan verksamheten börjar drabbas av allvarliga problem. Etablerade kommunikationsvägar till relevanta kontakter internt och externt spelar en nyckelroll i detta sammanhang.

It-relaterade störningar och andra oönskade händelser uppstår dagligen Att helt eliminera risken för dessa är inte en realistisk utgångspunkt. Det primära målet för organisationer bör i stället vara att minska risken för att de ska inträffa genom att vidta förebyggande åtgärder och arbeta proaktivt för att på bästa sätt kunna hantera de incidenter som inträffar.

Genom riskbedömningar och konsekvensanalyser som ingångsvärden kan organisationen skapa sig en helhetsbild av verksamhetens krav på kontinuitet[47]. Detta arbete är nödvändigt för att i nästa steg kunna utarbeta en kontinuitetsplan som styr verksamhetens återhämtning vid störningar och avbrott som bland annat påverkar informationssäkerheten.

Som organisation är det viktigt att se över sin it-miljö:

- Hur ser ansvarsfördelningen ut?
- Är mandat och roller tydliga?
- Hur ser beroendena ut i verksamheten som helhet (inklusive utkontraktering till it-leverantörer)?
- Är den teknik som används lämplig för den risknivå man vill hålla?
- Är samtliga ansvarsfrågor lösta?

44. Se bl.a. http://www.itil-officialsite.com/. Se även SS-ISO/IEC 270002:2014, kap. 16.
45. CERT-SE är Sveriges nationella CSIRT (Computer Security Incident Response Team) och finns vid MSB.
46. Se https://www.cert.se/incidenthantering/
47. Läs mer om kontinuitetshantering i kap. 17 Informationssäkerhetsaspekter avseende hantering av verksamhetens kontinuitet i standarden SS-ISO/IEC 27002:2014, Informationsteknik – Säkerhetstekniker – Riktlinjer för informationssäkerhetsåtgärder, SIS Förlag AB, 2014.

Det är viktigt att dessa frågor är utredda och besvarade innan it-incidenten är ett faktum. Bestämda, tydliga rutiner som personalen har kännedom är också av stor vikt. Noterbart är att de tillfrågade organisationer som tillämpade en förutbestämd rutin, en modell för incidenthantering, ansåg sig klara hanteringen bättre tack var detta. I standard SS-ISO/IEC 27002:2014 om informationsteknik finns en vägledning för hur en organisation kan gå tillväga för att skydda de av organisationens tillgångar som leverantören har åtkomst till genom avtal. Här beskrivs även vikten av att ställa krav på ”försörjningskedjan” för informationen[48].

4.2 Kommunikationens betydelse i incidenthanteringen

De fall som ligger till grund för denna rapport har det gemensamt att de beskriver it-incidenter som drabbade stora aktörer, inom kritiska sektorer som t.ex. vård och omsorg. Händelserna uppstod hastigt, mer eller mindre oväntat och utan förvarning. En allvarlig it-incident kan, som händelserna i denna rapport visat, snabbt utvecklas till en svår påfrestning, dvs. en kris. Att många av de drabbade organisationerna utsattes för en svår påfrestning råder inga tvivel om. Kretsen av de som berördes av respektive it-incident var dessutom väldigt stor.

Både företag och myndigheter drabbades och därmed deras anställda och kunder och i några fall även allmänheten i stort. För många innebar störningarna att deras kommunikationsförmåga sattes på prov. Det gäller både kommunikationen internt och den som riktades utanför den drabbade organisationen. En analys av händelseförloppen i vissa av fallen ger flera exempel på hur arbetet med hanteringen av själva incidenten var nära kopplat till kommunikationen internt och externt.

Kommunikationen måste kunna flyta i flera riktningar under en kris[49]. Informationsbehovet kan vara mycket stort och omfatta ett väldigt stort antal personer. Aktörerna och berörda kan ena stunden vara sändare och i den andra stunden mottagare av information. Att en leverantör av it-tjänster står i ständig kontakt med sina kunder, beställarna, och informerar dem om händelseutvecklingen kring en it-incident är en förutsättning för att dessa

48. SS-ISO/IEC 270002:2014 om Informationsteknik – Säkerhetstekniker –Riktlinjer för informationssäkerhetsåtgärder, kap. 15.
49. Stora delar av texten i detta avsnitt är baserad på det informationsstöd för krishantering i kommuner och landsting som MSB tagit fram. https://www.msb.se/sv/Kunskapsbank/Informationsstod-Krishantering-/

kunder i sin tur ska kunna föra informationen vidare internt eller externt. På motsvarande vis är leverantören i behov av att få bekräftat av sina kunder att de återställningsåtgärder som vidtagits också fungerar.

Användarna, dvs. de övriga anställda, som i en drabbad organisation inte är involverade i själva hanteringen av incidenten är en kategori som nästan alltid drabbas av konsekvenserna av en störning. De behöver därför löpande hållas informerade om händelseutvecklingen och prognosen för återställande. De måste också få veta var sådan information går att finna. I SLL:s slutrapport avseende driftstoppen som drabbade TakeCare framkom t.ex. *"att informationen till användarna i verksamheterna varierade i kvalitet under pågående driftavbrott. Flera användare har heller inte vetat var de skall söka aktuell information beträffande driftstörningarna"*[50].

Ur allmänhetens perspektiv är medierna ofta den viktigaste förmedlaren av bilden av en kris och det gör att den drabbade organisationen, oavsett omständigheterna, är beroende av media som kommunikationskanal. Media spelar en enormt viktig roll i samband med kriser i samhället genom sin förmåga att snabbt nå ut med information till många på en gång. Det finns därför flera skäl till varför en aktör bör bygga upp en bra organisation och förmåga till kriskommunikation. Lyckas man med kommunikationen så ökar också möjligheterna att till att påverka hanteringen av krisen.

Exemplet Anonymous och dataintrånget i VGR

Det är ibland svårt att se betydelsen av kommunikation, särskilt internt. Detta gäller särskilt för it-incidenter där it-verksamheten kan uppleva att problemet är löst (ärendet avslutat), men där det kan uppstå stora informationsbehov ibland långt i efterhand.

I augusti 2012 drabbades Västra Götalandsregionen, VGR, av ett externt dataintrång. VGR fick tidigt information om att något inte stod rätt till genom att CERT-SE skickade ett säkerhetsmeddelande till VGR med information om att en eller flera av deras hemsidor hade förvanskats. Händelsen kunde hanteras relativt snabbt eftersom sårbarheten i systemet var begränsad[51].

Tre månader senare, i november 2012, blev incidenten medialt uppmärksammad av Expressen som gick ut med att Anonymous

50. Se Analyskommissionens slutrapport avseende driftstoppen som drabbade TakeCare 11 och 18 juni 2013, SLL, 2013-10-11, sid. 5.
51. Intrånget innebar åtkomst till system som innehöll patientuppgifter, men även andra system drabbades.

gjort intrång i VGR:s system, vilket väckte stor uppmärksamhet. VGR fick då hantera ett stort antal medier samt enskilda som ville ha information.

När dataintrånget skedde var den initiala bedömningen av VGR IT att händelsen inte skulle ge några stora konsekvenser för verksamheten. VGR:s ledning fick först information om att det var en hemsida som ändrats, vilket inte ansågs så farligt. För VGR IT som hanterade händelsen så var incidenten främst ett tekniskt problem som skulle lösas så att den vanliga verksamheten påverkades så lite som möjligt.

I regionens krisplan står det att krishanteringen i VGR bl.a. syftar till att skydda grundläggande värden som förtroende. Vid en extern utvärdering som VGR låtit utföra påpekas att VGR IT i det läge som uppstod borde ha funderat kring vad händelsen kunde få för konsekvenser för förtroendet för VGR (oavsett om händelsen offentliggjordes eller ej). VGR IT informerade ett antal aktörer inom organisationen om it-incidenten. Detta borde ha fått VGR att överväga att aktivera sin krisorganisation, men det skedde inte. Genom att initiera krisplanen så hade funktionen ”kriskommunikation” aktiverats. Därmed hade personer med expertkunskap på kommunikation kunnat förbereda både intern och extern kommunikation. När så Expressen tre månader senare började skriva om händelsen, så fanns det inga förberedda kommunikationsplaner eller budskap, varken in i organisationen (t.ex. till ledningen) eller ut till det offentliga. VGR hamnade därmed i en svår situation, där organisationen fick värja sig för påståenden om ”mörkläggning” m.m., samt att de hade mycket svårt att få ut sitt budskap.

Till it-organisationens försvar ska sägas att det många gånger är svårt att se de fullskaliga konsekvenserna av en it-incident innan den är ordentligt analyserad, vilket ofta tar tid (lägesbild). Till det kommer sedan att det ofta är svårt att göra bedömningen att man nått en punkt där man ska gå över till krisorganisation (lägesbedömning). Detta gäller särskilt om det inte rör sig om tillgänglighetsproblem utan snarare om konfidentialitets- eller riktighetsproblem.

Övriga reflektioner

5. Övriga reflektioner

I detta kapitel redovisas några ytterligare reflektioner som framkommit i arbetet med denna rapport. Då dessa inte ingick som del i de strukturerade intervjuerna har vi valt att lägga dessa i ett eget kapitel.

5.1 Kostnadsaspekten

Ett område som inte är så belyst är de kostnader som är förknippade med it-incidenter, detta gäller både på aktörsnivå och på samhällsnivå.

Vad kostar ett it-avbrott? Det kostar att systematiskt investera i informationssäkerhet, men kostnaden att inte göra det kan bli långt högre. Flera av de intervjuade säger, främst när det gäller kostnader som är svåra att mäta i pengar: *”Säkerhet kostar pengar, osäkerhet kostar mer.”* Ett förtroende kan snabbt urholkas och en organisations goda rykte kan snabbt raseras på grund av problem med informationshanteringen.

Kostnaden kan vara direkt (akuta åtgärder såsom extrapersonal, ytterligare tekniska åtgärder osv.) eller indirekt (kostnadsbortfall när inte it-miljön fungerar som tänkt, t.ex. att inga biljetter säljs). Kostnaden kan även vara av engångskaraktär (såsom övertidsersättning i en akut fas) eller återkommande (såsom nya tekniska skydd hos en leverantör som betalas månadsvis). Det är många parametrar som ska vägas samman för att räkna ut den totala kostnaden för en incident. Alla dessa parametrar borde tas hänsyn till när man ställer kostnad för ett ökat skydd i relation till kostnad för en incident.[52]

Flera av incidenterna i denna rapport har medfört stora kostnader, vilket sannolikt även medfört en kostnadsökning ute i slutanvändarledet. När det gäller tillgänglighetsattacken i södra Sverige 2013, så uppger Skånetrafiken att de tappade cirka 4,4 miljoner i intäkter på grund av uteblivna intäkter på biljetter med Jojo reskassa, SMS eller enkelbiljetter i biljettautomater.

52. Ett mätverktyg som kan användas för att beräkna hur stor finansiell påverkan som bristen på säkerhetsinvesteringar kan leda till är t.ex. ROSI-metoden (Return on security investment).

I samband med händelserna hade Skånetrafiken också ökade kostnader på närmare en halv miljon kronor för konsultinsatser och tekniska insatser i it-miljön. Dessutom har ett utökat skydd hos leverantören medfört en årlig kostnadsökning på cirka 400 000 kronor.

Även för leverantörer av it-tjänster kan avbrott bli kostsamma. Enligt medieuppgifter förväntades EVRY under våren 2014 presentera ett negativt resultateffektmått för första kvartalet 2014 som uppskattas till i storleksordningen 30–40 miljoner norska kronor[53]. Leverantören kan även få skadeståndskrav eller behöva betala vite i de fall där så avtalats.

I fallet med den skadliga koden i Västra Götaland 2012 beräknades enbart kostnaden för att omhänderta de tre läkemedelsautomaterna som drabbades på Södra Älvsborgs sjukhus till cirka en halv miljon kronor. En grov uppskattning på hela händelsen med skadlig kod har angetts till en kostnad på 2–3 miljoner kronor för bl.a. bortfall i produktion och övertid.

Att få ner kostnaderna för it-hantering är idag en mycket starkt pådrivande faktor för att välja en extern it-leverantör, men flera av de intervjuade har reflekterat över att utkontraktering idag är ett måste p.g.a. höga krav från användarna på flexibilitet och utvecklingskrav på den tekniska miljön. Kostnadsbilden gör att många aktörer tvekar att ens diskutera med sin ledning om möjligheterna att ha dubblerad datalagring (dvs. att ha lagring m.m. av data på fysiskt åtskilda platser, dvs. i olika datahallar).

En annan aspekt är den reflektion som leverantören EVRY gjorde i kontakten med sina kunder i samband med återställningsarbetet efter branden. EVRY:s bedömning var att kunder med moderna (och helst väl dokumenterade) system kunde återställas betydligt snabbare än äldre system. För en it-ansvarig kan det vara svårt att få fram pengar till moderniseringar av den egna organisationens it-system. Men mot detta bör ställas att det sannolikt kan minska tiden som systemen står stilla vid en incident, vilket är till (ekonomisk) gagn för organisationen.

Några av de intervjuade reflekterade över möjligheten att skapa en skyddad miljö, utan vinstkrav, hos en offentlig aktör. Detta ansågs vara en bra lösning för svenska krisberedskapsmyndigheter,

53. EVRY vinstvarnar efter nyårsbrand, IT24, 2014-02-10.

även om det fanns risk att det skulle snedvrida konkurrensen på marknaden samt att lösningen inte skulle omfatta all samhällsviktig verksamhet som idag bedrivs i privata företag.

Flera av de intervjuade kom tillbaka till frågan om förtroende; vad kostar egentligen förtroende, eller rättare sagt tappat förtroende?

5.2 Återställningsprioritet

En fråga som ställdes efter Tietokraschen 2011 var hur och på vilken grund leverantören prioriterade vilken kund som skulle få återställning av sina system först (återställningsprioritet). I en akut situation kan leverantören hamna i en målkonflikt där en viktig samhällsfunktion måste stå tillbaka för en annan eftersom leverantören inte hinner med att hjälpa alla samtidigt. I denna situation är det upp till leverantören att bestämma prioritetsordning.

Vid förfrågan hos de i denna rapport aktuella leverantörerna uppger de att återställningsprioritet skedde efter

- vad leverantören uppfattade var samhällsviktigt
- hur kundens avtal var formulerat
- hur kundens hårdvara var konfigurerad; nyare utrustning prioriterades.

Här aktualiseras frågan om vem som ska definiera vad som ska anses vara samhällsviktigt. För en del aktörer blir detta en kluven upplevelse. Ett stort bolag uppger att de inte definieras som samhällsviktiga enligt staten, men att bolaget däremot klassas som ”samhällskritiskt” av sin leverantör, som bedömer att bolagets verksamhet har stor samhällspåverkan. Här kan man enbart spekulera hur bolaget hade prioriterats vid incidenten om det motsatta förhållandet hade rått.

I detta sammanhang behöver man också trycka på varje aktörs egna ansvar för att upprätthålla sin verksamhet vid allvarliga störningar. Arbetet med samhällets krisberedskap utgår från ansvarsprincipen, vilket innebär att den som har ansvar för en verksamhet under normala förhållanden har motsvarande ansvar under kris- och krigssituationer. Ansvarsprincipen innebär också ett ansvar för varje aktör att samverka med andra.[54]

54. Ansvarsprincipen framgår bland annat av förordning (2006:942) om krisberedskap och höjd beredskap.

5.3 Timing och tur

Flera av de intervjuade pekar på att de haft tur att incidenten inträffat vid ett lågproduktionsläge eller att incidenten inte påverkat ”den andra servern”, dvs. att incidenten kunde förvärrats kraftigt om andra system påverkats. Timing och tur återkommer som en röd tråd i samtalen med aktörerna.

Det tydligaste exemplet på tur i denna rapport är nog branden hos EVRY där ett transportföretag bedömde att ett massivt transportstopp kunde ha blivit resultatet om deras andra server hade påverkats mer än den gjorde. PostNord påpekar också att de hade tur eftersom de befann sig i en lågproduktionsfas. Om incidenten inträffat vid högsta arbetstoppen hade problemen för verksamheten blivit betydligt större. Hade det skett innan jul, med dess ökade mängd paketleveranser, hade resultatet varit ytterst olyckligt för företaget. En praktisk effekt hade dessutom varit de problem som uppstått om företaget inte hade haft möjlighet att lagra alla leveranser som inte kunnat levereras.

Även en myndighet menar att det var tur att inte branden skedde vid en annan tidpunkt. Under vissa perioder har myndigheten stora transaktionsflöden, där både myndigheten och kunden är beroende av väl fungerande service.

Timing av en incident går sällan att påverka. Däremot går det att arbeta systematiskt med informationssäkerhet så att timing inte blir avgörande för utfallet.

Hur stärker vi då förmågan ytterligare?

6. Hur stärker vi då förmågan ytterligare?

En god informationssäkerhet är i hög grad beroende av organisatoriska förutsättningar. De organisatoriska förutsättningarna skapar styrning, medvetenhet, resurser och motivation för genomförandet av säkerhetsåtgärder. Förmågan att hantera it-incidenter av den typ som ingår i rapporten kan därför kopplas till de organisatoriska förutsättningarna.

Intervjuerna som utgör underlag för rapporten visar på att det finns stora skillnader både i hur man arbetar med informationssäkerhet och på den nivå av informationssäkerhet som finns i respektive organisation. I vissa (få) fall har det funnits en för organisationen inarbetad metod med utpekade funktioner och processer för att arbeta systematiskt med informationssäkerhet i hela verksamheten; i andra fall är det en ensam persons initiativ som har fått styra. I vissa fall har arbetet med informationssäkerhet accepteras av ledningen som ett grundläggande krav för verksamhetens överlevnad. I andra fall är det en pålaga, om det ens utförs några insatser. I vissa fall får säkerhet kosta och i andra fall inte.

Samhället i sin helhet är beroende av att de enskilda aktörerna har en ändamålsenlig informationssäkerhet i sin verksamhet. Det finns därför anledning att se närmare på några av de faktorer som kan leda till en bättre förmåga att hantera it-incidenter.

6.1 Ledningens engagemang måste öka

För att förebygga och hantera händelser, så krävs det att någon tar ansvar, sätter en kravställning och följer upp. Detta kan både ske inom den egna aktörens organisation, men det kan även vara externa krav som ställs t.ex. från samhället.

När det gäller enskilda aktörer och deras ansvar, så måste ledningen ta ett formellt ansvar för hanteringen av informationssäkerhetsrisker. Arbetet bör i första hand ske genom verksamhetens befintliga strukturer företrädesvis genom en implementering av en riskhanteringsmodell. Här är det viktigt att ledningens riskacceptans tydliggörs. Vidare bör ledningen besluta om att en beroendeanalys ska ske avseende den egna organisationens beroenden t.ex. vad avser försörjningskedjor.

Utöver att ta ett formellt ansvar, så bör ledningen aktivt engagera sig i arbetet med riskhantering. Genom detta arbete kan ledningen få en mycket bra bild av organisationens styrkor och svagheter.

För att nå fram till ledningen, så krävs det insatser med utbildning och information för att medvetandegöra.

6.2 Förmågan att styra och prioritera måste stärkas

En mycket stor del av all datalagring sker idag hos privata leverantörer. Att nyttja externa aktörer för sin datalagring är idag mer eller mindre ett måste för all verksamhet i samhället, även samhällsviktig sådan. Detta medför, liksom vid all form av utkontraktering, att risker måste analyseras och att medvetna avvägningar måste ske mellan kostnad och säkerhet i form av krav på tillgänglighet, konfidentialitet, riktighet och spårbarhet. Först därefter ska förankrade beslut tas. Aktörens ansvar för sin information kan inte delegeras till leverantören.

För myndigheter finns det en föreskrift från MSB med bestämmelser om myndigheternas arbete med informationssäkerhet[55]. Enligt föreskriften ska ledningen ta beslut om åtgärder för att säkra informationssäkerheten bl.a. utifrån risk- och sårbarhetsanalyser. Liknande krav på analys finns i förordning om krisberedskap och höjd beredskap[56], där även vissa affärsverk ingår. I denna står bl.a.: *"Varje myndighet ansvarar för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt."* Detta ställer stora krav på myndigheter att ta ansvar för sin informationssäkerhet och säkerställa att kontinuitet kan hållas i verksamheten.

Idag spelar i stort sett alla samhällsaktörer på samma spelplan när det gäller kraven på it- och informationssäkerhet[57]. Det finns inga undantag när det gäller upphandling av it-stöd för samhällsviktig verksamhet. Vidare finns det inga krav på att samhällsviktiga system ska hålla viss standard när det gäller informationssäkerhet, bortsett från de myndigheter som omfattas av MSB:s föreskrift om statliga myndigheters informationssäkerhet. Oavsett

55. MSBFS 2009:10 Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet.
56. Förordning (2009:942) om krisberedskap och höjd beredskap.
57. Det finns vissa undantag: MSB:s föreskriftsrätt vad avser statliga myndigheter, se MSBFS 2009:10 Föreskrifter om statliga myndigheters informationssäkerhet, samt de krav som finns för system som ska hantera viss sekretessmarkerad information.

om det är företagskänslig data eller om det är samhällsviktig information, så är det affärsavtal som gäller för att sätta krav på informationssäkerhet gentemot leverantörer.

Vid en allvarlig it-incident finns idag inga möjligheter för staten att gå till en leverantör och begära att samhällsviktig verksamhet ska prioriteras t.ex. vid uppstart. Detta är en utmaning. Att lagstiftningsvägen ställa särskilda krav på skydd av samhällsviktig verksamhet skulle sannolikt bli kostnadsdrivande och frågan blir då vem som ska bära kostnaden. Att ställa krav på leverantörerna skulle på motsvarande sätt driva upp kostnadsbilden. Att arbeta med it-incidentrapportering samt att stärka upphandlingsförfarandet, t.ex. med tillsyn vad avser informationssäkerheten, skulle eventuellt vara framkomliga vägar som skulle kunna stödja förmågan att hantera och förebygga. Oavsett vilket alternativ som väljs så behövs frågan belysas ytterligare.

6.3 Förutsättningarna för lägesbild måste stärkas

Ur ett samhällsperspektiv är det ett problem att olika samhällsviktiga verksamheter, genom omedvetna beslut, hamnar hos samma driftleverantör. I kombination med undermåliga avtal och/eller en oansvarig leverantörs beteende, kan en incident därigenom få mycket stora konsekvenser för samhället.

Idag finns inget krav på myndigheter med samhällsviktig verksamhet att meddela vilken it-leverantör de anlitar till MSB eller någon annan myndighet. Det finns inte heller några möjligheter för MSB eller någon annan att få ut information från leverantören om de inte själva väljer att delge den. Den enskilda kunden kan dock få ut information om avtalet är rätt skrivet. Men ur ett krishanteringsperspektiv är förutsättningarna inte särskilt goda för att kunna skapa en god lägesbild vid större it-incidenter som drabbar flera olika delar av samhället. För att komma till rätta med detta lämnade MSB 2011 respektive 2012 förslag till regeringen avseende ett nationellt system för it-rapportering[58].

Det ligger idag ett stort ansvar på de myndigheter som är centrala för att samhället ska fungera. Dessa måste säkerställa att beslut om it- och informationssäkerhet tas med en hög medvetenhet om säkerhet och att ett aktivt arbete med informationssäkerhetsfrågorna sker för hela sitt ansvarsområde. Det gäller både tekniska

58. System för obligatorisk incidentrapportering för statliga myndigheter, MSB 2011, respektive Nationellt system för it-incidentrapportering. Svar på regeringens uppdrag till MSB, 2012.

installationer, riskhantering, administrativa rutiner och organisatoriska ansvarsfrågor. De måste även kunna leverera en (sektors-) lägesbild inom sitt område när så krävs. Detta ansvar kan inte delegeras till en leverantör.

6.4 Satsa på riskhantering och informationsklassning

Den enskilt viktigaste faktorn för att få till ett framgångsrikt riskhanteringsarbete är att ledningen beslutar om att organisationen ska satsa på att arbeta förebyggande och investera i åtgärder för att avvärja incidenter, inte enbart kunna hantera uppkomna situationer. En bra riskanalys där ledningens riskacceptans finns dokumenterad är en god början. Utifrån en sådan kan man sedan planera lämpliga åtgärder för att upprätthålla informationsförsörjningen till de prioriterade processerna. Det är viktigt att ledningen tar medvetna beslut, även om besluten kan var svåra att ta.

Arbetet med att använda en informationsklassningsmodell är ofta omoget i många organisationer. Frågor som *Vad ska klassificeras?*, *Vem är mottagare av modellen?* och de juridiska aspekterna orkas många gånger inte med. För att detta ska fungera på ett tillfredsställande sätt måste det finnas klara ansvarsförhållanden som styr vilken aktör som har ett visst ansvar. Grundläggande roller är informationsägare respektive system/tjänsteägare där informationsägaren är den aktör som är kravställare även vad gäller informationssäkerhet.

Tyvärr så händer dessutom allt för ofta att organisationer inte fullt ut känner sin it-miljö och därigenom inte heller inser vilka konsekvenser olika lösningar kan ha på verksamheten. Till detta kommer också det faktum att allt för många, som har upphandlat en tjänst, har en dålig uppfattning om vad deras upphandlande tjänst faktisk omfattar. En analys som visar på olika beroenden, i alla perspektiv, är central så att beslutsfattare förstår konsekvenser av störningar och av de åtgärder som kan behövas för att kunna återgå till normalläge igen.

6.5 Förmåga till kommunikation vid kris måste öka

Förmågan att upprätthålla en god kommunikation mellan den som har ansvar för en viss verksamhet och de som blir, eller riskerar att bli, direkt eller indirekt påverkade av it-incidenten är ofta en vattendelare. Alla samhällsviktiga aktörer bör bygga upp en organisation och förmåga till kriskommunikation. Alla

medarbetare i organisationen behöver förstå vikten av kommunikation vid kriser. Nyckelpersoner måste ha kunskap om hur kommunikation ska gå till. Informatörer behöver få utbildning i handgrepp, kunskap och verktyg. Slutligen måste chefer och andra företrädare utbildas och tränas i att möta medier.

Lyckas man hantera kommunikationen så ökar också möjligheterna att påverka uppfattningen om hanteringen av krisen. Konsekvenserna kan minimeras och man riskerar förhoppningsvis inte att läget förvärras.

6.6 Satsa på övning och kompetens

Utbildning och övning utgör grunden för att organisationen ska kunna ha en väl fungerande krisorganisation. Organisationen bör ha en implementerad kontinuitetsplan, som övas till dess att den är väl förankrad i organisationen. Som visat i ett exempel i denna rapport, så kan improviserade informationsöverföringar och ansvarsfördelningar uppfattas som oklara och riskabla när man tvingas bort från sina ordinarie rutiner.

Övningar utvecklar och stärker individers och gruppers agerande för att förebygga och hantera händelser. Med rätt kompetens kan organisation och individ lösa uppgifter även vid svåra it-incidenter. Roller, mandat och rutiner ska vara tydliga innan en it-incident inträffar.

Det bör satsas mer på övningar med inriktning på att testa organisationers förmåga att hantera information säkert. Till viss del sker det idag övningar med inriktning mot tillgänglighet, medan perspektiven konfidentialitet, riktighet och spårbarhet i stort sett aldrig övas. Övningarna bör involvera hela organisationen och inte enbart it-avdelningen. Vidare bör fler övningar ske tillsammans med de viktigaste externa aktörer som organisationen är beroende av t.ex. leverantörer av utkontrakterad it och internetleverantörer.

Bilagor

Bilagor

Källor och underlag från intervjuer

I syfte att inhämta närmare information om konsekvenser och vidtagna åtgärder i de olika beskrivna fallen, så har sexton personer/funktioner intervjuats[59]. Målsättningen har varit att få en bra balans mellan intervjuer av drabbade aktörer respektive orsakande aktörer (i de fall det fanns).

Funktioner som har intervjuats:

- It-säkerhetschef och/eller säkerhetschef eller motsvarande
- Driftansvarig it
- Chief information officer
- Verksamhetsansvarig för drabbad verksamhet.

I de fall det varit aktuellt har målsättningen varit att incidenthanterare hos leverantör/facilitator intervjuats. Förutom intervjuer har nedan listade källor använts i rapporten.

Generellt underlag

Handlingsplan för skydd av samhällsviktig verksamhet, MSB 2013.

Informationssäkerhetsaspekter avseende hantering av verksamhetens kontinuitet i standarden SS-ISO/IEC 27002:2014, Informationsteknik – Säkerhetstekniker – Riktlinjer för informationssäkerhetsåtgärder, SIS Förlag AB, 2014.
https://www.informationssakerhet.se/sv/ (MSB:s hemsida för informations-säkerhetsfrågor)

Nationellt system för it-incidentrapportering. Svar på regeringens uppdrag till MSB, Dnr 2012-2637.

MSB740 En bild av myndigheternas informationssäkerhetsarbete 2014 – tillämpning av MSB:s föreskrifter.

Prop. 2007/08:92 Stärkt krisberedskap – för säkerhets skull.

Reflektioner kring samhällets skydd och beredskap vid allvarliga it-incidenter, MSB 2011.

59. I fallet med TDC har enbart skriftligt material använts.

Samhällets informationssäkerhet – nationell handlingsplan 2012, MSB 2012.

SS-ISO/IEC 270002:2014 om Informationsteknik – Säkerhetstekniker – Riktlinjer för informationssäkerhetsåtgärder.

System för obligatorisk incidentrapportering för statliga myndigheter. Svar på regeringens uppdrag till MSB Fö2010/701/SSK, MSB 2011.

Vägledning för fysisk informationssäkerhet i it-utrymmen, MSB 2014.

Vägledning för samhällsviktig verksamhet, MSB 2014.

Vägledning – informationssäkerhet i upphandling, MSB 2013.

Överbelastningsattacker

Att hantera överbelastningsattacker, MSB 2014.

Computer Sweden, 2013-09-17 ”Kris i Skånetrafiken efter DDoS-attack”.

HD 2014-01-16 ”Hackers stör kommunens datatrafik”.

Kvällsposten, 2013-02-06 ”Kävlinge kommuns hemsida hackad – igen”.

MSB 2013-10-16, Statusrapport DDoS-attackerna 17–19 september 2013.

Ny Teknik, 2013-09-19 ”IT-attack slog ut SJ:s biljettsystem”.

Ny Teknik, 2013-09-20 ”Grupp tar på sig hackerattacker”.

Sydnytt, 2013-09-21 ”Polisen om it-attackerna: ”Vi jobbar intensivt”.

Sydsvenskan, 2013-09-19 ”Tunga instanser drabbade av IT-attacker”.

Sydsvenskan, 2013-02-06 ”Kävlinges webb hackad”.

Sydsvenskan, 2013-09-18 ”Flera stora hemsidor slogs ut”, ”Kävlinge kommun hackad”, ”IT-attack mot Region Skåne”.

Underlag CERT.SE.

Skadlig kod samt intrång VGR

IT-säkerhetshändelser 2011, årsrapport VGR IT, version 1.0.1, dnr SN 134-2012, 2012-01-30.

IT-säkerhetshändelser 2010, årsrapport VGR IT, version 1.0.1, dnr SN 00166-2011, 2011-01-30.

Läkemedelsautomaterna utsatt för skadlig kod, Händelseanalys, ärendenummer AV-095407, Södra Älvsborgs Sjukhus.

Rapport gällande ”skadlig kod” Västra Götalandsregionen Dec 2012–Jan 2013, version 1.0, VGR IT, Västra Götalandsregionen, 2013-09-19.

Rapport Översyn av informationssäkerheten i Västra Götalandsregionen, 2013-01-31, dnr RS 518-2011.

Störning hos tele/nätoperatör

Anteckningar från telefonmöte med TDC 130409, MSB.

Ekot 130403, Just nu: Svårt att ringa sjukvården.

Göteborgsposten, 130403: Internet slocknade för tusentals arbetsplatser,
http://www.gp.se/nyheter/sverige/1.1506623-internet-slocknade-for-tusentals-arbetsplatser

IDG: Jättehaveri hos TDC,
http://www.idg.se/2.1085/1.500213/stort-haveri-hos-tdc

Inera:
http://www.inera.se/OM-OSS/Nyheter/Nyheter/Handelseanalys-ska-goras-av-onsdagens-driftstopp/

http://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=5493323

PM om incidenten: MSB (arbetsmaterial, ej publicerat).

Sjunet – kvalitetssäkrat kommunikationsnät,
http://www.inera.se/TJANSTER--PROJEKT/Sjunet/

Nätverksbortfall och fel i operativsystem

Knutsson (S) med anledning av landstingets IT-säkerhet.

Läkartidningen 2013-11-01 ”Nationell kontroll av informationssäkerheten behövs”.

Analyskommissionens slutrapport avseende driftstoppen som drabbade TakeCare den 11 juni och den 18 juni 2013, SLL 131011.

Svenska Dagbladet 2013-06-11 ”Vi kunde inte läsa journalerna”.

Svenska Dagbladet 2013-06-18 ”Journalsystemet nere – igen”.

Tjänsteutlåtande LS 1311-1405 2013-11-29 Skrivelse från Helene Hellmark.

Tjänsteutlåtande LS 1311-1449 2014-02-18 Genomlysning av rutiner, direktiv och policy om informationssäkerhet.

Tjänsteutlåtande LS 1311-1456 2014-02-18 Förslag på kort- och långsiktiga lösningar för bättre och tydligare IT-säkerhet.

Brand i datahall hos leverantör

Computer Sweden, 2014-01-03 ”Posten plågas fortfarande efter branden”.

Computer Sweden, 2014-01-08 ”Fortsatta problem efter EVRY-brand”.

Computer Sweden, 2014-01-13 ”EVRYs släcksystem var utslaget vid branden”.

Computer Sweden, 2014-01-28 ”Så ska SL stoppa nya krascher”.

Computer Sweden, 2014-02-07 ”Tågsystem slogs ut i EVRY-branden”.

Computer Sweden, 2014-01-31 Låst skåp blev EVRYs fall **http://computersweden.idg.se/2.2683/1.544785/last-skap-blev-EVRYs-fall**

HelaHälsingland, 2014-01-03, ”Serverbrand påverkar tidningens kunder”.

Insatsrapport Storstockholms brandförsvar, nr 2014166161, 2014-01-01 Logg från NOS/MSB 2014-01-01–03.

IT24: EVRY vinstvarnar efter nyårsbrand, 2014-02-10, **http://www.idg.se/2.1085/1.546284/EVRY-vinstvarnar-efter-nyars-branden**

Ka.se, 2014-01-07 ” Kommunal drabbat av datahaveri”.

2014-01-20 Mötesanteckningar angående driftincidenten hos EVRY 2014-01-01.

2014-01-22 Arbetsanteckningar möte med EVRY.

http://computersweden.idg.se/2.2683/1.544785/last-skap-blev-EVRYs-fall/sida/2/nu-kommer-den-praktiska-processen

MyNewsdesk.com, 2014-01-04 ”Brand i Tomteboda påverkade XLKläder i Vilhelmina”.

Svenska Dagbladet, 2014-02-07 ”Stora störningar hos SL” **http://www.svd.se/nyheter/inrikes/stora-problem-med-sls-sajt_8862152.svd**

Tjänsteanteckning MSB 2013-3729 (tidigare störning i juli 2013).

Kriskommunikation

Kriskommunikation i praktiken. Populärvetenskaplig sammanfattning, MSP-rapport.

Informationsstöd för krishantering i kommuner och landsting (Kommun-paketet), MSB.
https://www.msb.se/sv/Kunskapsbank/Informationsstod-Krishantering-/

NISÖ2012 Erfarenhetsrapport, MSB-rapport 2013.

Utvärdering SAMÖ-KKÖ 2011, MSB-rapport, 2011.

Rapport ang. stoppet av webbserver intra8 och cfwebb mellan 21/8 och 30/8 för NU-sjukvården, version 2.0, VGR IT, Västra Götalandsregionen, 120910.

Krishanteringsplan Västra Götalandsregionen, beslutad 2011-02-01, Dnr RSK 136-2010.

Granskning av hanteringen av dataintrånget, Ernst & Young, Dnr Rev 19-2013, Västra Götalandsregionen, 2013-02-27.

Granskning av hanteringen av dataintrånget 21 aug 2012. Informationshantering och kommunikation i samband med händelsen/incidenten, Ernst & Young 27 februari 2013.

CERT-SE Säkerhetsmeddelande ID #12012, 2012-08-21.

Handlingar till ägarutskottets sammanträde Vänersborg 2013-04-25.

Rapport gällande intrång i Västra Götalandsregionen 2012-08-21, VGR IT, Västra Götalandsregionen, utfärdad 2012-09-12, Diarium nr RS 2504-2012, (Ank. 2012-11-23).

Skadlig kod – några lärdomar i korthet

I samband med att Västra Götalandsregionen (VGR) drabbades av skadlig kod i december 2012, så gjorde regionen en mångfald erfarenheter. Här återges några i korthet:

- Se till att ha *en* struktur för förvaltning och systemägarskap av it.
- Se till att ha kontroll över hela datasystemet! Ha kontroll på inkopplade datorer, även leverantörers.
- Ha starka lösenord, även på leverantörens maskiner.
- Ha flera oberoende övervakningsmekanismer (redundanta larmsystem).
- Se till att användarna inte går utanför rutiner och uppmana dem att använda tillräckligt starka lösenord.
- Kontrollera it-infrastrukturen efter sårbarheter på kontinuerlig basis.
- Se till att det går att ta ut datasystem för underhållsdrift utan att verksamheten påverkas.
- Avveckla onödiga eller föråldrade system.
- Se till att ha redundans på it-specialister även under längre ledigheter som jul och sommar.
- Vid incident, gå ut med information bredare och snabbare än du tänkt! Informera andra även om du ser det som en intern it-händelse.
- Återställ inte parametrar utan att ha kollat igenom hela systemets funktionalitet först.
- Specialister behövs, men för att helheten ska bli bra krävs olika kompetenser i kombination.
- Se till att ha loggranskningsverktyg. Inför loggkorrelerings- och tidssynkroniseringsverktyg.
- Jobba systematiskt med arbetet kring it-säkerheten.
- Inför verktyg för att kunna analysera säkerhetshändelser (Security information and event management, SIEM) samt verktyg för it-forensik.
- Om möjligt, se till att ha en central för bedömning och analys av it-säkerheten.
- Utbilda personalen inom informationssäkerhet och rekrytera personal som är kunnig på it- och informationssäkerhet.

Namn, akronymer och begrepp

Här redogörs för några av de begrepp som används i rapporten. För mer om terminologi kring informationssäkerhet, se bl.a. SIS 27000-serie (SS-ISO/IEC 270002:2014).

CERT-SE
CERT-SE är Sveriges nationella CSIRT (Computer Security Incident Response Team) och finns vid MSB.

Inera
Inera ägs av de stora sjukvårdshuvudmännen i Sverige (landstingen). Inera driver en rad sjukvårdsgemensamma tjänster, som 1177.se samt kommunikationsnätet Sjunet, som byggts med hjälp av länkförbindelser hos TDC.

Kaskadeffekter
En kaskadeffekt är en ofta oförutsedd händelsekedja, beroende på en starthandling i ett system (i denna rapport it-system). Om det finns en möjlighet att kaskadeffekten har negativ påverkan på systemet är det möjligt att analysera effekten med hjälp av en konsekvensanalys eller en sårbarhetsanalys.

Region Skåne
Region Skåne, formellt Skåne läns landsting, är landstinget i Skåne län. Region Skåne ansvarar för hälso- och sjukvård, kollektivtrafik och en hållbar utveckling i Skåne. Det högsta beslutande organet är regionfullmäktige, som väljs direkt av invånarna i Skåne.

Sjunet
Sjunet är ett nationellt nätverk mellan landsting, kommuner och privata vårdgivare. Sjunet är byggt för att vara ett robust kommunikationsnät anpassat för de krav som finns i vård och omsorg.

Service level agreement (SLA)
Service level agreement, SLA, anger genom kontrakt vilken servicenivå som kunden kan förvänta sig av sin leverantör och inom vilka tidsmarginaler.

Västra Götalandsregionen (VGR)
Västra Götalandsregionen, formellt Västra Götalands läns landsting, är landstinget i Västra Götalands län. Västra Götalandsregionen

ansvarar främst för hälso- och sjukvård. Regionen har även ansvar för regional utveckling i länet och för regional kollektivtrafik samt är ägare till kollektivtrafikbolaget Västtrafik. Regionen äger även bl.a. Göteborgsoperan, Film i Väst och Göteborgs botaniska trädgård.

Myndigheten för samhällsskydd och beredskap (MSB)
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB721 - januari 2015 ISBN 978-91-7383-465-0