Myndigheten för samhällsskydd och beredskap

Reflektioner kring samhällets skydd och beredskap vid allvarliga it-incidenter

En studie av konsekvenserna i samhället efter driftstörningen hos Tieto i november 2011

MSB:s kontaktpersoner:
Enheten för samhällets informationssäkerhet
Richard Oehme, 0771-240 240

Publikationsnummer MSB 367-12
ISBN 978-91-7383-209-0

Förord

Den ökade koncentrationen av it-drift och andra it-relaterade tjänster, exempelvis molntjänster, skapar både nya möjligheter och risker.

Syftet med rapporten är att utifrån den uppmärksammade driftstörningen hos Tieto i november 2011 illustrera vilka samhällskonsekvenser en allvarlig it-incident kan ge upphov till. Till detta kommer att dra lärdomar av det aktuella fallet, främst vad gäller samhällets krishantering.

Stockholm 2012-02-21

Cecilia Nyström
Chef, Avdelningen för risk och sårbarhetsreducerande arbete

Richard Oehme
Chef, Enheten för samhällets informationssäkerhet

Innehållsförteckning

Sammanfattning

Fredagen den 25 november 2011 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. Konsekvenserna varierade kraftigt. Vissa kunder kom lindrigt undan, med enstaka funktioner utslagna under några dagar. De värst drabbade saknade i princip möjlighet att använda sina it-lösningar under flera veckor.

Den ökade koncentrationen av it-drift och andra it-relaterade tjänster, exempelvis molntjänster, skapar både nya möjligheter och risker i samhället. Denna förändring av leveransformer kan vara ett sätt att både öka kvaliteten och sänka kostnaderna i en verksamhet. Incidenten visar dock att en driftstörning hos en stor it-driftleverantör kan påverka hela samhället och att konsekvenserna kan bli omfattande. Det moderna samhället står i allt högre grad stilla när it-systemen inte är tillgängliga.

För att förebygga och hantera allvarliga it-incidenter i samhället behöver det förebyggande informationssäkerhetsarbetet stärkas ytterligare – på alla ansvarsnivåer och inom alla sektorer. Detta kräver en ökad samverkan mellan offentliga och privata aktörer. Särskilt fokus bör läggas på riskanalyser och kontinuitetsplanering som stöd både för upphandlingar och för att minska konsekvenserna av it-incidenter.

Alla aktörer i samhället måste bli bättre på att använda upphandling som ett medel för att öka sin informationssäkerhet. För att detta ska bli verklighet krävs dock en bättre kunskap om hur krav ställs på säkerhet i avtal, samt bättre tillgång till rekommendationer och praktiskt stöd. De upphandlingar som görs med stöd av Kammarkollegiet är ett viktigt verktyg för att öka informationssäkerheten i den offentliga förvaltningen.

När det gäller it-incidenter är förvarningen kort eller obefintlig, tempot högt och händelsen oftast geografiskt obunden. Den ökade koncentrationen av it-drift, och andra it-relaterade tjänster, innebär att ett stort antal aktörer kan komma att drabbas samtidigt av en incident och att konsekvenserna för samhället kan bli allvarliga. Detta ställer ökade krav på samordning och samverkan.

Samverkan och samordning vid en allvarlig it-incident förutsätter att det finns relevanta och aktuella lägesbilder på lokal, regional, sektoriell och nationell nivå. Driftstörningen hos Tieto visar att aktörerna i krisberedskapssystemet behöver utveckla förmågan vad gäller lägesbilder samt samlade konsekvens- och hanterandebedömningar. Berörda aktörer behöver skapa processer för informationsinhämtning och informationsdelning. I detta bör även ingå att kunna kommunicera information till medborgarna, vilket förutsätter en informationssamordning. Det behöver även utvecklas system för it-incidentrapportering.

1. Inledning

Driftstörningen hos it-driftleverantören Tieto i november 2011 drabbade ett stort antal samhällsaktörer inom flera olika sektorer och resulterade i flera fall i långvariga verksamhetsstörningar. Konsekvenserna av driftstörningen hade nationell spridning, var tvärsektoriell och drabbade i flera fall samhällsviktiga verksamheter.[1] Myndigheten för samhällsskydd och beredskap (MSB) inledde därför, i enlighet med myndighetens instruktion, ett antal aktiviteter. En av de centrala uppgifterna är att skapa och upprätthålla en nationell lägesbild, till detta kommer att stödja och samordna arbetet med samhällets informationssäkerhet, i vilket även ligger att rapportera till regeringen om förhållanden på området som kan leda till behov av åtgärder.

Den här rapporten har tagits fram för att beskriva de samhällskonsekvenser som en storskalig it-driftstörning kan ge upphov till. Ambitionen har inte varit att ge någon detaljerad beskrivning av själva driftstörningen hos Tieto. Syftet har heller inte varit att lämna någon uttömmande redovisning av exakt vilka organisationer som drabbades eller hur de drabbats, något som inte heller har kunnat göras då ingen enskild aktör har den överblicken.

Fokus har legat på konsekvenser inom olika samhällsverksamheter och vilka lärdomar som kan dras vad gäller krishantering – både ur enskilda verksamheters perspektiv och ur ett samhällsperspektiv. Detta för att kunna stärka samhällets förmåga att förebygga och hantera liknande händelser. Intresset är med andra ord riktat mot säkerhet och stabilitet i samhällets informationshantering (informationssäkerhet) snarare än de tekniska förutsättningarna för denna informationshantering (it-säkerhet). Det handlar således om det moderna samhällets förmåga att motstå och återhämta sig från den typ av ”tekniska kollapser” som driftstörningen hos Tieto representerar, det vill säga samhällets resiliens.

De förslag till fortsatt arbete som lämnas i rapporten tar inte sikte på att hantera den tekniska utvecklingen som sådan, eller påverka förvaltningsutvecklingens inriktning. Däremot pekar slutsatserna på att det finns informationssäkerhetsrelaterade faktorer som kan ha en stark inverkan på e-förvaltningens säkerhet och stabilitet.

En annan fråga som inte heller ligger inom ramen för rapporten är de samhällsekonomiska kostnaderna av driftstörningen.

1 För en diskussion om samhällsviktig verksamhet, se *Ett fungerande samhälle i en föränderlig värld. Nationell strategi för skydd av samhällsviktig verksamhet*. Publikationsnummer: MSB266 - december 2011, MSB.

2. Bakgrund

2.1 Ökad koncentration av it-drift och it-relaterade tjänster

På senare år har det blivit vanligt bland företag och den offentliga sektorn såväl i Sverige som i andra länder att samla sin it-drift och placera den i en central driftmiljö. Detta sker ofta i en eller flera egna datadrifthallar. Under en följd av år har många olika utrustningar med skilda egenskaper och driftsförutsättningar ersatts av så kallade virtualiserade servermiljöer. I anslutning till dessa har även datalagringen centraliserats i lagringsnätverk. Denna förändring har erbjudit såväl kostnadsfördelar som förenklad administration.

Ökande teknisk komplexitet, höga etableringskostnader och snabb teknisk utveckling har lett till att det uppstått betydande skalfördelar inom it-drift-verksamhet. Detta har fått till följd att ytterligare kostnadsfördelar idag kan erhållas genom att lägga serverdriften utanför den egna verksamheten, genom så kallad outsourcing av hela eller delar av den egna it-driften till en eller flera driftleverantörer.

Idag väljer fler och fler svenska organisationer att på detta sätt utkontraktera sin it-drift. Detta segment av it-branschen domineras av stora företag varav Tieto är ett.[2]

Till detta kommer utvecklingen av it-relaterade tjänster, bland annat så kallade molntjänster, där en organisation kan välja att låta en leverantör hantera allt från lagring av information till mycket kvalificerade tjänster. Liksom vid ren outsourcing av it-drift innebär användandet av it-relaterade tjänster en koncentration av informationshanteringen.

Utvecklingen är inte unik för Sverige, det är en internationell trend som bland annat uppmärksammats av den amerikanska motsvarigheten till Riksrevisionen, Government Accountability Office (GAO).[3] Det faller sig därför naturligt att även den offentliga sektorn tillämpar sådana lösningar för att nyttja sina resurser på bästa möjliga sätt. Detta ligger också väl i linje med regeringens övergripande mål att Sverige ska vara bäst i världen på att använda

2 Vilka de största aktörerna är går bland annat att utläsa av de ramavtal Kammarkollegiet tecknat på IT-driftområdet. Så kallade hostingtjänster avropas från Compose IT System (CITS) AB, Cypoint IT Services AB, EDB Business Partner Sverige AB, IBM Svenska Aktiebolag, IDENET AB, Office IT-Partner i Sverige AB, Qbranch Stockholm AB, TeleComputing Sweden Aktiebolag, Tripnet Aktiebolag och Volvo Information Technology Aktiebolag. Helhetsdrift avropas från CSC Sverige AB, EDB Business Partner Sverige, Fujitsu Sweden AB, Hewlett-Packard Sverige AB, IBM Svenska Aktiebolag, Logica Sverige AB, Qbranch Stockholm AB, SYSteam Outsourcing Services AB, TeleComputing Sweden Aktiebolag och Tieto Sweden AB.

3 *Testimony Before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, House of Representatives: INFORMATION SECURITY – Additional Guidance Needed to Address Cloud Computing Concerns*. Statement of Gregory C. Wilshusen, Director, Information Security Issues, Thursday, October 6, 2011 (www.gao.gov/new.items/d12130t.pdf).

digitaliseringens möjligheter.[4] Genom rationellt resursutnyttjande och genom olika typer av e-tjänster ska Sverige gå i täten för att öka den statliga och kommunala förvaltningens effektivitet.

Vid sidan om den tekniska utvecklingen har det även skett stora förändringar i samhällets struktur. Verksamhet som tidigare utförts av offentliga aktörer, levereras i allt högre grad av privata organisationer på uppdrag av offentliga beställare. Denna rollförändring har förändrat den offentliga förvaltningen, både i den enskilda organisationen och på nationell nivå.

I sin roll som kund reglerar den offentliga aktören ansvarsförhållanden kring säkerhet med leverantörer genom avtal. De offentliga organisationerna måste därför vara aktiva avtalsparter som förmår inkludera säkerhetsaspekter i sina upphandlingsprocesser – från riskanalys till konkreta krav. För verksamheter som kan betraktas som samhällsviktiga är detta av särskild betydelse eftersom kraven även kan komma att omfatta leveranser som påverkar samhällets skydd och beredskap.

2.2 Det svenska krishanteringssystemet

Svensk krishantering bygger på samverkan. Alla aktörer måste vid händelse av en kris kunna agera tillsammans och samverka kring beslut och insatser. Det gäller oavsett region eller affärsområde: privat näringsliv, polis, räddningstjänst, beslutsfattare inom kommun, länsstyrelse, centrala myndigheter eller statsledning. Krishanteringssystemet inkluderar sektorsansvar, områdesansvar och verksamhetsansvar, indelat på kommunal nivå (lokalt), på länsstyrelse- och landstingsnivå (regionalt) och på central myndighets- och regeringsnivå (nationell nivå).[5]

En kris hanteras till en början i dess omedelbara närhet, samtidigt som det finns resurser beredda på regional och nationell nivå om händelserna blir för omfattande för att hantera på lokal nivå. Detta innebär att kommunernas verksamhet är grunden för i stort sett all hantering av kriser. Under en kris ska länsstyrelsen i egenskap av geografiskt områdesansvarig på regional nivå stödja kommunen när det gäller samverkan mellan myndigheter, kommuner och andra aktörer. Länsstyrelsens stöd innebär inte någon förändring av övriga aktörers ansvar för att hantera krisen.

Tre viktiga grundprinciper i det svenska krishanteringssystemet är de så kallade ansvars-, likhets- och närhetsprinciperna.

I ansvarsprincipen, som innebär att den som bedriver verksamhet under normala förhållanden har motsvarande ansvar även under krissituationer, ingår även att initiera och bedriva samverkan.[6]

Likhetsprincipen innebär att verksamheten under en kris ska fungera på liknande sätt som vid normala förhållanden – så långt det är möjligt.

---

4 *It i människans tjänst – en digital agenda för Sverige*, Näringsdepartementet 2011, dnr 2011/342/ITP, samt regeringens budgetproposition för 2012 (prop 2011/12:01).

5 Se exempelvis https://www.msb.se/sv/Forebyggande/Krisberedskapssystemet/

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

Verksamheten ska också, om det är möjligt, skötas på samma plats som under normala förhållanden.

Med närhetsprincipen menas att en kris ska hanteras där den inträffar och av dem som är närmast berörda och ansvariga. Först om de lokala resurserna inte räcker till blir det aktuellt med regionala och statliga insatser.

3. Händelseförlopp och konsekvenser i samhället

3.1 Övergripande beskrivning

Fredagen den 25 november inträffar ett maskinvarufel hos it-driftleverantören Tieto. En central del av ett större datalagringssystem vid en anläggning i Stockholm drabbas av ett akut driftstopp. Först faller en viktig nyckel-komponent i systemet bort. I det momentet finns det fortfarande möjlighet att falla tillbaka på ett reservsystem, som står i ständig beredskap att ta över. Men efter en kort stund upphör även detta system att fungera. Därmed fungerar inte datalagringen längre för de anslutna serversystemen.[7]

Exakt vad som hände har inte offentliggjorts av Tieto, men på mycket kort tid upphör datalagringen att fungera för ett stort antal servrar. Driftstörningen drabbar runt 50 av Tietos kunder, såväl företag som myndigheter och kommuner. Exakt vilka kunder som berörs av driftstörningen är fortfarande okänt utanför Tieto. Men till de drabbade hör Apoteket AB, Apotekens Service AB, Bilprovningen, SBAB, Vetenskapsrådet, Nacka kommun, Sollentuna kommun och Stockholms stad. För några organisationer upphör it-stödet nästan helt att fungera, medan andra får uppleva hur vissa specifika tjänster blir utslagna. Flera tjänsteleverantörer verkar dessutom ha legat anslutna till lagringssystemet, företag som levererar webbaserade verktyg för exempelvis administration, resehantering och liknande. Från flera kommuner i landet rapporteras det om hur bland annat delar av ekonomihanteringen och hanteringen av tjänstepensioner inte fungerar efter driftstörningen hos Tieto.

Det är svårt att ge någon exakt bild av haveriets direkta konsekvenser, hur många it-tjänster eller servrar som slogs ut. Det går emellertid att få en grov uppfattning av omfattningen baserad på de outsourcingkontrakt Tieto skrivit med några av de drabbade organisationerna. En av de drabbade kommunerna, Sollentuna, har till exempel överfört 14 anställda och driften av runt 130 servrar till Tieto. Nacka har överfört it-drift samt 4 anställda till Tieto. Från Bilprovningen har it-drift samt 15 anställda överförts till Tieto, och från ett drabbat större logistikföretag 10 personer. Driftstörningen påverkade runt 50 kunder. Följden blev att ett stort antal servrar, eller så kallade virtuella servrar, på kort tid slogs ut när lagringssystemet havererade.

Det är dessutom inte enbart de system som Tieto sköter driften av som drabbats. Företaget säljer även automatiserad driftövervakning av kundservrar. Flera av Tietos kunder märker följaktligen snabbt att de inte längre har någon kontroll över tillståndet hos sina egna servrar. Detta innebär att de snabbt behöver övergå till manuell övervakning, vilket resulterar i betydande merarbete.

7 http://www.tieto.se/press/driftsstorningar/fragor-och-svar

Åtminstone två kommuner i Stockholms län, Haninge och Södertälje, drabbas av att driftövervakningen faller bort när Tietos lagringssystem drabbas av driftstopp. Från att tidigare ha haft närmast momentan övervakning av sina system får dessa kunder i all hast ordna fram manuella kontroller, som av naturliga skäl får ske med relativt glesa intervall. För en av kommunerna resulterar detta i ett omfattande följdfel. Under avbrottsperioden upphör ett antal funktioner kopplade till kommunens centrala e-postsystem att fungera, och den manuella övervakningen förmår inte upptäcka detta i tid. Resultatet blir att dessa funktioner slås ut under flera dygn.

3.2 Det tekniska felet

Det tekniska felet hos Tieto drabbade en central komponent av datalagrings-utrustningen. Det innebar att i stort sett all datalagring hos de berörda kunderna på kort tid upphörde att fungera. Tieto har inte offentliggjort några mer detaljerade uppgifter om det maskinvarufel som var den direkta felorsaken, utöver att det handlade om en central del av ett lagringssystem. Felet inträffade under fredagen den 25 november. Det direkta felet tog två dygn att åtgärda, vilket innebär att utrustningen hos leverantören fungerade igen redan under söndagen den 27 november.

Kundernas information, alltså de data som lagrats i lagringssystemet, kunde emellertid inte återställas enbart genom att byta ut en komponent i den tekniska utrustningen. Maskinvarufelet utlöste nämligen en kedja av incidenter som resulterade i en komplex och tidsödande återställningsprocess. Därför dröjde det betydligt längre innan kunderna kunde återställa sina lagrade data i samma skick som under fredagen, innan maskinvarufelet inträffade.

Det är mycket stora datamängder som oupphörligen sparas till och hämtas från ett datalagringssystem av det slag Tieto driftar. Det rör sig i själva verket om ett helt eget nätverk i driftcentralen, ett lagringsnät, som ligger direktkopplat till servrarna för att så snabbt och effektivt som möjligt kunna hämta och lagra data, utan att trängas med annan datatrafik.

Genom lagringsnätet passerar alla data till och från databaser, verksamhets-system, onlinetjänster, webbplatser och annat som finns i kundservrarna. Efter en kort mellanlagring stoppas de enligt ett komplicerat schema in på en stor mängd olika hårddiskar, bandminnen och andra lagringsmedia.

Ett fungerande lagringsnät är av central betydelse för servrarnas funktion – och ytterst för alla de tjänster som kunderna låtit Tieto hantera driften för. Så snart lagringsnätet upphör att fungera kommer de anslutna systemen redan på några ögonblick att ha fått föråldrade data i sina lagringsutrymmen. Data-lagringen blir korrupt. För att kunna återställa alla data och återgå till normal-drift behövs i det läget tillgång till reservkopior.

3.3 Händelseförlopp i samhället

Följande avsnitt bygger på den information som MSB inhämtat i samband med driftstörningen hos Tieto. Sammanställningen över händelseförloppet gör inte anspråk på att vara heltäckande.

3.3.1 Driftstörningen upptäcks på en fredag

Driftstörningen hos Tieto inträffar på fredag eftermiddag, och det står snabbt klart för driftleverantören att någonting mycket allvarligt har inträffat. Den interna krisorganisationen hos Tieto aktiveras och ger sig i kast med uppgiften att åtgärda det direkta felet. Eftersom många av kunderna har sin huvudverksamhet förlagd till vardagar finns det en möjlighet för Tieto att i viss mån begränsa skadan genom att hinna åtgärda den direkta felorsaken under helgen, något företaget också lyckas med.

Åtskilliga av Tietos kunder har dock direkt fått allvarliga problem, eftersom verksamheten hos dem pågår ständigt. Redan under helgen börjar driftstörningen hos Tieto också uppmärksammas i rikspressen, främst på grund av att runt 350 av Apoteket AB:s apotek över hela landet plötsligt inte har kontakt med sina it-system längre och därför inte kan lämna ut receptbelagda mediciner enligt normala rutiner. [8]

Det är hittills inte känt om den utslagna recepthanteringen resulterat i några patientskador. Men olägenheten upplevs på många håll som stor, speciellt på sjukhusapoteken och i glesbygden. Vissa apotek börjar i detta ansträngda läge hantera sina recept manuellt, medan andra ganska snabbt kan återinstallera ett äldre it-system vilket resulterar i att hanteringen hjälpligt kan upprätthållas.

En närliggande verksamhet, Apotekens Service AB, drabbas också av driftstoppet hos Tieto. Företagets externa webbplats ligger nere under helgen och därefter under hela den påföljande veckan. Webbplatsen är en viktig informationskälla för vård- och omsorgssektorn i Sverige. Den innehåller bland annat läkemedelsinformation, kontaktuppgifter och information om driftstörningar. Företagets övriga tjänster kan dock upprätthållas på grund av att beslut tidigare fattats om att verksamhetskritiska tjänster ska hanteras i egna redundanta miljöer.

Även det statligt ägda bostadsfinansieringsföretaget SBAB drabbas av driftstoppet. Här är händelsen egentligen kritisk redan på fredagen som råkar infalla den 25:e, det datum i månaden då många får ut sin lön. Inom bank- och finanssektorn betraktas det av tradition som en extra känslig tidpunkt, då störningar kan få stora konsekvenser. Här lyckas företaget emellertid begränsa skadan och kundernas tillgång till likvida medel påverkas därför inte i någon mer betydande omfattning. Däremot får driftstörningen stor effekt på SBAB:s låneverksamhet, som inte är i normal drift igen förrän påföljande onsdag.

En annan finansiell aktör får också problem. Bland annat drabbas dess kundtjänst av störningen, produktionen av kreditkort stoppas tillfälligt och inbetalningar till kundkonton går temporärt inte att se. Här räddas företaget emellertid av sina reservkopior och kan relativt snabbt återgå till normal verksamhet.

Ett stort logistikföretag tillhör också kretsen av drabbade. Företaget har stora leveranskontrakt med offentlig sektor, och driftstoppet gör det bland annat

8 *Vissa av Apoteket AB:s apotek har för närvarande problem att lämna ut receptförskrivna läkemedel*, 2011-11-27, http://www.mynewsdesk.com/se/pressroom/apoteket_ab/pressrelease/view/vissa-av-apoteket-ab-s-apotek-har-foer-naervarande-problem-att-laemna-ut-receptfoerskrivna-laekemedel-709363

omöjligt att kommunicera med kunderna via e-post eller via den interna respektive externa webbplatsen. Här anar företaget tidigt vad som kan komma att ske om driftproblemen visar sig vara långvariga, och företaget sammankallar därför snabbt sin krisgrupp. En omständighet som underlättar är att företaget varit med om en större krissituation tidigare, och har en framtagen kontinuitetsplan, vilket kraftigt underlättar arbetet.

Det dröjer till söndagseftermiddagen den 27 november innan Tieto offentliggör att företaget har driftproblem till följd av ett maskinvarufel. Tidigt under söndagskvällen rapporterar också Nacka Värmdö Posten att Nacka kommun har fått problem med sin hemsida till följd av problem hos kommunens it-leverantör. Detta är bara en liten föraning av vad som kommer att märkas ett halvt dygn senare, på måndag morgon, när människor runt omkring i landet återvänder till sina arbetsplatser och upptäcker att it-tjänsterna de använde så sent som under fredagen inte fungerar längre.

3.3.2 Första vardagen efter kraschen

Redan tidigt på måndagen den 28 november börjar det stå klart för massmedia och allmänhet hur omfattande konsekvenserna är av driftstoppet. Informationen från driftleverantören själv är emellertid fortfarande knapp, och det är främst genom mängden följdverkningar som driftstoppet börjar bli synligt.

I takt med att måndagen närmat sig har krishanteringen eskalerats hos det stora logistikföretaget. På måndag morgon är situationen kritisk för verksamheten. Utan it-stöd går det inte att sköta verksamheten, och som det ser ut på måndagen går det inte ens att nå det stora antalet anställda i koncernen med information. Som en nödlösning tar företaget i det läget till sms-utskick, vilket tillfälligt räddar situationen. Det väljer också att prioritera sina kunder inom den offentliga sektorn, och drar istället ner på annan verksamhet. Prioriteringen sker utifrån vad företagsledningen anser som samhällsviktig verksamhet och den uppger att affärsmässiga hänsyn har fått stå tillbaka med tanke på allvaret i situationen.

Hos statliga Bilprovningen är det totalstopp i it-systemet på måndagen.[9] [10] Bilprovningen kontrollbesiktigar runt 5,5 miljoner fordon om året, vilket innebär att det varje dag rullar in runt 20 000 fordon på företagets kontrollstationer. Här finns det plötsligt inget it-stöd längre. Bara telefonerna fungerar. Bilprovarna vid 180 kontrollstationer över hela landet får snabbt övergå till helt manuell registrering av provresultaten, med papper och penna i händerna. Det bromsar förstås arbetet och leder efterhand till omfattande merarbete och kostnader när alla data ska efterregistreras.

Hos den statliga myndigheten Vetenskapsrådet tvärstannar den normala verksamheten då myndigheten drabbas av ett nästan totalt driftstopp för it-

9 *Driftstörningar hos Tieto kan skapa förseningar hos Bilprovningen*, 2011-11-28, http://www.bilprovningen.se/externt/bpwebabout.nsf/va_LookupWeb/55A5618F0F97DA2EC125781500389CF9!OpenDocument&m=0

10 *Driftstörningar hos Tieto påverkar möjligheten att registreringsbesikta fordon*, 2011-11-28, http://www.bilprovningen.se/externt/bpwebabout.nsf/va_LookupWeb/55A5618F0F97DA2EC125781500389CF9!OpenDocument&m=0

stödet. Ekonomisystemet fungerar inte längre, e-posten är borta, myndighetens webbtjänster går inte att nå. Ansökningssystemet, det ärendehanteringssystem som hanterar forskningsansökningar och granskningar, är inte heller tillgängligt. För att överhuvudtaget kunna kommunicera med omvärlden får Vetenskapsrådet istället inrätta en tillfällig blogg på internet. [11]

3.3.3 Kommunen får ta till Twitter

I en av Stockholms kranskommuner, Nacka kommun, drabbas verksamheten av likartade problem. [12] Samtliga kommunala aktiviteter och verksamheter påverkas av driftstoppet hos Tieto, från ekonomi till utbildning och kommunal vård och omsorg. Webbplatsen försvinner också, och det går inte att kommunicera med e-post i kommunen. Allt ligger hos it-driftleverantören. Kommunikationen med allmänheten, med landstinget, med varu- och tjänsteleverantörer är borta. Kommunen tvingas i det läget ta till sociala medier som Twitter och Facebook för att på något sätt hantera kommunikationen med sina medborgare och sina samarbetspartner.

Senare under måndagen börjar massmedia på allvar uppmärksamma vad som hänt, och Nacka kommuns socialtjänst tvingas bland annat meddela att det uppstått förseningar i utbetalningen av försörjningsstöd till följd av drift-stoppet. Kommunen får temporärt övergå till manuella utbetalningar.

Under måndagen har massmedia också börjat spekulera i hur stora störningens konsekvenser är – och vilka som drabbats. Tidningen Ny Teknik publicerar redan på förmiddagen en lång lista över myndigheter som är kunder till Tieto och därför kan vara drabbade, en lista som även fångas upp av andra medier.[13] Uppgifterna är emellertid inte särskilt träffsäkra. De har hämtats från en webbplats som publicerar uppgifter från statlig fakturahantering och begränsar sig inte till it-driftkunder. MSB finns till exempel listat som kund, eftersom myndigheten köpt dokumentmallar för projektledning från företaget.

Strax norr om Stockholm, i Sollentuna kommun, har socialkontoret fått samma problem som i Nacka. Även här tvingas kommunen betala ut ekonomiskt bistånd manuellt.[14] Senare står det klart att åtminstone en kommun till, Kalmar, haft samma problem och fått betala ut försörjningsstöd manuellt. [15]

I Sollentuna kommun blir det inte totalstopp i verksamheten, men ett stort antal kommunala tjänster går inte att nå längre. Bland annat får de kommunala skolorna stora problem.[16] Där fungerar inte e-posten längre, och det går inte att logga in och komma åt pågående arbeten. Runt 6 000 elever och lärare får

11 http://vetenskapsradet.wordpress.com/2011/12/05/vara-it-system-fungerar-igen-men-e-post-och-ansokningar-kan-vara-drabbade/, postningar 28, 29, 30 november samt 1 och 5 december.

12 *Driftstörningarna i Nacka kommuns IT-system*, 2011-12-12, http://www.nacka.se/web/Nyheter/Sidor/Nackasefungerarigen.aspx

13 *Stort mörkertal när Tieto havererar*, Ny Teknik 2011-11-28, http://www.nyteknik.se/nyheter/it_telekom/allmant/article3355166.ece

14 *Problem med utbetalningar av ekonomiskt bistånd*, 2011-11-30, http://www.sollentuna.se/Nyheter/Nyheter/Omsorg--socialt-stod/Asa-Hinndal-Anrin/

15 *Dataproblem stoppar betalningar*, Sveriges Radio, 2011-11-29, http://sverigesradio.se/sida/artikel.aspx?programid=86&artikel=4828825

16 *IT-störningar påverkar skolan*, 2011-11-30, http://www.sollentuna.se/Nyheter/Nyheter/NYHET---Barn--utbildning/IT-strorningar-paverkar-skolan/

plocka fram läroböcker, papper och pennor istället. Sollentunas skolverksamhet är omfattande, i kommunen ligger bland annat en av Sverige största gymnasieskolor.

Stora delar av den kommunala administrationen i Sollentuna berörs när handläggarna plötsligt inte längre kan arbeta med sina ärenden.[17] Flera system är beroende av länkar till filsystemet och fungerar därför inte. Vid sidan av utbetalningsproblemen kan socialkontoret inte nå sin journalföring och alla ansökningar om ekonomiskt bistånd får därför hanteras manuellt. Dokument och datafiler i administrationen går inte att nå, vilket skapar förseningar i handläggning av bygglov, ärenden hos överförmyndaren, handläggning av livsmedelsärenden och miljö- och hälsoskyddsärenden.[18] Protokoll från fullmäktige och kommunstyrelse försenas, det går inte att utfärda parkeringstillstånd till funktionshindrade[19], månadsbokslut försenas och idrottsföreningar kan inte boka lokaler. Dessutom leder driftstoppet till att inpasseringen till lokaler som ägs av kommunen får skötas manuellt.

Inte heller Stockholms stad undgår att drabbas av driftstoppet hos Tieto. Här påverkar driftstörningen framför allt stadens webbplats stockholm.se samt stadens interna intranät. Stockholm.se är visserligen åtkomlig, men dras med störningar. Intranätet ligger tidvis helt nere. Stadens interna användare kan emellertid arbeta som vanligt under störningen, och intranätet betraktas inte av kommunen som verksamhetskritiskt.

Stockholms skolwebb, en tjänst som används för skolresultat, frånvarorapportering och kontakt med vårdnadshavare, ligger helt nere under avbrottet. Det kommer i drift igen först på torsdagen, den 1 december. Rekryteringsverktyget ”Jobb i stan” drabbas och ligger nere fram till kvällen den 30 november. Under tiden får ansökningshandlingar sändas in via alternativa vägar.

3.3.4 Problem på flera håll i landet

Störningarna är emellertid inte begränsade till Stockholm och dess kranskommuner. På flera andra håll i landet rapporteras det om problem till följd av driftstoppet. I Flen försvinner kommunens självservicesystem, som hanterar personalens tidrapportering. Det leder till ökad belastning på personalavdelningen när allt får läggas in manuellt istället och i vissa fall dubbelrapporteras. Dessutom visar det sig efterhand att vissa uppgifter försvunnit helt från systemet. I Vingåker blir lönekontoret nedringt av användare sedan kommunens lönesystem slutat fungera, vilket innebär att en ansluten självservicefunktion också faller bort.

I Skinnskatteberg i Bergslagen går det inte längre att skicka bankgirofiler. Längre söderut i landet får Kalmar kommun problem med ekonomisystemet och indirekt även med lönesystemet och socialsystemet. Betalningen av löner

17 *Stora IT-problem i Sollentuna kommun*, 2011-11-30, http://www.sollentuna.se/Nyheter/Nyheter/NYHET---Om-kommunen/Stora-IT-problem-i-Sollentuna-kommun/

18 *IT-driftstörningar på miljö- och byggnadskontoret*, 2011-11-30, http://www.sollentuna.se/Nyheter/Nyheter/NYHET---Bostad--miljo/IT-driftstorningar-pa-miljo--och-byggnadskontoret/

19 *Problem med tillverkning av P-tillstånd*, 2011-11-30, http://www.sollentuna.se/Nyheter/Nyheter/Trafik--teknik/Problem-med-tillverkning-av-P-tillstand/

och försörjningsstöd försenas, leverantörer får inte betalt i tid och det skickas ut felaktiga betalningspåminnelser.

I Nyköpings kommun blir det tvärstopp i handläggningen av tjänstepensioner under fyra, fem dagar till följd av driftstoppet. Störningen drabbar emellertid enbart tjänstepensionshandläggningen, och konsekvenser betraktas därför som små. Men Nyköping är inte ensamt om att få pensionsproblem. Längre söderut i Sverige rapporterar också ett landsting om liknande störningar i samma tjänst.

Driftstörningen påverkar även tjänsten Nationell Patientöversikt (NPÖ) hos den svenska vård- och omsorgssektorns gemensamma it-infrastrukturföretag Inera AB. NPÖ är det samlade vårdinformationssystem med journalfunktioner som planerats för sjukvården i Sverige och som successivt håller på att tas i drift. Här blir den testmiljö och det demonstrationssystem som finns för NPÖ plötsligt otillgängliga. Detta påverkar enligt Inera AB främst de vårdgivare som just står i begrepp att införa systemet och utbildar personal i att hantera det. Inera AB uppger att produktionsmiljön för NPÖ inte ska ha påverkats av driftstörningen.

De flesta av de drabbade kunderna tycks ha problem under hela helgen den 26–27 november och under den påföljande måndagen den 28 november, trots att det direkta felet är åtgärdat redan under söndagen. Återställningen av kunddata tar uppenbarligen tid, och att döma av de rapporter i massmedia som börjar publiceras i ett större antal under tisdagen tar det tid för it-driftleverantören att återställa normaldriften för kunderna.

3.3.5 Tjänsterna kommer tillbaka

En av de första stora kunderna som får tillbaka it-stödet i delar av sin verksamhet är Apoteket AB. Det dröjer emellertid till framåt måndag kväll innan runt hälften av de berörda apoteken åter är i drift.[20] [21] I det läget har Tieto lagt ner extra energi på att återställa datadriften hos just Apoteket AB, eftersom dess verksamhet betraktas som samhällsviktig. Det är värt att notera att det inte rör sig om någon bakomliggande prioritering från samhällets sida, utan ett beslut från it-driftleverantören att prioritera apoteken. På tisdagen har Tieto klarat av att återställa driften, och runt onsdag lunch meddelar Apoteket AB att alla apotek är igång igen.[22]

För Bilprovningen sker återställandet senare i veckan. Det som först kan återställas är företagets e-post, som kommer tillbaka under tisdagen – efter närmare fyra dygns bortfall. Andra funktioner dröjer längre. Sammantaget påverkar driftstoppet Bilprovningens rikstäckande verksamhet under hela den påföljande arbetsveckan.

---

20 *IT-problem kvarstår i hälften av Apoteket AB:s butiker*, 2011-11-28,
http://www.mynewsdesk.com/se/pressroom/apoteket_ab/pressrelease/view/it-problem-kvarstaar-i-haelften-av-apoteket-ab-s-butiker-709582

21 *Fortsatta IT-problem i Apoteket AB*, 2011-11-28,
http://www.mynewsdesk.com/se/pressroom/apoteket_ab/pressrelease/view/fortsatta-it-problem-i-apoteket-ab-709698

22 *Nu kan Apotekets kunder återigen hämta ut receptläkemedel på samtliga apotek*, 2011-11-30,
http://www.mynewsdesk.com/se/pressroom/apoteket_ab/pressrelease/view/nu-kan-apotekets-kunder-aaterigen-haemta-ut-receptlaekemedel-paa-samtliga-apotek-710514

En särskild konsekvens av driftstoppet vid Bilprovningen är dessutom att all den automatiska vidarerapportering av godkända kontrollbesiktningar som normalt sker till Transportstyrelsen inte längre fungerar. Trivialt, kan tyckas, men detta fel får snabbt till följd att många fordon automatiskt blir belagda med körförbud, eftersom Bilprovningen inte längre har någon förmåga att rapportera in godkända besiktningsresultat.[23] Först efter tio dygn, på förmiddagen måndagen den 5 december, rapporterar Bilprovningen att bolagets kontrollstationer åter fått fungerande it-stöd, och att kontroll-besiktningar och bokning fungerar som vanligt igen.

Även för Stockholms stad dröjer det nästan en vecka innan verksamheten återgår till det normala. Tieto kontaktar Stockholm stad redan tidigt lördag morgon den 26 november och det förs därefter en tät dialog. På stadens anmodan står Tieto i direktkontakt med berörda systemägare. Under första halvan av den följande arbetsveckan kan systemmiljöerna återställas och Stockholms stad bedömer därför att det inte finns några kvardröjande effekter av driftstörningen efter torsdagen den 1 december.

Hos det stora logistikföretaget är it-driften helt borta i elva dagar och företaget säger sig inte vara helt uppe i normalläge ens två månader efter den inträffade incidenten.

Även för Nacka är situationen komplicerad. Här dröjer det till onsdagen den 30 november innan webbplatsen åter är i drift. Under tiden kommunicerar kommunen med omvärlden på andra sätt. En vecka efter driftstoppet är flera centrala it-system i Nacka fortfarande inte i drift. Handlingar och protokoll är inte tillgängliga, funktioner för kommunal felhantering fungerar inte och inloggning med e-legitimation är inte i drift.

Först i mitten av december kan Nacka kommun meddela att verksamheten till 95 procent kunnat återgå till det normala. Först den 4 januari fungerar alla datasystem igen. Fortfarande pågår dock arbete med att hinna ikapp och kommunen har identifierat dataförluster. Merkostnaden till följd av haveriet uppskattas till minst 7,5 miljoner kronor.[24]

Sollentuna kommun pekar i mitten av december på flera kvardröjande konsekvenser av driftstörningen. Den försenade handläggningen kommer till exempel att vara svår att ta igen. Journaler som förts för hand måste matas in elektroniskt vilket påverkar det dagliga arbetet där andra uppgifter riskerar att inte bli utförda. Projekt har dessutom försenats på ett sätt som kommer att vara svårt att ta igen. Vad värre är; filarean visar sig vara svår att återskapa i exakt samma skick som tidigare, vilket bland annat medför att olika fil-versioner återskapas. Länkar mellan filer bryts, och under tiden efter drift-stoppet pågår ett tidsödande detektivarbete för att förstå vilka länkar som brutits.

23 *Har du fått körförbud på ett fordon med godkänd besiktning?*, 2011-11-29, http://www.transportstyrelsen.se/sv/Nyhetsarkiv/Har-du-fatt-korforbud-pa-ett-fordon-med-godkand-besiktning/

24 *IT-haveriets kostnad hittills: 7,5 miljoner*, Nacka Värmdö Posten, 2012-01-24, http://www.nvp.se/Nacka/Nacka/IT-haveriets-kostnad-hittills-75-miljoner/

3.4 MSB:s arbete med händelsen

3.4.1 Formella utgångspunkter för MSB:s arbete

MSB har ett ansvar för frågor om krisberedskap och krishantering i den utsträckning någon annan myndighet inte har det. Det framgår av förordning (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap:

1 § Myndigheten för samhällsskydd och beredskap har ansvar för frågor om skydd mot olyckor, krisberedskap och civilt försvar, i den utsträckning inte någon annan myndighet har ansvaret. Ansvaret avser åtgärder före, under och efter en olycka eller en kris.
/.../
7 § Myndigheten ska ha förmågan att bistå med stödresurser i samband med allvarliga olyckor och kriser samt stödja samordningen av berörda myndigheters åtgärder vid en kris. Myndigheten ska se till att berörda aktörer vid en kris får tillfälle att
1. samordna krishanteringsåtgärderna,
2. samordna information till allmänhet och media,
3. effektivt använda samhällets samlade resurser och internationella förstärkningsresurser, och
4. samordna stödet till centrala, regionala och lokala organ i fråga om information och lägesbilder.
Myndigheten ska ha förmåga att bistå Regeringskansliet med underlag och information i samband med allvarliga olyckor och kriser.
/.../

Vidare framgår det av myndighetens instruktion att:

11a § Myndigheten ska stödja och samordna arbetet med samhällets informationssäkerhet samt analysera och bedöma omvärldsutvecklingen inom området.
/.../
Myndigheten ska vidare svara för att Sverige har en nationell funktion med uppgift att stödja samhället i arbetet med att förebygga och hantera IT-incidenter. Myndigheten ska i detta arbete
1. agera skyndsamt vid inträffade IT-incidenter genom att sprida information samt vid behov arbeta med samordning av åtgärder och medverka i arbete som krävs för att avhjälpa eller lindra effekter av det inträffade,
/.../

3.4.2 MSB:s aktiviteter

Söndag 27 november

MSB uppmärksammade driftstörningen hos Tieto vid 16-tiden på söndagen den 27 november, då en rapport inkom till myndighetens Tjänsteman i beredskap (TiB) om it-störningar hos Apoteket AB. Berörda chefer och beredskapsfunktioner vid myndigheten informerades om detta inom 15-20 minuter.

Måndag 28 november

Klockan 08:30 den 28 november ringde Nacka kommun och undrade om de kunde lägga ut information från kommunen på Krisinformation.se eftersom deras sida inte var tillgänglig. Krisinformation publicerade nyheten klockan 09:00 med hänvisning till Nacka kommuns Facebooksida. It-störningen togs samtidigt upp vid MSB:s dagliga stabsorientering klockan 09:00 i myndighetens lägescentral. Kort därefter fick Nacka kommun upp en enkel reservsida med den viktigaste informationen och telefonnumren. Efter stabsorienteringen började MSB:s experter på informationssäkerhet att mer aktivt söka efter ytterligare information i frågan. MSB tog bland annat kontakt med Tieto och med några av de organisationer som identifierats som drabbade av driftstörningen.

Även Apoteket hörde av sig och ville ha ut information om störningarna via Krisinformation.se. Redaktionen skapade en särskild sida om störningarna med hänvisningar till vart allmänheten kunde vända sig (även i Krisinformations kanaler på Facebook och Twitter). Detta resulterade i många besök och frågor på hemsidan. Krisinformation rapporterade till TiB om tagna kontakter och om frågor från aktörer och allmänhet. MSB TiB rapporterade om händelsen i den dagliga kontakten med Försvarsdepartementets TiB.

Det stod snabbt klart att även Bilprovningen drabbats, att Tieto hade ett stort antal myndigheter bland sina kunder, samt att händelsen kunde få mer omfattande konsekvenser. Det stod också klart att ingen annan offentlig aktör på nationell nivå hade för avsikt att direkt agera. Därför beslöts strax efter klockan 10:00 att den Nationella samverkansfunktionen för informationssäkerhet (NOS) skulle aktiveras.[25] Ett första möte hölls därefter klockan 10:45. Där togs beslut om att upprätta en första informationssäkerhetsrelaterad lägesbild till 12:50 samt att kontakta berörda parter inom de etablerade nätverk MSB har inom informationssäkerhetsområdet. Vid möte klockan 12:50 presenterades en översiktlig lägesbild kompletterade med en redogörelse över de kontakter som tagits.

Under eftermiddagen fortsatte analysarbetet och det hela sammanfattades i en informationssäkerhetsrelaterad lägesbild klockan 16:30, vilken redovisades för berörda. Vid alla dessa möten övervägdes huruvida MSB:s nationella hanterandeplan för allvarliga it-incidenter skulle aktiveras, vilket inte bedömdes nödvändigt, se vidare avsnitt 4.3.

Tisdag 29 november

Under tisdagen den 29 november genomfördes först en information om läget vid stabsorienteringen och därefter följde formella möten i NOS klockan 11:50 och 15:00. Under tisdagen kontaktades också MSB av flera massmedier som hade frågor om händelserna och om MSB:s roll. En kort information kring detta publicerades på MSB:s externa webbplats vid lunchtid på tisdagen och ansvarig chef deltog under tisdagen och under resten av veckan i flera intervjuer.

25 NOS är en funktion (samverkansform) som MSB etablerat i syfte att systematisk kunna arbeta med allvarliga it-incidenter. Arbetet är under utveckling och funktionen byggs upp successivt inom MSB och i samverkan med olika aktörer i samhället.

MSB genomförde en konsekvensanalys med bedömningen att inga samhällsviktiga verksamheter var drabbade på ett sådant sätt att samhällets funktionalitet var allvarligt hotad. De samhällsviktiga verksamheter som bedömdes vara berörda var läkemedelsförsörjningen genom störningar hos Apoteket AB, samt utbetalning av försörjningsstöd genom störningar hos vissa kommuner. Uppgifter från berörda aktörer visade på att verksamheterna trots störningarna fungerade på ett godtagbart sätt på grund av att alternativa rutiner infördes. Övriga kända konsekvenser bedömdes inte allvarligt störa samhällets funktionalitet eller befolkningens liv och hälsa. Eftersom det var svårt att få information om vilka av Tietos kunder som var drabbade gjordes även bedömningen att det under de närmsta dagarna skulle kunna inkomma uppgifter om att ytterligare samhällsviktiga verksamheter var drabbade.

Onsdag 30 november till fredag 9 december

Under onsdagen den 30 november färdigställdes en preliminär lägesbedömning till Försvarsdepartementet.

Under onsdagen var MSB TiB i kontakt med Länsstyrelsen i Stockholm, PTS och Finansinspektionen för att stämma av läget inom deras respektive ansvarsområden.

Formella möten inom ramen för arbetet i NOS hölls sedan fredagen den 2 december, måndagen den 5 december, tisdagen den 6 december och fredag den 9 december, varvid fortsatta kontakter redovisades och lägesbilden kunde kompletteras. Vid mötet under fredagen den 9 december fattades beslut om att avaktivera samverkansfunktionen (NOS) och att bedriva fortsatt utredningsarbete i normala arbetsformer.

Det saknades emellertid en helhetsbild av konsekvenserna i samhället, och MSB beslutade därför under måndagen den 5 december att hemställa till myndigheter med särskilt ansvar enligt 15 § förordningen (2006:942) om krisberedskap och höjd beredskap (KBF) att redovisa konsekvenserna av driftstörningen inom sina respektive ansvarsområden. Under måndagen färdigställdes en sådan hemställan och den upprättades och expedierades tisdagen den 6 december, se vidare bilaga 1 och avsnitt 3.5.

3.4.3 Kontakter mellan Tieto och MSB

MSB tog, som nämnts ovan, i ett tidigt skede direkt kontakt med Tieto för att få en bättre uppfattning om läget. Företaget var välvilligt inställt till att träffas, men meddelade redan från början att det på grund av affärssekretess inte kunde gå närmare in på vare sig vilka tekniska problem som lett fram till driftstörningarna eller vilka kunder som blivit drabbade. Ett krav för att delge annan information än vad som lagts ut i pressmeddelande var att både MSB som organisation, och de tjänstemän som tog del av informationen, skulle skriva under ett så kallat Non-disclosure Agreement (sekretessavtal). Avtalen skulle förhindra att informationen spreds utanför den krets som Tieto valt att lämna informationen till. Mellan två privata parter är detta förfarande både etablerat och logiskt, men för en svensk myndighet kolliderar ett fast avtal om att inte sprida viss information vidare med offentlighetsprincipens krav att allmänna uppgifters offentlighet måste prövas vid varje förfrågan om

utlämnande. Avtalen, särskilt de med de inblandade tjänstemännen personligen, skulle kunna stå i strid med den grundlagsskyddade meddelarfriheten. MSB har inte något föreskrivet tillsynsmandat eller motsvarande som ger myndigheten rätt att begära ut information från privata aktörer i denna typ av situationer. MSB är alltså helt beroende av att de privata aktörerna frivilligt lämnar uppgifter.

Problemet fick en tillfällig lösning genom att MSB:s jurister upprättade en ”sekretessförklaring” som beskrev de lagkrav som ställs på en myndighet samt de lagrum som kan användas för att skydda känslig information som inkommit och som potentiellt skulle kunna innebära ekonomisk eller annan skada om de utlämnas, se vidare bilaga 2. Företaget menade att de, under dessa omständigheter, inte kunde lämna ut skriftlig information, men däremot kunde delge information i speciella läsrum i de egna lokalerna.

Tieto erbjöd MSB att som utomstående part ingå i företagets ”haverikommission”, vilken inledde sitt arbete runt årsskiftet. Inledningsvis deltog MSB tillsammans med Läkemedelsverket, Finansinspektionen och Kammarkollegiet, samt ett antal representanter för drabbade och icke-drabbade kunder, i en referensgrupp som Tieto skapat som diskussionspartner för de två konsultföretag som genomför själva haveriutredningen.

MSB:s bedömning är att myndigheten genom sin samverkan med Tieto tagit del av mycket litet information som inte varit allmänt tillgänglig. Detta är en uppfattning som även delas av Kammarkollegiet.

Vid det möte som skedde med referensgruppen till Tietos haverikommission den 16 januari framkom inget nytt i sakfrågan. Tietos representanter meddelade att de inte ville berätta något innan kommissionens arbete blivit slutfört. Efter detta möte meddelade Kammarkollegiet att myndigheten inte avsåg att fortsätta delta i Tietos referensgrupp.

MSB bedömde dock att det fanns anledning att fortsätta bevaka Tietos arbete med haverikommissionen för att om möjligt få ytterligare information och har därför deltagit i ytterligare möten. Det har då framkommit viss information som inte tidigare varit känd kring incidentens förlopp och konsekvenser.

3.5 Information från hemställan enligt KBF

3.5.1 Hemställan till myndigheter enligt KBF

Under veckan som följde direkt efter driftstoppet följde MSB händelseutvecklingen genom öppna källor, egna kontaktnät och kontakt med berörda parter. MSB fick snabbt kontakt med såväl Tieto, som med flera av de drabbade organisationerna som tidigare beskrivits. Det visade sig emellertid svårt att via dessa kanaler nå en samhällsövergripande bild av situationen där det gick att se de mer spridda konsekvenser som driftstoppet gett upphov till.

Av denna anledning upprättades den 6 december en hemställan[26] till flertalet av de myndigheter som är särskilt utpekade i förordningen (2006:942) om krisberedskap och höjd beredskap (KBF) om att till MSB inkomma med en

26 *Hemställan angående information om driftstörningar orsakade av större hårdvarufel hos Tieto*, MSB dnr 2011-6477

lägesrapportering med anledning av driftstörningen hos Tieto. De totalt 36 myndigheter som berördes av hemställan var följande: Datainspektionen, Energimyndigheten, Finansinspektionen, Kustbevakningen, Livsmedelsverket, Läkemedelsverket, Post- och telestyrelsen, Rikspolisstyrelsen, SMHI, Socialstyrelsen, Strålsäkerhetsmyndigheten, Svenska Kraftnät, Trafikverket, Transportstyrelsen och Tullverket, samt landets 21 länsstyrelser.

Hemställan översändes även till Försvarsmakten som inte omfattas av 15 § KBF, för eget beslut om rapportering.

3.5.2 Svar från regionalt ansvariga myndigheter

Länsstyrelsen Gävleborg uppger att en kommun informerat länsstyrelsen om störningar vid ett storkök till följd av driftstörningen. Storköket kunde inte ta emot beställningar av specialkost. En annan kommun hade information om att trafikskolors möjlighet att kommunicera med Trafikverket och Transportstyrelsen hade påverkats.

Länsstyrelsen i Kalmar län noterar att Kalmar kommun fått problem med sitt ekonomisystem, samt att det förekommit problem i länet med Apoteket AB:s recepthantering.

Länsstyrelsen i Norrbotten uppger att Swedavia AB drabbats av störningar i sin telefoni och sina transaktionssystem till följd av driftstörningen.

Länsstyrelsen Södermanlands län rapporterar att tre kommuner haft störningar i sina lönehanteringssystem, men att det inte lett till några konsekvenser för allmänheten.

Länsstyrelsen i Västmanlands län meddelar att Kriminalvården och Skinnskattebergs kommun drabbats till följd av störningen. Kriminalvården fick problem med att få ut receptbelagda mediciner i sin sjukvårdsverksamhet, vilket var kopplat till driftstörningarna hos Apoteket AB. Skinnskattebergs kommun fick även problem på ekonomikontoret.

Vad gäller övriga länsstyrelser uppger exempelvis en länsstyrelse att ”inga aktörer, som Länsstyrelsen känner till, har drabbats av några särskilt allvarliga konsekvenser…”, men anger inte var de icke allvarliga konsekvenserna identifierats. Sex länsstyrelser pekar ut indirekt påverkan inom det geografiska området. En av dessa pekar på problemen hos Apoteket AB och Bilprovningen. En länsstyrelse pekar på att Apoteket och några kommuner drabbats, men namnger inte kommunerna. Fyra länsstyrelser pekar enbart på problemen hos Apoteket. Slutligen uppger en länsstyrelse att den själv inte drabbats, samt anger uttryckligen att den inte bedömt situationen i regionen utan enbart den egna verksamheten.

Två länsstyrelser inkom inte med något svar på MSB:s hemställan om lägesrapportering.

3.5.3 Svar från övriga myndigheter utpekade i KBF

Läkemedelsverket rapporterade att en större apotekskedja (Apoteket AB) drabbats, vilken täcker ungefär en tredjedel av landets apotek. Receptexpeditionen slogs ut. Berörda personer vid Läkemedelsverket informerades

samma dag som störningen inträffade och har sedermera fått information om att totalstoppet åtgärdats. Kvardröjande negativa effekter går för närvarande inte att bedöma.

Post- och telestyrelsen (PTS) har efter kontakt med operatörer inte noterat några störningar på allmänt tillgängliga elektroniska kommunikationsnät eller tjänster i Sverige. Däremot drabbades PTS i mindre omfattning genom att en tjänst till allmänheten, ”Testa datorn”, under en kortare period inte var tillgänglig. Driften av denna tjänst sköts för närvarande av Tieto.

Socialstyrelsen angav att Apoteket AB drabbats av driftstörningen.

Strålsäkerhetsmyndigheten lämnade en utförlig rapport där myndigheten rapporterade att inga egna, verksamhetskritiska system drabbats. Vid de kärntekniska anläggningarna påverkades inte heller några verksamhetskritiska system. Däremot påverkades ett system för hantering av leverantörsfakturor vid ett av kärnkraftverkens ägarbolag.

Kustbevakningen, Rikspolisstyrelsen, Datainspektionen, Svenska Kraftnät, Försvarsmakten, Livsmedelsverket och Energimyndigheten rapporterar inga kända konsekvenser av incidenten inom sina respektive ansvarsområden.

Fem av de särskilt utpekade myndigheterna inkom inte med något formellt svar på MSB:s hemställan om lägesrapportering.

4. Analys

4.1 Ny teknik och affärslogik skapar nya möjligheter och samhällsrisker

Driftstörningen hos Tieto understryker med stor tydlighet ett redan känt förhållande, nämligen att ny teknik har skapat nya möjligheter och risker på samhällsnivå. Ny teknik och nya affärslösningar har möjliggjort en koncentration av information, tjänster, kommunikation och it-drift i samhället. Inom offentlig sektor har trenden mot koncentration förstärkts genom en rad initiativ såsom E-delegationens arbete[27], Nationell E-hälsa[28], förslaget om gemensam servicemyndighet[29], samt de ramavtal som Kammarkollegiet sluter med ett antal stora aktörer[30].

Den ökade koncentrationen, tillsammans med nya driftsformer och ökad integration skapar en ny kategori av sårbarheter, där tekniska fel på mycket kort tid kan slå ut en rad olika samhällsverksamheter. Det leder också till att det är mycket svårt för enskilda organisationer att överblicka de it-resurser som de är beroende av för sin verksamhet, något som är särskilt allvarligt för verksamheter som kan betraktas som samhällsviktiga.

Diskussionen kring informationssäkerhet har på senare tid varit fokuserad på antagonistiska hot, exempelvis hackerintrång, cyberkriminalitet eller säkerhetspolitiskt motiverade it-angrepp. Dessa fenomen representerar en viktig dimension av informationssäkerhetsproblematiken men utgör samtidigt enbart en delmängd av det övergripande säkerhetsproblemet. Driftstörningar orsakade av tekniska fel, naturhändelser eller mänskliga handhavandefel är inte lika spektakulära som de avsiktliga angreppen, men kan orsaka stora samhällsproblem. Den aktuella driftstörningen bekräftar den bilden. Det bör också understrykas att effekterna vad gäller krishanteringen i samhället i hög grad skulle vara desamma om incidenten haft uppsåtligt ursprung, det vill säga varit resultatet av brottslig aktivitet.

Driftstörningen hos Tieto berodde på ett tekniskt problem, som inte beskrivs i detalj denna rapport. I detta sammanhang är de tekniska detaljerna emellertid mindre intressanta. Det räcker med att konstatera att olika typer av tekniska problem även i framtiden kommer att leda till it-incidenter där viktiga delar av samhället påverkas allvarligt.

---

27 Se till exempel SOU 2009:86 *Strategi för myndigheternas arbete med e-förvaltning*, SOU 2010:20 *Så enkelt som möjligt för så många som möjligt*, samt SOU 2011: 67 *Så enkelt som möjligt för så många som möjligt - vägen till effektivare e-förvaltning*.

28 *Nationell eHälsa– strategin för tillgänglig och säker information inom vård och omsorg*, S2010.020, Socialdepartementet.

29 SOU 2011:38 *Ett myndighetsgemensamt servicecenter*, samt Dir. 2011:99 *Tilläggsdirektiv till Utredningen Ett myndighetsgemensamt servicecenter för en effektivare statlig administration* (Fi 2010:08)

30 Se till exempel Kammarkollegiets upphandlingsdokument *E-förvaltningsstödjande tjänster 2010* och *IT-driftstjänster 2010*.

Regeringen har pekat på hur viktigt det är ”att det offentliga vet hur man upphandlar lösningar för säker informationshantering och därmed sätter standarder för informationssäkerhet”.[31] Säkerhet har identifierats som en förutsättning både för att uppfylla de krav som ställs från medborgare och statsmakt på att utveckla e-förvaltningen, men också för att nå de fördelar som e-tjänster kan innebära för den enskilda myndigheten. En fungerande säkerhet är en av förutsättningarna för förbättrad service och för effektivare förvaltning med möjlighet till ekonomisk rationalisering. En säker e-förvaltning kan innebära fördelar inom näringslivet genom att så kallad e-handel kan underlättas. Säkerhet för it-drift är idag även en förutsättning för en fungerande kommunikation med allmänheten, i vardag och vid kris.

Om den offentliga sektorn ska kunna tillgodogöra sig de fördelar som marknaden erbjuder, måste den kunna kravställa och upphandla på ett adekvat sätt. Informationssäkerhetsaspekter måste få en central roll i kravställningen såväl i samordnade ramavtalsupphandlingar som vid enskilda aktörers upphandlingar. Implicit innebär detta att upphandlingarna behöver föregås av olika former av verksamhetsanalyser.

På detta område finns det fortfarande brister, något som nyligen uppmärksammats av Riksrevisionen.[32] I en granskning av 95 myndigheter konstaterar Riksrevisionen att det stora flertalet inte kan anses ha gjort rimliga prövningar om den egna myndigheten eller någon annan aktör är bäst lämpad att producera den it som organisationen har behov av. Brister i den interna styrningen av it-verksamheten, oförmåga att redovisa sina it-kostnader, otydlig informationsklassificering, krångliga regelverk kring offentlig upphandling och brist på beställarkompetens är några av de problemområden som pekas ut.

Kammarkollegiets upphandlingar är en central komponent för att långsiktigt kunna förena de stora funktionella och ekonomiska fördelar som ligger i den tekniska utvecklingen med god informationssäkerhet. I och med att svensk offentlig sektor har möjlighet att göra i princip alla sina upphandlingar av it-drift och stödjande e-förvaltningstjänster via Kammarkollegiets ramavtal finns här stora möjligheter att bygga in gemensamma säkerhetskrav.[33] Rätt utformade kan ramavtalens säkerhetskrav ge även organisationer med begränsad egen kompetens i säkerhetsfrågor stöd att välja rätt säkerhetsnivå för de tjänster som upphandlas.

Sammanfattningsvis krävs det ytterligare ansträngningar för att den offentliga sektorn ska kunna dra maximal nytta av digitaliseringens möjligheter. Vid outsourcing måste de förebyggande åtgärderna finnas med redan i upphandlingsfasen, eftersom det vanligen är både komplicerat och mer kostnadskrävande att komplettera med sådana åtgärder i ett senare skede. Detta kräver emellertid både en medvetenhet om riskerna i den egna verksamheten och en vilja att hantera dem. Först då går det att fatta väl

---

31 *It i människans tjänst – en digital agenda för Sverige*, dnr 2011/342/ITP, Näringsdepartementet

32 *IT inom statsförvaltningen – har myndigheterna på ett rimligt sätt prövat frågan om outsourcing bidrar till ökad* effektivitet?, RiR 2011:4, Riksrevisionen

33 Jämför även med den diskussion om gemensam kravställning och utvecklad upphandling som förs i rapporten *Tillgänglig och skyddad kommunikationsinfrastruktur för offentlig sektor, Svar på regeringens uppdrag till Myndigheten för samhällsskydd och beredskap (Fö2010/701/SSK, Regeringsbeslut 12, 2010-04-14)*, Dnr. 2010-6304, MSB

avvägda beslut om vilka risker som kan accepteras – och vilka som måste undvikas.

4.2 Nationell lägesbild vid allvarliga it-incidenter

En krissituation kännetecknas av såväl många informationskällor som många informationsmottagare. Lägesinformation utgör en nödvändig förutsättning för att alla inblandade aktörer ska förstå situationen och kunna hantera den. Ska aktörerna samordnat kunna planera åtgärder och fördela resurser måste lägesinformationen dessutom delas mellan aktörerna för att åstadkomma en gemensam lägesuppfattning. Samordnat handlande kräver med andra ord en gemensam uppfattning om det aktuella läget så att aktörerna tillsammans kan gå vidare mot ett koordinerat beslutsfattande. Det kan till exempel gälla hur aktörerna ska lämna samlad information till allmänheten eller vilken handlingslinje de ska välja.

Det är av stor vikt att snabbt kunna detektera och presentera händelseförloppet vid allvarliga it-incidenter. Om den informationssäkerhetsrelaterade lägesbilden visar att många aktörer i samhället samtidigt är drabbade ställer det krav på ett annat agerande än om endast enstaka aktörer har drabbats. I princip alla kriser har i dag en it-dimension och MSB sammanfogar därför den informationssäkerhetsrelaterade lägesbilden med den övergripande nationella lägesbilden som myndigheten har ansvar för att upprätthålla och rapportera till regeringen.[34]

Den inträffade incidenten visade att den nödvändiga informationsinsamlingen som krävs för att skapa en informationssäkerhetsrelaterad lägesbild, och i förlängningen en nationell lägesbild, var svår att genomföra. Avgörande för att kunna sprida information om it-incidenter, samt samordna och medverka i arbetet för att avhjälpa eller lindra effekterna av it-incidenter, är att MSB har tillgång till aktuell och relevant information från olika aktörer. Information av hög kvalitet är också nödvändig för att kunna utvärdera och dra strategiska slutsatser av det inträffade.

Tieto har sekretessavtal med sina kunder, och kunde på grund av affärssekretess inte lämna ut information om vilka kunder som berördes av it-incidenten. MSB har inte mandat att begära in denna typ av information från privata aktörer och information fick därför sökas via andra källor. Även för sektorsansvariga myndigheter finns inte de rätta instrumenten för att i ett akut skede kunna bilda sig en uppfattning om vad som hänt. För att skapa en bild över vilka aktörer i samhället som drabbats av it-incidenten samlade och bearbetade MSB information från öppna källor, andra myndigheter och egna nätverk. Då detta inte bedömdes som tillräckligt skickades en hemställan, med stöd av 15 § i krisberedskapsförordningen, till länsstyrelser och andra utpekade myndigheter. Enligt hemställan skulle myndigheterna inkomma med information om eventuella effekter av incidenten.

34 Se vidare 7 § förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap.

MSB kan konstatera att eftersom Tietos information om vilka aktörer som drabbats var mycket knapphändig blev det både en stark tidsfördröjning och en stor osäkerhet kring vilka som drabbats och på vilket sätt. Värt att notera är dock att MSB och den aktuella it-driftleverantören redan i ett tidigt skede i den inträffade händelsen hade en dialog. Tieto hävdade, som tidigare påpekats, affärssekretess. För att skapa en lägesbild som på ett heltäckande sätt beskriver samhällskonsekvenserna av incidenten, hade det dock inte räckt att få tillgång till företagets information. För att skapa en sådan bild behövs information från en vid krets av aktörer, både sådana som direkt drabbats av incidenten och sådana som berörts av indirekta följdverkningar.

Den aktuella it-incidenten drabbade aktörer över hela landet inom flera sektorer, vilket gjorde att MSB snabbt behövde vända sig till ett stort antal myndigheter för att få en tillräckligt god överblick. Detta kan jämföras med kriser och incidenter som har geografiskt avgränsade effekter, exempelvis översvämningar och stormar.

En viktig slutsats från de svar som inkommit på MSB:s hemställan är att i många fall saknar länsstyrelser och utpekade myndigheter rutiner för att hantera denna typ av informationsinhämtning i sin egen region eller sektor. I ett flertal fall rapporterades endast sådant som framkommit via massmedia, det vill säga ingen egen inhämtad information. Några aktörer misstolkade även frågan och svarade bara för den egna organisationen – inte sektorn eller regionen.

Under driftstörningen visade sig de informella kontakterna (nätverk) vara mycket värdefulla. Det är dock viktigt att arbeta vidare med de etablerade nätverk för informationsdelning som finns i samhället när det gäller informationssäkerhet. De informella nätverken bygger i hög grad på förtroende mellan nyckelpersoner. Sjukdom eller annan bortavaro kan därför allvarligt minska förutsättningarna att dela information i ett kritiskt skede. Det är MSB:s bedömning att den formella processen för informationsinhämtning, exempelvis efter hemställan enligt förordningen om krisberedskap, behöver fortsätta utvecklas när det gäller it-incidenter.

Vid en it-incident kan konsekvenserna beröra olika myndigheters områden och sekretessreglerna varierar mellan områdena. Det är därför svårt att omedelbart se vilken typ av information som går att dela mellan olika myndigheter. Den information som en myndighet med tillsynsansvar inhämtar kan exempelvis vara svår att dela i annat syfte. Någon myndighet har även påpekat att en sådan delning av information kan skada förtroenderelationen med verksamheter som tillsynen gäller. Kammarkollegiet var inte förberett på förfrågningar om vilka offentliga verksamheter som nyttjar ramavtalstjänster hos en viss leverantör. Viss information finns dock redan tillgänglig hos Kammarkollegiet och genom exempelvis utökade krav på statistik från leverantörerna skulle myndigheten kunna skapa uppdaterade listor över aktuella kunder på olika avtal.

Massmedia och internet, speciellt vissa internetforum, är snabba nyhetskanaler. Det förekom dock spekulationer och en hel del felaktigheter i samband med rapporteringen av störningen som drabbade Tieto. Detta är krisdrivande i sig själv eftersom många organisationer har dessa kanaler som

enda källa. En möjlighet är att ytterligare använda Krisinformation.se för spridning av bekräftad och samordnad information. Många myndigheter, kommuner och andra aktörer hämtar information från webbplatsen, inklusive de sociala mediekanalerna som Krisinformation.se har, och som fungerar som snabba informationsspridare. Centrala aktörer bör i ökad omfattning ha tillgång till egen information. I de fall olika aktörers lägesbild endast bygger på rapporteringar via massmedier är källkritik extra viktigt.

Sammanfattningsvis kan det konstateras att MSB hade svårigheter att snabbt skapa en heltäckande bild över hur it-incidenten påverkade det svenska samhället. Ingen aktör har idag någon sådan fullständig bild av samhällskonsekvenserna. Den förmåga som finns i samhället när det gäller lägesuppfattning rör främst sådana konsekvenser som allvarligt skadar samhällets funktionalitet. Även där är viss information svår att få tillgång till. Slutsatsen är att det finns formella begränsningar för MSB och andra myndigheter att få tillgång till relevant information.

4.3 Samlad konsekvens- och hanterandebedömning vid allvarliga it-incidenter

Driftstörningen ledde till omfattande skadeverkningar hos ett stort antal organisationer i samhället, främst vad gäller tillgängligheten till olika it-baserade tjänster. Massmedia har huvudsakligen lyft fram hur driftstörningen påverkat tillgängligheten i Tietos kunders tjänster. Det måste dock understrykas att det även finns andra konsekvenser som inte är fullt klarlagda, och då framförallt den möjliga förlusten av information. Några aktörer har redan meddelat att de förlorat data då de varit tvungna att ställa om sina system till tidigare versioner, andra befarar att de gjort dataförluster men har ingen möjlighet att verifiera detta. MSB:s bedömning är att driftstörningen hade kunnat få ännu allvarligare konsekvenser i samhället, exempelvis om den inträffat tidigare under månaden och i större omfattning påverkat utbetalningar av löner och andra transfereringar. Störningen hade även kunnat drabba ytterligare verksamheter och därigenom lett till värre konsekvenser, om exempelvis Apotekens Service AB:s distributionssystem hade drabbats.

Driftstörningen ledde inte till att MSB aktiverade den nationella hanterandeplanen för allvarliga it-incidenter.[35] I planen finns kriterier för vad som utgör en allvarlig it-incident. Där ställs bland annat krav på att händelsen ska kräva snabba och samordnade insatser på nationell nivå. Någon sådan situation förelåg inte enligt MSB:s bedömning. Att MSB inte aktiverade hanterandeplanen betyder dock inte att händelsen inte betraktades som ”allvarlig”. Det betyder heller inte att samhällsviktiga verksamheter inte drabbades. Jämför med diskussionen ovan. När det gäller att avgöra om incidenten var allvarlig – eller kanske till och med en ”kris” – är det viktigt att skilja på samhällets perspektiv och det perspektiv som enskilda individer och organisationer har. Driftstörningen har med säkerhet gett upphov till stora negativa konsekvenser för enskilda personer och organisationer. I det

35 *Hantering av allvarliga IT-incidenter: Nationell hanterandeplan. Interimistisk version, mars 2011.* Publikationsnummer: MSB328 – november 2011, MSB.

avseendet var driftstörningen mycket allvarlig. I de propositioner och skrivelser från regeringen som på senare år behandlat samhällets krisberedskap finns en definition på kris och utöver det definieras, för kommuner och landsting, begreppet extraordinär händelse i lag.[36] Utifrån detta perspektiv kan inte konsekvenserna av driftstörningen hos Tieto betecknas som en samhällskris, möjligen som en extraordinär händelse för några av de drabbade kommunerna. Jämför även med de diskussioner som förs i MSB:s utvärdering av hur krisberedskapen fungerat under perioder med stora snömängder vintern 2010.[37]

En viktig process i arbetet med att hantera en allvarlig it-incident är en fördjupad analys av konsekvenser och en bedömning av hanteringen, inklusive en bedömning av om det finns behov av specifika resurser. Processen att göra en samlad konsekvens- och hanterandebedömning kan ses som en del av en fördjupad lägesförståelse och kompletterar därför lägesbilden som diskuteras ovan. Det är med andra ord nästa steg i arbetet med att skapa en koordinerad hantering av händelsen och syftar till att skapa goda möjligheter för att berörda aktörer ska kunna samordna åtgärder och insatser. En naturlig del i konsekvens- och hanterandebedömningen är att ge rekommendationer och varningar till representanter för samhällsviktiga verksamheter, men även till allmänheten.

I dag använder många samhällsviktiga verksamheter centraliserade it-tjänster, antingen i kommersiella molntjänster eller i nationella partnermoln. En mer omfattande driftstörning hade enligt MSB:s bedömning kunnat få mycket stora konsekvenser för exempelvis transporter och vård. Det är dock svårt att bedöma konsekvenserna av större it-incidenter på samhällsnivå; dels på grund av de komplexa beroenden som den nya tekniken skapar, dels därför att det inte är entydigt vad som utgör samhällsviktig verksamhet. Centraliserade it-tjänster gör det även svårare för de enskilda aktörerna att överblicka de beroenden som verksamheten har.

Den aktuella driftstörningen visar mycket tydligt att information om att vissa aktörer drabbats av händelsen inte med automatik ger en kunskap om beroenden i samhället och en förståelse för möjliga följdverkningar. För att kunna göra en samlad konsekvens- och hanterandebedömning av en pågående it-incident krävs en samverkan mellan de berörda aktörerna. Privat-offentlig samverkan är i dag en förutsättning för att hantera alla typer av kriser i samhället. Vid mer omfattande it-incidenter är behovet av privat-offentlig samverkan särskilt framträdande beroende på att de offentliga aktörerna i så

36 **Kris** definieras på följande sätt i regeringens skrivelse 2009/10:124 *Samhällets krisberedskap – stärkt samverkan för ökad säkerhet*: ”En händelse som drabbar många människor och stora delar av samhället och som hotar grundläggande värden och funktioner. Kris är ett tillstånd som inte kan hanteras med normala resurser och organisation. En kris är oväntad, utanför det vanliga och vardagliga. Att lösa krisen kräver samordnade åtgärder från flera aktörer”. Denna definition av kris ges även i proposition 2007:08:92 *Stärkt krisberedskap för säkerhets skull.*

Extraordinär händelse definieras i lag (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap: ”En händelse som avviker från det normala, innebär en allvarlig störning eller överhängande risk för en allvarlig störning i viktiga samhällsfunktioner och kräver skyndsamma insatser av en kommun eller ett landsting”.

37 *Perioder med stora snömängder vintern 2009/2010. Redovisning av regeringsuppdrag att analysera och utvärdera hur krisberedskapen fungerat under perioder med stora snömängder vinterna 2010.* Publikationsnummer: MSB 0199-10, MSB

hög grad förlitar sig på privata tjänsteleverantörer. Privata aktörer behöver delta i de processer som finns för samverkan och samordning inom den offentliga sfären. I den utvärdering som genomfördes efter den nationella krisövningen SAMÖ-KKÖ 2011 pekas bland annat på att det finns anledning att se över formerna för vem som deltar och hur samverkan i mötesform i övrigt struktureras i det inledande skedet av en kris.[38]

MSB kan konstatera att det förekom brister bland de berörda aktörerna när det gällde att analysera konsekvenser och beroenden i samband med driftstörningen. Flera av de berörda aktörerna har själva inte tillräcklig kunskap om sina egna beroenden och därigenom inte heller sina samverkansbehov. Om it-incidenten lett till större samhällsproblem skulle MSB därför haft svårt att samordna arbetet med att avhjälpa och lindra effekterna av incidenten, samt med att skapa en tillräckligt bra grund för samverkan.

4.4 Informationssamordning och kommunikation

Driftstörningen drabbade ett stort antal organisationer och enskilda medborgare. Att kunna ge information om vad som hänt och att fortlöpande ge råd och rekommendationer är en central uppgift i krishanteringen för alla offentliga aktörer och för drabbade verksamheter. Det är av avgörande betydelse att kunna samordna informationen till allmänheten i syfte att ge en enhetlig bild av konsekvenser, berörda aktörer, behov av åtgärder och händelseförlopp.

Förutom behovet av att nå ut till enskilda medborgare och verksamheter måste massmedias behov av information tillgodoses. Massmedia är en viktig kanal för kommunikation och information. Kontakterna med massmedia kan dock leda till ytterligare spekulationer om det inte finns en tydlig kommunikations-strategi. Massmedia måste i ett tidigt skede ges tillgång till information av hög kvalitet.

Vid it-incidenter är ett tillkommande problem att de normala informations- och kommunikationskanalerna kan ha drabbats av incidenten, det vill säga att exempelvis webbplatser, telefoni och e-post inte är tillgängliga.

När det gäller driftstörningen hos Tieto ligger ett stort ansvar på de drabbade verksamheterna, det vill säga företagets kunder, att själva kunna informera sina avnämare och även andra intressenter. Händelsen visar att detta ansvar är svårt för många aktörer att fullt ut leva upp till. Det finns tre huvudsakliga skäl till detta:

- Tieto kunde inte ge information om när incidenten förväntades vara avhjälpt. Detta var den fråga som intresserade drabbade verksamheter och deras avnämare mest.

38 *Utvärdering SAMÖ-KKÖ 2011 – Kortversion*. Publikationsnummer: MSB326 – oktober 2011, MSB.

- De drabbade verksamheternas normala kommunikationskanaler, som exempelvis interna och externa webbplatser samt e-post, fungerade i flera fall inte.
- Många av de drabbade verksamheterna hade inte förberett alternativa kommunikationskanaler.

Webbplatsen Krisinformation.se förmedlar information från myndigheter och andra ansvariga om hur de hanterar olika kriser – före, under och efter krisen. Webbplatsen riktar sig till allmänhet och media. Krisinformation.se drivs av MSB och innehållet är framtaget genom myndighetsgemensamma arbetsgrupper inom olika områden. I samband med driftstörningen fördes en diskussion kring huruvida Krisinformation.se skulle kunna fungera som alternativ webbplats för Apoteket AB. Detta ansågs dock inte lämpligt eftersom webbplatsen endast ska fungera som plattform för myndighetsinformation.

Idag drivs allt mer samhällsviktig verksamhet i privat regi. Uppdragsgivaren kan dock fortfarande vara en offentlig organisation. Den aktuella driftsstörningen visar att det hos olika aktörer finns oklarheter kring rollerna när det gäller kommunikation kring bortfall av tjänster. Bortfallet av funktioner hos det stora logistikföretaget påverkade bland annat ett stort antal verksamheter inom Stockholm läns landsting. I en sådan situation kan det vara svårt att veta om företaget ska kommunicera med varje verksamhetsdel eller med beställarorganisationen som en enhet. Ska kommunikationen hanteras av den offentliga beställaren eller av den upphandlade, privata utföraren? Kan en privat utförare få tillgång till samma kommunikationskanaler som sin uppdragsgivare och därigenom få en möjlighet att kommunicera på samma villkor?

Här är det viktigt att klargöra att även om verksamhet har outsourcats är den offentliga beställaren ansvarig inför medborgarna. Om en privat verksamhet som utför ett offentligt uppdrag förväntas kommunicera med medborgarna måste detta framgå i upphandlingsprocessen. Lämpliga kommunikationskanaler måste också förberedas.

4.5 Beredskaps- och kontinuitetsplanering med inriktning på informationssäkerhet

Beredskap och kontinuitetsplanering för längre avbrott krävs i de flesta verksamheter, men särskilda behov uppstår då en organisation outsourcar sin it-drift eller använder molntjänster för vitala delar av sin verksamhet. I sådana fall behövs det avtal mellan kund och leverantör som tydliggör ansvaret och de aktiviteter eller åtgärder som ska tillämpas vid oplanerade avbrott.

När en organisation outsourcar it-drift till en leverantör, eller använder molntjänster i större omfattning, är det viktigt att komma ihåg att ansvaret för att kunna upprätthålla verksamheten alltid kvarstår hos den outsourcande organisationen. Det innebär att organisationen måste ha egen beredskap och planering för vilka åtgärder som ska vidtas vid ett längre avbrott där kraven på leverantören blir en del av den egna planeringen.

Kontinuitetsplaneringen måste basera sig på en riskanalys och tydlig prioritering från ledningen – vilka delar av verksamheten som är mest centrala att upprätthålla. Utifrån denna prioritering kan sedan krav ställas på it-resurser som förvaltas både internt och externt. Riskanalys är alltså en nödvändig förutsättning för kravställande.

Statliga myndigheter[39] omfattas av MSB:s föreskrifter om informationssäkerhet. I dessa föreskrifter, som utgår från ledningssystem för informationssäkerhet, är risk- och sårbarhetsanalyser en central beståndsdel liksom hur risker ska hanteras. I ledningssystemet är sedan kontinuitetsplanering en central beståndsdel.

Vidare har de myndigheter som pekas ut i förordningen (2006:942) om krisberedskap och höjd beredskap ett särskilt ansvar att planera för åtgärder för att samhället ska kunna motstå påfrestningar av olika slag, från kriser till höjd beredskap. Regeringen betonar vikten av att denna planering genomförs och att det finns en helhetssyn som omfattar hela hotskalan. Myndigheter som omfattas av förordningen bör därför, exempelvis inom samverkansområdena, arbeta med såväl åtgärder för fredstida krissituationer som planering av åtgärder vid höjd beredskap.[40]

Ett antal kommuner drabbades av driftstörningen hos Tieto. Kommunerna är enligt lag (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap, skyldiga att upprätthålla en beredskapsplanering. Dock är lagen inte skriven specifikt för it-incidenter. Kommunerna omfattas däremot av MSB:s föreskrifter om risk- och sårbarhetsanalyser och i dessa finns krav på att varje kommun och landsting ska bedöma sin krisberedskapsförmåga. En indikator för bedömningen är huruvida det finns en plan för hur de ska hantera extraordinära händelser. Med tanke på att alla organisationer idag är beroende av informationshantering för att kunna upprätthålla sina verksamheter bör det vara rimligt att en planering innehåller uppgifter om krav på leverantörer av it-drift och it-relaterade tjänster.

Kunder som upphandlar it-drift av olika slag har i princip goda möjligheter att i avtal reglera kraven för tillgänglighet; framförallt genom de standardiserade avtal om SLA (Service Level Agreement) som driftsleverantörerna tillhandahåller. Dessa avtal definierar i allmänhet nivån av accepterade avbrott och får därför ses som en beskrivning av ett normalläge. Utöver detta bör avtalen även innehålla krav för att minimera negativa konsekvenser av ett krisläge samt aktiviteter som ska vidtas under en återställningsfas. Här bör finnas krav på kontinuitetsplanering hos leverantören och att leverantören förbinder sig att delta i övningar av kundens planering. Krav på leverantören förutsätter en väl utarbetad planering hos kunden, för att kundens processer verkligen ska kunna upprätthållas vid längre avbrott. Leverantören bör också kunna erbjuda olika nivåer av redundans så att kunden själv kan välja vilken risk den är beredd att ta. Detta kan till exempel ske via funktionen ”dual sites”, geografiskt åtskilda

39 Författningen gäller för myndigheter under regeringen med undantag för Regeringskansliet, kommittéväsendet och Försvarsmakten.

40 Prop. 2011/12:1 (Budgetpropositionen för 2012), utgiftsområde 6

plattformar som är sammankopplade vilket leder till att information och tjänster är replikerade och åtkomliga från mer än ett ställe.

Offentliga aktörer, cirka 700 organisationer, har möjlighet att använda Kammarkollegiets ramavtal när det gäller bland annat it-drift och e-förvaltningsstödjande tjänster. I det senare avtalet finns en bilaga kring tillgänglighet[41], något som saknas i ramavtalet för it-drift. I båda fallen gäller ”IT-företagens Allmänna Bestämmelser: IT-Drift version 2008” som innehåller ett övergripande krav på leverantören att avhjälpa fel i tjänsten.[42] Dessutom kan de offentliga kunderna sluta ytterligare tilläggsavtal som innefattar mer explicita krav på att upprätthålla tjänsten samt på kontinuitetsplanering och redundans. Kammarkollegiets uppfattning är att denna möjlighet inte har utnyttjats i någon högre grad hittills.

Bilden kompliceras ytterligare av att en offentlig verksamhets krav på kontinuitet ofta måste överföras i flera avtalsled som när ett landsting upphandlar en privat vårdgivare som anlitar en stor logistikleverantör, som i sin tur upphandlar en it-driftleverantör. Här kan det till exempel bli mycket svårt för den ansvarige sjukvårdshuvudmannen (landstinget) att verkligen kunna kontrollera att kraven efterlevs i varje led.

Intrycket från driftstörningen är att aktörernas kontinuitetsplanering varit av skiftande karaktär. Vissa drabbade har haft en relativt god planering där exempelvis det drabbade logistikföretaget haft god nytta av den planering som gjordes i samband med pandemin, influensan A(H1N1), medan andra aktörer har arbetat mer improviserat. Apoteket AB kunde delvis ställa om till ett äldre system och komplettera med manuella rutiner, medan andra drabbade förefaller ha haft mycket rudimentär planering för denna typ av händelse. Värt att notera är att flera av aktörerna inte haft reservrutiner för att kommunicera med sina medarbetare, sina medborgare eller sina kunder trots att god kommunikation är en förutsättning för att kunna hantera ett krisläge.

Formella krav på leverantören vad gäller beredskaps- eller kontinuitets-planering tycks ha förekommit i begränsad omfattning i de organisationer som varit berörda av driftsstörningen. Det drabbade logistikföretaget uppger till exempel att en av deras kunder – en stor offentlig aktör – i avtal ställt krav på att de ska ha en beredskapsplanering och det framgår även att Tieto haft liknande krav på sig från vissa kunder.

Tieto har muntligen presenterat sin kontinuitetsplanering, vilken är utformad efter framför allt de internationella standarder som är aktuella för it-drift, och

41 Kammarkollegiets ramavtal för e-förvaltningsstödjande tjänster, § 3.14: ”Tjänstekontinuitet och tillgänglighetshantering Leverantören skall ha en process för hantering av tjänstekontinuitet och tillgänglighet. Kraven på tjänstens tillgänglighet och kontinuitet skall identifieras på grundval av kundernas verksamhetsplaner, överenskommelse om tjänstenivå och riskbedömningar. Kraven skall omfatta åtkomsträttigheter och svarstider såväl som tillgänglighet för hela kedjan av systemkomponenter. Tillgänglighets- och kontinuitetsplaner för tjänsten skall utvecklas och granskas minst en gång per år för att ge möjlighet att säkerställa att kraven uppfylls enligt avtal under alla omständigheter, från normal drift till långa eller allvarliga avbrott i tjänsten. Tillgängligheten skall mätas och registreras. Oplanerad brist i tillgänglighet skall undersökas och lämpliga åtgärder genomföras."

42 IT & Telekomföretagen, *Allmänna bestämmelser, IT-drift version 2008*, § 15.1: ”Leverantören skall avhjälpa fel i Tjänsten som beror på omständighet för vilken leverantören ansvarar inom den tid som anges i Bilaga om garanterad servicenivå om sådan är tillämplig. I övrigt skall fel avhjälpas med den skyndsamhet omständigheterna kräver.”

uppger att planeringen visat sig fungera väl efter omständigheterna. En erfarenhet företaget dragit som leverantör är att de kunder som haft en mer omfattande kontinuitetsplanering, och därmed gjort en mer kvalificerad kravställning, drabbats lindrigare av incidenten än övriga kunder. Dessa kunder har till exempel ställt krav på dual sites-lösningar som förutom bättre säkerhet även innebär en ökad kostnad för kunden.

Både Tieto och andra leverantörer har framfört att de i ett krisläge gör egna prioriteringar, oavsett SLA eller andra avtal, av sina kunder utifrån vad de anser vara samhällsviktig verksamhet. Prioriteringarna har i vissa fall gått emot leverantörens eget kommersiella intresse. Det innebär att även kunder som gör en mer omfattande planering och inkluderar avtal med leverantörer om tillgänglighet ändå inte kan vara säkra på att få den leverans de avtalat om när det gäller informationssäkerheten. Här finns alltså ett starkt element av oförutsägbarhet både för den enskilde kunden och för helheten då det i praktiken blir den enskilda leverantören som beslutar om prioriteringen mellan olika kunder.

Diskussionen om vad som är samhällsviktig verksamhet, och önskan från olika samhällsaktörer om att det bör fastställas vad som är samhällsviktig verksamhet, är inte ny. I utvärderingen av förberedelser och hantering av pandemin, influensan A(H1N1), pekar MSB och Socialstyrelsen på att processen för identifiering och prioritering av samhällsviktiga verksamheter vållade problem för berörda aktörer.[43] Begreppet samhällsviktig verksamhet har dock förtydligats i den nationella strategin för skydd av samhällsviktig verksamhet som MSB redovisade i maj 2011.[44] Inom ramen för projektet Styrel har även kriterier för identifiering och prioritering av samhällsviktig verksamhet utarbetats.[45]

MSB:s sammanfattande bedömning är att det finns brister i kontinuitets-planeringen och beredskapen för denna typ av händelser hos många av de drabbade organisationerna.

4.6 Riskanalyser med inriktning på informationssäkerhet

Riskanalys är en förutsättning för att kunna genomföra outsourcing av it-drift eller upphandling av mer omfattande molntjänster på ett medvetet sätt.

Informationssäkerhet ska behandlas i de risk- och sårbarhetsanalyser som offentliga verksamheter enligt MSB:s föreskrifter är skyldiga att genomföra årligen.[46] Till detta kommer även krav på att statliga myndigheter och andra, till exempel kommuner och landsting, som omfattas av

43 *Influensa A(H1N1) 2009: Utvärdering av förberedelser och hantering av pandemin*. MSB och Socialstyrelsen.

44 *Ett fungerande samhälle i en föränderlig värld. Nationell strategi för skydd av samhällsviktig verksamhet*. Publikationsnummer: MSB266 - december 2011, MSB.

45 Styrel är ett landsomfattande planeringssystem för prioritering av samhällsviktiga elanvändare vid en förutsedd eller plötsligt uppkommen kortvarig elbrist. Energimyndigheten ansvarar för Styrelplaneringens genomförande. Under 2011 har planeringen skett i alla landets kommuner, landsting och län. Från och med 2012 kan en frånkoppling av elanvändare, enligt planeringen, ske.

46 MSBFS 2010:7 *föreskrifter om statliga myndigheters risk- och sårbarhetsanalyser*, samt MSBFS 2010:6 *föreskrifter om kommuners och landstings risk- och sårbarhetsanalyser*.

säkerhetsskyddsförordningen (1996:633) är skyldiga att undersöka vilken verksamhet som kräver ett säkerhetsskydd med hänsyn till rikets säkerhet eller skydd mot terrorism. Detta kan omfatta skyddsvärd information och resurser för att hantera skyddsvärd information. En viktig del i detta är skyldigheten att genomföra en säkerhetsanalys.

Det finns även krav på risk- och sårbarhetsanalys enligt personuppgiftslagen (1998:204). Den personuppgiftsansvarige måste genomföra en risk- och sårbarhetsanalys för att bedöma om det är möjligt att anlita tjänsteleverantören för behandling av de tänkta personuppgifterna, vilken säkerhetsnivå som är lämplig och vilka åtgärder som måste vidtas. Det är även värt att notera att den som använder andras tjänster för sin personuppgiftsbehandling är personuppgiftsansvarig för behandlingen av uppgifterna även om den utförs av tjänsteleverantören eller dess underleverantörer.[47]

Arbetet med att inkludera informationssäkerhet i de risk- och sårbarhetsanalyser som genomförs befinner sig hos många aktörer fortfarande i en utvecklingsfas. Det är dessutom svårt för en enskild aktör att bedöma i vilken grad den tilltagande koncentrationen på it-driftområdet påverkar dess egen riskexponering.

En separat riskanalys bör göras inför varje större upphandling som kan påverka informationssäkerheten. En viktig del i detta är den informationsklassning som varje verksamhet bör tillämpa för att kunna bedöma olika alternativ, och för att ställa säkerhetskrav.

En iakttagelse i analysarbetet efter den aktuella driftstörningen är att det framstår som om få aktörer låtit upphandling och utläggning av tjänster föregås av informationsklassning eller riskanalys. MSB:s bedömning är att detta försvårar en väl fungerande kontinuitetsplanering eftersom organisationerna sannolikt inte har gjort någon närmare analys av sitt beroende av den utlagda resursen.

4.7 Att lära av it-incidenter

Under det akuta skedet av en större incident eller kris är möjligheten till reflektion starkt begränsad. För att bedöma de långsiktiga verkningarna finns därför ett behov av återkoppling efter en tid då verksamheten återgått till ett normalläge. Att lära av olyckor och kriser är en viktig del i det förebyggande och förberedande arbetet och utgör viktigt underlag i arbetet med beredskapsplaner, risk- och sårbarhetsanalyser, samverkan, reglering, utbildningar, övningar med mera.

I samband med driftstörningen har framför allt tillgänglighetsaspekterna uppmärksammats. Det finns dock anledning att återkomma till hur riktighet och spårbarhet påverkats, samt i vilken omfattning information har försvunnit. Sannolikt finns också ytterligare aktörer som drabbats indirekt av incidenten.

47 Läs vidare om molntjänster och personuppgiftslagen på Datainspektionens webbsida: http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/molntjanster/

En intressant aspekt som särskilt bör uppmärksammas är de ekonomiska konsekvenserna, vilka med all sannolikhet blivit mycket omfattande. Detta är en viktig faktor att ta hänsyn till i framtida riskanalyser på alla ansvarsnivåer och inom alla sektorer i samhället.

För MSB:s fortsatta arbete inom informationssäkerhetsområdet, och ur ett bredare krishanteringsperspektiv, är det av vikt att få ta del av aktörernas erfarenheter från den inträffade incidenten och den hantering av händelsen som genomfördes. Detta för att kvalitetssäkra det förebyggande arbetet, men också för att dra nyttiga lärdomar i arbetet med att stödja och samordna i ett akut skede (förberedande).

5. Avslutande reflektioner och fortsatt arbete

5.1 Avslutande reflektioner

Svensk krishantering bygger på samverkan. Alla aktörer måste vid händelse av en kris kunna agera tillsammans och samverka kring beslut och insatser. Ansvarsprincipen, närhetsprincipen och likhetsprincipen är viktiga utgångspunkter i den svenska krisberedskapen. En kris hanteras till en början i dess omedelbara närhet, samtidigt som det finns resurser på regional och nationell nivå om händelserna blir för omfattande för att hantera på lokal nivå. Kommunernas verksamhet är grunden för i stort sett all krishantering. Under en kris ska länsstyrelsen, i egenskap av geografiskt områdesansvarig på regional nivå, stödja kommunen när det gäller samverkan mellan myndigheter, kommuner och andra aktörer.

Den ökade koncentrationen av it-drift och andra it-relaterade tjänster, exempelvis molntjänster, skapar både nya möjligheter och risker i samhället. Denna förändring av leveransformer kan vara ett sätt att både öka kvaliteten och sänka kostnaderna i en verksamhet. Incidenten hos Tieto visar att en driftstörning hos en stor it-driftleverantör kan påverka hela samhället och att konsekvenserna kan bli omfattande. Det moderna samhället står i allt högre grad stilla när it-systemen inte är tillgängliga.

När det gäller it-incidenter är förvarningen kort eller obefintlig, tempot högt och händelsen oftast geografiskt obunden. För att förebygga och hantera allvarliga it-incidenter krävs en ökad förmåga hos alla aktörer i samhället – på alla ansvarsnivåer och inom alla sektorer. Den aktuella driftstörningen visar att aktörerna i krishanteringssystemet behöver utveckla förmågan när gäller lägesbilder och samlade konsekvens- och hanterandebedömningar. Flera av de berörda aktörerna har själva inte en tillräcklig kunskap om sina egna beroenden och därigenom inte heller sina samverkansbehov. Den egna beredskapen kan också i flera fall utvecklas.

Det är viktigt att i ännu högre grad än vad som idag är fallet skapa förutsättningar för att kunna använda samhällets samlade resurser för att förebygga och hantera allvarliga it-incidenter. Kunskap om kompetenser och roller inom både offentlig och privat sektor behöver ökas. Inblandade aktörer måste ha kunskap om varandras roller och vilken information olika aktörer behöver och kan erbjuda.

5.2 Fortsatt arbete

Stärkt förebyggande informationssäkerhetsarbete i hela samhället

Det förebyggande informationssäkerhetsarbetet behöver utvecklas – på alla ansvarsnivåer och inom alla sektorer – och samordnas ytterligare för att kunna förebygga och hantera allvarliga it-incidenter i samhället. För att öka

samhällets informationssäkerhet krävs en ökad samverkan mellan offentliga och privata aktörer.

Arbetet bör fortsätta i linje med strategin för samhällets informationssäkerhet.[48] Det kommer även att förtydligas ytterligare genom den nationella handlingsplan som för närvarande utarbetas i samverkan mellan de myndigheter som ingår i Samverkansgruppen för informationssäkerhet (SAMFI)[49] och andra berörda myndigheter.

Driftstörningen visar att sektorsansvariga myndigheter, länsstyrelser, landsting och kommuner behöver utveckla förmågan att förebygga och hantera it-relaterade kriser.

Bättre säkerhet med upphandling som verktyg

Det finns en stor potential när det gäller upphandling där alla aktörer i samhället behöver utveckla sin kompetens för att bättre kunna använda upphandling som ett medel för att styra sin informationssäkerhet.

I avtal går det också att formulera regler som stödjer samhällets krishantering, till exempel kan det ställas krav på rapportering kring incidenter samt hur leverantörerna ska bidra vid en allvarlig störning. Denna typ av styrning framstår som ändamålsenlig eftersom de offentliga verksamheterna alltmer agerar som beställare av olika tjänster. Avtalsvillkor kan då också flyttas med till eventuella underleverantörer.

De upphandlingar som sker via Kammarkollegiet är ett viktigt verktyg för att öka informationssäkerheten i den offentliga förvaltningen

Särskilt fokus på riskanalys och kontinuitetsplanering

Den aktuella driftstörningen visar på brister i kontinuitetsplaneringen och beredskapen hos flera av de drabbade organisationerna. Ett systematiskt arbete med informationsklassning och riskanalys är en grundförutsättning för allt informationssäkerhetsarbete.

Då viktiga samhällsaktörers informationshantering i allt högre grad bygger på tekniskt och organisatoriskt integrerade lösningar blir både riskanalys och kontinuitetsplanering komplexa att genomföra. Riskanalyser, och då särskilt informationsklassning, är ett viktigt redskap vid upphandlingar och även ur denna synpunkt är samordning väsentlig eftersom den offentliga sektorns upphandlingar till stor del kan ske via Kammarkollegiets ramavtal. Riskanalyser kan därmed vara en pådrivande faktor för en generellt förbättrad informationssäkerhet.

48 *Strategi för samhällets informationssäkerhet 2010-15*. Publikationsnummer: MSB 0171-10, MSB

49 Samverkansgruppen för informationssäkerhet (SAMFI) består av sex myndigheter med särskilda uppgifter inom informationssäkerhetsområdet. SAMFI ska genom informationsutbyte och samverkan stödja de aktuella myndigheternas uppdrag inom området. Följande myndigheter är medlemmar i SAMFI: Försvarets materielverk (FMV), Försvarets Radioanstalt (FRA), Försvarsmakten (FM), Myndigheten för samhällsskydd och beredskap (MSB), Post- och telestyrelsen (PTS), samt Rikspolisstyrelsen (RPS) som representeras genom Säkerhetspolisen (SÄPO) och Rikskriminalpolisen (RKP).

Det är viktigt att utveckla stöd som gör det möjligt även för organisationer med begränsade resurser att genomföra riskanalyser och informationsklassning, samt kontinuitetsplanering.

Kontinuitetsplaner och andra ramverk för it-incidenthantering behöver övas och uppdateras regelbundet.

Nationell och regional informationssäkerhetsrelaterad lägesbild

Den ökade koncentrationen av it-drift och andra it-relaterade tjänster innebär att ett stort antal aktörer kan komma att drabbas samtidigt av en incident och att konsekvenserna för samhället kan bli allvarliga. Detta ställer ökade krav på samordning och samverkan.

Samverkan och samordning vid en allvarlig it-incident förutsätter att det finns relevanta och aktuella lägesbilder på lokal, regional, sektoriell och nationell nivå. Driftstörningen visar att de berörda aktörerna behöver utveckla processer för informationsinhämtning och informationsdelning. I detta bör även ingå att kunna kommunicera informationen till medborgarna och det förutsätter att informationen samordnas.

MSB avser att fortsätta arbeta med att utveckla en nationell informationssäkerhetsrelaterad lägesbild i samverkan med berörda aktörer i samhället. En grundförutsättning i det arbetet är den Nationella samverkansfunktionen för informationssäkerhet (NOS). Särskilt fokus kommer att läggas på behovet av att snabbt kunna inhämta lägesinformation från olika aktörer i samhället, som till exempel sektorsansvariga myndigheter och länsstyrelser. En viktig fråga som behöver hanteras är hur lägesinformation ska kunna inhämtas från privata aktörer på ett sätt som inte riskerar att äventyra deras affärsverksamhet eller behov av sekretess.

Ytterligare en viktig del i arbetet med att skapa en nationell informationssäkerhetsrelaterad lägesbild är system för obligatorisk it-incidentrapportering för statliga myndigheter.[50] Mot bakgrund av den aktuella driftstörningen anser MSB att det i det fortsatta arbetet bör övervägas om en sådan rapportering också ska omfatta andra offentliga aktörer, som exempelvis kommunerna.

50 Se vidare MSB:s svar på regeringsuppdraget om obligatorisk it-incidentrapportering (uppdragsredovisning 2011-03-01, dnr 2010-6307). I proposition 2011/12:1 (Utgiftsområdet 6) skriver regeringen att MSB kommer att ges i uppdrag att göra en fördjupad analys om obligatorisk it-incidentrapportering för statliga myndigheter.

Bilaga 1: Hemställan enligt KBF

Myndigheten för samhällsskydd och beredskap

Hemställan

1 (3)

Datum
2011-12-06

Diarienr
2011-6477

Ert datum

Er referens

Avdelningen för samordning och insats
Tjänsteman i beredskap

Enligt sändlista

Hemställan angående information om driftstörningar orsakade av större hårdvarufel hos Tieto

Under den senaste veckan har ett antal samhällsaktörer som Apoteket AB, Apotekens Service AB, Stockholms stad och Bilprovningen drabbats av omfattande driftsstörningar orsakade av problem hos deras tjänsteleverantör Tieto. På grund av de avtalsmässiga förhållandena kan Tieto inte avslöja vilka kunder som har blivit drabbade.

Myndigheten för samhällsskydd och beredskap (MSB) kommer att göra en utredning angående vad som hänt hos Tieto. Utredningen kommer att ske med utgångspunkt från MSB:s uppdrag att analysera hot och risker i samhället som kan anses vara särskilt allvarliga. En viktig del i detta är att förstå de konsekvenser som incidenten lett till samt att ta fram förslag på åtgärder som kan leda till ett förbättrat skydd för såväl samhället som för enskilda aktörer.

Myndigheten för samhällsskydd och beredskap (MSB) begär i enlighet med 15 § förordningen (2006:942) om krisberedskap och höjd beredskap att myndigheterna enligt sändlistan lämnar en lägesbedömning enligt nedanstående punkter. Försvarsmakten lämnar uppgifter efter eget beslut.

1. Är några aktörer inom ert ansvarsområde drabbade av ovanstående händelse?

Om svaret är ja på fråga 1 besvaras även följande frågor:

2. Vilka aktörer har blivit drabbade och på vilket sätt?
3. På vilket sätt har ni fått information om det inträffade hos dessa aktörer?
4. Kan ni bedöma om aktörernas verksamhet i nuläget fungerar normalt eller finns det kvardröjande negativa effekter?

Lägesbedömningen ska lämnas till MSB senast kl 13.00 den 14 december på adressen:

MSB Myndigheten för samhällsskydd och beredskap

Postadress:
651 81 Karlstad

Besöksadress:
Stockholm: Kungsgatan 53
Karlstad: Norra Klaragatan 18
Sandö: Sandövägen 7
Revinge: Revingeby

Telefon: 0771-240 240
Fax: 010-240 56 00
Kryfax 010-240 43 63

registrator@msb.se
www.msb.se

Org nr.
202100-5984

Fia Ewald
Avd. för risk- och sårbarhetsreducerande arbete
Enheten för samhällets informationssäkerhet
fia.ewald@msb.se

Postadress:
651 81
KARLSTAD

Om de svar ni lämnar innehåller känslig information använd kryfax 010-240 43 63. Informationen kommer att skyddas i enlighet med Offentlighets- och sekretesslagen (2009:400).

SÄNDLISTA

Datainspektionen datainspektionen@datainspektionen.se
Energimyndigheten registrator@energimyndigheten.se
Finansinspektionen finansinspektionen@fi.se
Kustbevakningen registrator@kustbevakningen.se
Livsmedelsverket livsmedelsverket@slv.se
Läkemedelsverket registrator@mpa.se
Länsstyrelsen i Blekinge blekinge@lansstyrelsen.se
Länsstyrelsen i Dalarna dalarna@lansstyrelsen.se,
Länsstyrelsen i Gävleborg gavleborg@lansstyrelsen.se,
Länsstyrelsen Gotlands län gotland@lansstyrelsen.se,
Länsstyrelsen i Halland halland@lansstyrelsen.se,
Länsstyrelsen i Jämtlands län jamtland@lansstyrelsen.se,
Länsstyrelsen i Jönköpings län jonkoping@lansstyrelsen.se,
Länsstyrelsen i Kalmar län kalmar@lansstyrelsen.se,
Länsstyrelsen i Kronobergs län kronoberg@lansstyrelsen.se
Länsstyrelsen i Norrbottens län norrbotten@lansstyrelsen.se
Länsstyrelsen i Skåne skane@lansstyrelsen.se
Länsstyrelsen i Stockholms län stockholm@lansstyrelsen.se
Länsstyrelsen i Södermanland sodermanland@lansstyrelsen.se
Länsstyrelsen i Uppsala län uppsala@lansstyrelsen.se
Länsstyrelsen i Värmlands län varmland@lansstyrelsen.se
Länsstyrelsen i Västerbotten vasterbotten@lansstyrelsen.se
Länsstyrelsen i Västernorrlands län vasternorrland@lansstyrelsen.se
Länsstyrelsen i Västmanland vastmanland@lansstyrelsen.se
Länsstyrelsen i Västra Götalands län vastragotaland@lansstyrelsen.se
Länsstyrelsen i Örebro län orebro@lansstyrelsen.se
Länsstyrelsen Östergötland ostergotland@lansstyrelsen.se
Post- och telestyrelsen pts@pts.se
Rikspolisstyrelsen rikspolisstyrelsen@polisen.se
SMHI smhi@smhi.se

Socialstyrelsen socialstyrelsen@socialstyrelsen.se
Strålsäkerhetsmyndigheten registrator@ssm.se
Svenska Kraftnät svenska.kraftnat@svk.se
Trafikverket registrator@trafikverket.se
Transportstyrelsen registrator@transportstyrelsen.se
Tullverket tullverket@tullverket.se
Försvarsmakten (omfattas ej av 15 §, eget beslut om rapportering)
exp-hkv@mil.se

För kännedom:

Fö/SSK

Bilaga 2: Sekretessförklaring

Myndigheten för samhällsskydd och beredskap

1 (3)

Datum
2012-01-09

Diarienr

Ert datum

Er referens

Verksamhetsstöd
Rättssenheten
Torkel Schlegel
010-2405069
torkel.schlegel@msb.se

Tieto Sweden AB
Katarina Aurell
Fjärde bassängvägen 15
115 83 Stockholm

Förklaring om sekretess i samband med MSBs utredningar m.m.

Inledning

Myndigheten för samhällsskydd och beredskap (MSB) har genom sin instruktion ett generellt uppdrag att samverka med näringslivet för att identifiera och analysera sådana sårbarheter, hot och risker i samhället som kan anses vara särskilt allvarliga. MSB ska värdera, sammanställa och rapportera resultatet av sådant arbete till regeringen.

MSB har nu inlett en samverkan med Tieto Sweden AB (Tieto) för att utreda en under november 2011 inträffad IT-incident hos Tieto.

För MSBs verksamhet gäller offentlighetsprincipen som innebär att de handlingar som förvaras på myndigheten och som inkommer eller upprättas på myndigheten är allmänna handlingar. Dessa ska som huvudregel vara offentliga och lämnas ut på begäran. Finns däremot en tillämplig sekretessbestämmelse får myndigheten inte lämna ut sekretessbelagda uppgifter i handlingen. Sekretessbestämmelsen innebär också en tystnadsplikt för myndighetens medarbetare gällande de uppgifter som träffas av sekretessbestämmelsen. Brott mot tystnadsplikten är straffsanktionerat enligt 20 kap. 3 § Brottsbalken.

Frågan om sekretess för en uppgift prövas inte i förväg utan först när uppgiften ska lämnas ut. Det är MSB som självständigt prövar frågan och MSBs beslut att neka utlämnande kan överklagas till Kammarrätt.

Om MSB genom sin samverkan med näringslivet genomför en utredning för att identifiera och analysera allvarliga sårbarheter, hot och risker i samhället finns det tillämpliga sekretessbestämmelser varav den mest relevanta för nu aktuella utredningsverksamhet beskrivs nedan.

Tillämpliga regler

Genom offentlighets- och sekretesslagen (OSL) 30 kap. 23 §, offentlighets- och sekretessförordningen 9 § och förordningens bilaga punkt 13 följer att när MSB utreder frågor med avseende på näringslivet gäller sekretess för uppgifter om affärs- eller driftförhållanden, uppfinningar eller forskningsresultat om det kan antas att näringsidkaren lider skada om uppgifterna röjs.

Om MSB t.ex. samverkar med näringslivet för att utreda vilken samhällspåverkan ett inträffat fel i ett IT-system kan ha, är denna sekretessbestämmelse tillämpbar. Sekretessen gäller inte alla uppgifter som myndigheten kan tänkas ta del av men borde täcka det som är väsentligast för näringsidkarna i och med skaderekvisitet.

Enligt samma lagrum råder en absolut sekretess för uppgifter som rör den som trätt i affärsförbindelse eller liknande (t.ex. Tietos kunder m.fl.) med den näringsidkare som myndigheten samverkar med.

Även andra sekretessbestämmelser kan vara tillämpliga beroende på vad för slags uppgifter det gäller. Enligt 18:8 OSL gäller sekretess för uppgifter om säkerhets- eller bevakningsåtgärder om det kan antas att syftet med åtgärden motverkas om uppgiften röjs och åtgärderna avser telekommunikation eller system för automatiserad behandling av information. Denna sekretess kan t.ex. användas för uppgifter om "brandväggar" och liknande.

Meddelarfrihet

Meddelarfrihet innebär i korthet att den enskilde myndighetsmedarbetaren kan lämna muntliga uppgifter till media. Meddelarfriheten följer av tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Meddelarfriheten bryter sekretess enligt 30:23 OSL för uppgifter som rör den näringsidkare myndigheten samverkar med, dock inte för denne näringsidkares affärspartners m.fl.. Se 30:30 OSL. Meddelarfrihet gäller inte heller för uppgifter som omfattas av sekretess enligt 18:8 OSL.

Förfogande över material

Om handlingar lämnas över till myndigheten, sk inkomna handlingar, förlorar näringsidkaren rådigheten över dessa och dess information. Näringsidkaren kan inte begära att få tillbaka dessa eller att materialet ska förstöras. Det kan i och för sig finnas upphovsrätt till materialet men det begränsar bara vad myndigheten kan utnyttja materialet till, inte att myndigheten får och ska behålla det.

Samverkan mellan MSB och Tieto

Gällande rätt

MSB kommer att hantera all information, skriftlig eller muntlig, i enlighet med gällande rätt och enligt de skyldigheter gällande rätt ålägger myndigheten. MSB kommer också att göra vad som åligger myndigheten för att informera myndighetens medarbetare vilka skyldigheter de har enligt gällande rätt.

Dokumentation och skriftligt material

MSB kommer under samverkan med Tieto inte att begära in någon dokumentation eller skriftligt material. MSB kommer endast att ta emot sådant material om det är Tietos avsikt att MSB ska ta emot materialet.

Tietos företagshemliga material

MSB är införstådda med att Tieto anser att allt material och all information som MSB kan komma att få ta del av kan vara sådan att det skadar bolaget eller bolagets affärspartners om det offentliggörs.

Yttrande i samband med skadeprövning

Om det blir aktuellt att pröva en fråga om att lämna ut uppgifter eller allmänna handlingar som kan omfattas av sekretess och där uppgifterna eller handlingarna på något sätt härrör från Tietos verksamhet och kommit MSB tillhanda i samband med samverkan för utredning om nu aktuella IT-incident kommer MSB att ge Tieto tillfälle att yttra sig om på vilket sätt ett offentliggörande kan vålla Tieto eller dess affärspartners skada.

Vid en begäran om utlämnande av allmän handling är MSB skyldig att skyndsamt pröva frågan. Tietos måste därför också hantera sitt yttrande skyndsamt.

Beredning

Denna avsiktsförklaring har gjorts av Richard Oehme, chef för enheten för samhällets informationssäkerhet. Torkel Schlegel, chef för Rättsenheten har varit föredragande.

Richard Oehme

Torkel Schlegel

Myndigheten för samhällsskydd och beredskap
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB 367-12 ISBN 978-91-7383-209-0