Myndigheten för samhällsskydd och beredskap

FORSKNING

Driftavbrott i samhällsviktiga it-tjänster

Faktaruta

Driftavbrott i samhällsviktiga it-tjänster (DRISTIG)

2016-2018

RISE Research Institutes of Sweden

Ulrik Franke

Det moderna samhället är beroende av it-tjänster. Driftavbrott kan leda till allt från kortare elavbrott till brist på livsmedel eller läkemedel. Projektet DRISTIG har under drygt två år studerat driftavbrott i samhällsviktiga it-tjänster. Rapporten redovisar kort några forskningsresultat relaterade till kostnader för avbrott, försäkringar mot avbrott och så kallade *Service Level Agreements* (SLA).

MSB:s kontaktpersoner:
Ulrika Mollstedt, 010-240 52 15
Johan Turell, 010-240 41 55

Foto: Johan Eklund, MSB

Publikationsnummer MSB1281 – oktober 2018
ISBN 978-91-7383-877-1

MSB har beställt och finansierat genomförandet av denna forskningsrapport. Författarna är ensamma ansvariga för rapportens innehåll.

Förord

Projektet DRISTIG har med finansiering av MSB under perioden mars 2016-september 2018 studerat olika aspekter av driftavbrott i samhällsviktiga it-tjänster. Projektet har syftat till att fylla kunskapsluckor och ta fram praktiskt relevant kunskap som kommer till nytta för att bedöma risker och minska konsekvenserna av it-driftavbrott.

Projektets resultat redovisas kortfattat i denna populärvetenskapliga sammanfattning. Litteraturlistan på slutet innehåller referenser till en del av de vetenskapliga artiklar som har publicerats under projektets gång. Ytterligare ett antal sådana artiklar genomgår i skrivande stund *peer review* och kommer att publiceras i sinom tid.

Projektet har berikats av samarbete med forskningsmiljöerna vid SINTEF i Trondheim, TTU i Tallinn och NTU i Singapore. Ett stort tack riktas till dessa partners, liksom till alla de informanter som på olika sätt bidragit till projektets resultat.

Ulrik Franke, projektledare

Innehållsförteckning

1. Vad är it-driftavbrott? 6
2. Vad kostar it-driftavbrott? 8
2.1 Transportföretag (11 st) 9
2.2 Livsmedelsföretag (9 st) 9
2.3 Statliga myndigheter (19 st) 10
2.4 Olika kostnadsstrukturer 10
2.5 Kostnadsstruktur och åtgärder 11
3. Hur kan man försäkra sig mot it-driftavbrott? 13
4. It-driftavbrott och avtal 15
4.1 Exempel: Detaljhandel 15
4.2 Checklista: Försäkring mot avbrott 16
5. Framtida utveckling 17
6. Mer läsning 18

Bilaga 1: Exempel på kostnadsuppskattning för it-driftavbrott. 19

Sammanfattning

Det moderna samhället är beroende av it-tjänster. Avbrott i dessa får stora konsekvenser. Eftersom it-tjänster i allmänhet är beroende av varandra beror avbrott inte sällan på problem med att hantera svåröverskådliga korsberoenden. Ett exempel är att omgivningen har ändrats – en tjänst slutar fungera för att en annan tjänst har uppdaterats och därmed har förändrats. Ett annat exempel är när ny mjukvara inte är tillräckligt testad innan den tas i drift. Att systematiskt testa alla tänkbara fel är oerhört svårt. Även om de allra flesta avbrott i it-tjänster är korta så förekommer det ibland långa avbrott. Det är lätt att underskatta hur långa avbrotten faktiskt kan vara, eftersom de längsta avbrotten förekommer så sällan.

It-avbrott medför typiskt både fasta och rörliga kostnader. De förstnämnda beror inte på avbrottets längd, medan de sistnämnde blir större ju längre avbrottet varar. En enkätundersökning med ett fyrtiotal olika verksamheter i såväl offentlig som privat sektor visar att olika verksamheter har olika kostnadsstrukturer vid avbrott. Vissa har nästan bara fasta kostnader, vissa har nästan bara rörliga. För den som ska vidta åtgärder mot driftavbrott är det viktigt att förstå sin egen kostnadsstruktur, eftersom den påverkar vilka åtgärder som är lämpliga.

Cyberförsäkringar har fått mycket uppmärksamhet på senare år. Förenklat består de av två huvudkomponenter: Dels en skadeförsäkringsdel som täcker exempelvis intäktsbortfall vid it-driftavbrott. Dels en ansvarsförsäkringsdel som täcker exempelvis kostnader vid skadeståndskrav från andra till följd av incidenter. I Sverige säljs cyberförsäkringar av ungefär ett dussin försäkringsbolag. Produkterna ser något olika ut beroende på om de är till för stora eller små företag. De årliga premierna ligger någonstans kring 0,5–1% av försäkringsbeloppet. Ett problem för alla försäkringsbolag är svårigheten att uppnå tillförlitlig riskspridning av cyberrisker.

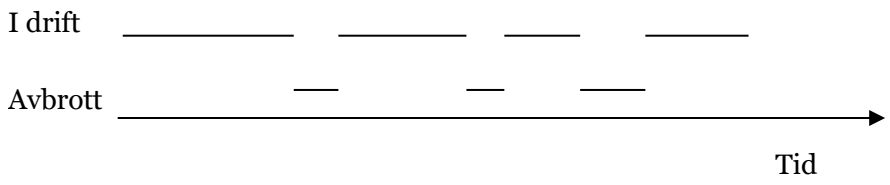
Beroendena mellan it-tjänster hanteras med hjälp av avtal, så kallade *Service Level Agreements* (SLA), som hjälper till att minska risker och upprätthålla kvalitet. Att teckna ett bra SLA är svårt och kräver bland annat god förståelse för verksamhetens behov och riskprofil, tydliga definitioner och en tydlig ansvarsfördelning mellan avtalsparterna. SLA och cyberförsäkringar kan i viss mån användas som komplement till varandra.

1. Vad är it-driftavbrott?

Det moderna samhället är helt beroende av it-tjänster för att fungera. De gör att vi idag arbetar, umgås och roar oss på sätt som hade varit helt främmande för bara tio år sedan. I mångt och mycket är det en positiv utveckling. Men det finns också baksidor. Att it-tjänster finns överallt gör oss också mer sårbara när dessa tjänster *inte* fungerar.

Viktiga it-tjänster finns spridda i hela samhället, i såväl privat som offentlig sektor. Livsmedels- och dricksvattenförsörjning, elektroniska kommunikationer, energiförsörjning, betalningssystem, transporter samt hälso- och sjukvård är några exempel på system som idag är beroende av fungerande it-tjänster – och som därför är känsliga för driftsstörningar.

Att en it-tjänst är tillgänglig (eng. *available*) definieras ofta som att den förmår utföra sin funktion vid en viss tidpunkt eller under ett visst tidsintervall. När tjänsten inte är tillgänglig får vi ett avbrott. Fig. 1 illustrerar hur en tjänst över tiden växlar mellan att fungera och ha avbrott.



Figur 1
Principskiss av hur en tjänst växlar mellan att fungera och ha driftavbrott över tiden.

Driftavbrott i it-tjänster kan leda till allt från fördröjda leveranser och kortare elavbrott till butikshyllor som gapar tomma och brist på allt från livsmedel till läkemedel. Det finns alltså all anledning att i det moderna samhället betrakta fungerande it som en kritisk infrastruktur.

Vad är det då som ”går sönder” vid ett driftavbrott? Svaret har varierat över tiden. I datorernas barndom var hårdvarufel vanligt förekommande och orsakade därför ofta avbrott. I takt med att hårdvaran har blivit mer alltmer tillförlitlig har dock hårdvarufel som bakomliggande orsak till avbrott blivit allt ovanligare. Någon gång på 1980-talet blev fel i mjukvara eller it-administration vanligare som orsaker till avbrott än fel i hårdvara.

Vad är då ett mjukvarufel? Mjukvara är en uppsättning instruktioner för vad en dator ska göra. Sådana instruktioner blir inte fysiskt utslitna på samma sätt som exempelvis kugghjul eller vattenledningar. Felen ser alltså annorlunda ut. Ett vanligt fel är att mjukvaran gör det den alltid har gjort, men att omgivningen har ändrats. En annan mjukvara kanske plötsligt använder ett nytt meddelandeformat, en kund kanske höjer sina säkerhetskrav eller ett årtal

som betecknas 00 kanske plötsligt följer på ett som betecknas 99. I takt med att allt fler it-tjänster levereras som komplicerade sammansättningar av flera olika tjänster, inte sällan från olika leverantörer, blir sådana fel både viktigare och svårare att hantera. Ett annat vanligt fel är att mjukvaran helt enkelt inte är tillräckligt testad innan den tas i drift. Trots att de flesta stora organisationer arbetar aktivt med omfattande automatiserade tester innan de tar nya versioner av mjukvara i drift så slinker det igenom fel. Ibland beror det på slarv eller tidspress, men det finns också en fundamental svårighet i att systematiskt testa de otroligt många tänkbara fel som kan uppstå i en modern it-tjänst.

Här finns också förklaringen till att man talar om bristande it-administration som orsak till avbrott. En välfungerande it-administration kan förstås som de processer utanför själva hård- och mjukvaran som är nödvändiga för att allt ska fungera. Det omfattar bland annat ändamålsenlig kravställning på de it-tjänster som utvecklas, systematisk testning av det som ska tas i drift, en process för ändringshantering som minimerar risken att olika ändringar krockar med varandra samt en fungerande driftövervakning som larmar när något ändå går fel. När it-administrationen brister i någon av dessa funktioner uppstår det ofta driftavbrott.

Det är viktigt att skilja på hanteringen av själva avbrottet och hanteringen av den underliggande orsaken. Om en mjukvaruuppdatering visar sig leda till ett driftavbrott så hanterar man oftast själva avbrottet genom att, mer eller mindre automatiserat, återgå till den senaste fungerande versionen, en s.k. *rollback*. Det sker typiskt på några sekunder, minuter eller timmar beroende på hur snabbt det upptäcks, hur viktig tjänsten är och hur komplicerad driftsmiljön är. Men när själva *avbrottet* på så sätt är hanterat återstår att hantera själva felet i uppdateringen. Att leta upp och rätta det kan ta timmar, dagar, veckor eller månader, återigen beroende på viktigt det bedöms och hur komplicerat det är. Avbrottshanteringen sker alltså på en helt annan och mycket snabbare tidsskala än felrättningen.

Tillgänglighet hos it-tjänster (och andra tekniska system) beskrivs ofta med hjälp av statistik över hur länge tjänsten i genomsnitt fungerar innan det blir avbrott (MTTF – eng. *mean time to failure*) och hur lång tid det i genomsnitt tar att avhjälpa ett sådant avbrott (MTTR – eng. *mean time to repair*). I Fig. 1 utgör genomsnittslängden hos de övre sträckorna MTTF och genomsnittslängden hos de undre MTTR. Genom att bilda en kvot av tid i drift (MTTF) genom totaltid (MTTF+MTTR) får man ett tillgänglighetsmått mellan 0 och 1. Oftast uttrycks detta i procent, t.ex. 99,98% tillgänglighet och liknande. Ibland talar man om antalet 'nior', där 99,9% är tre nior, 99,99% fyra nior och så vidare.

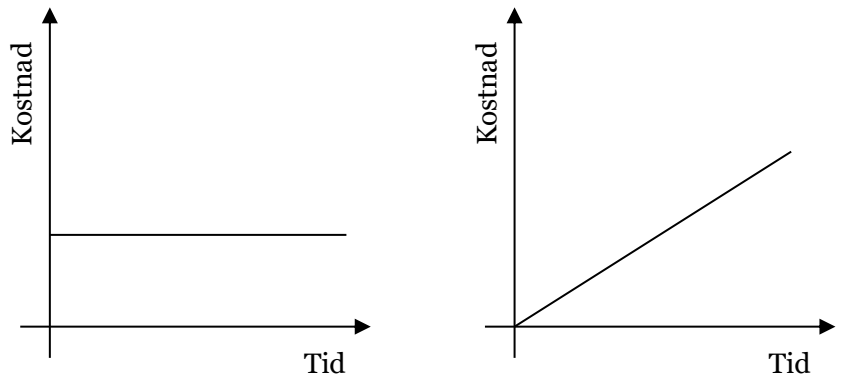
Ett viktigt resultat i forskningen är att även om de allra flesta avbrott är korta, så förekommer det då och då även längre avbrott. Det betyder i sin tur bland annat att det är lätt att underskatta hur långa avbrotten faktiskt kan vara, eftersom de längsta avbrotten förekommer så sällan.

2. Vad kostar it-driftavbrott?

En viktig aspekt av ett it-driftavbrott är dess *kostnad*. Även om kostnader inte är det enda som spelar roll ger kostnaderna ändå en bild av hur allvarligt ett avbrott är och en fingervisning om hur mycket resurser det är värt att lägga på att försöka undvika det.

En användbar distinktion när man ska analysera kostnader för it-driftavbrott är att skilja på *fasta* och *rörliga* kostnader. Fasta kostnader är sådana kostnader som inte växer eller krymper med storleken på det som kostar. För en restaurang är belysningen ett exempel på en fast kostnad – den kostar lika mycket oavsett om man har en eller tjugo gäster i lokalen. Råvarorna till köket däremot är en rörlig kostnad – fler gäster kräver mer mat.

För it-driftavbrott är det *längden* på avbrottet som varierar och kostnaden är fast eller rörlig med avseende på denna tid. Exempel på fasta kostnader för ett it-driftavbrott kan vara konsultkostnader, krishanteringskostnader och ny hårdvara. Exempel på rörliga kostnader för ett it-driftavbrott kan vara *förlorad produktivitet* för individer som inte kan utföra sitt arbete under avbrottet och *förlorade intäkter* i form av försäljning som inte kan ske under avbrottet. Fig. 2 illustrerar fasta och rörliga kostnader för avbrott. I det vänstra diagrammet är kostnaden densamma oavsett hur lång tid avbrottet pågår. Ett avbrott på en minut kostar lika mycket som ett avbrott på en timme. I det högra diagrammet växer däremot kostnaden med varje tidsenhet. Ett avbrott på en timme kostar sextio gånger mer än ett avbrott på en minut.



Figur 2
Principskiss av fasta (vänster) och rörliga (höger) kostnader för ett it-driftavbrott.

Projektet DRISTIG har vidareutvecklat en befintlig metod för att uppskatta kostnader för driftavbrott i it-tjänster. Grundtanken är att fånga både fasta och rörliga kostnader – de flesta avbrott ser inte ut *antingen* som det vänstra *eller* som det högra diagrammet i Fig. 2, utan har inslag av båda. Bilaga 1 illustrerar metoden och ger ett räkneexempel.

Kostnadsuppskattningsmetoden har inom projektet testats genom en enkät som besvarades av ett fyrtiotal olika verksamheter i såväl offentlig som privat sektor. Eftersom urvalet inte är slumpmässigt ska man vara försiktig med att dra alltför generella slutsatser av materialet. Istället bör man se underlaget som tre *fallstudier* av intressanta sektorer.

De tre sektorstudierna sammanfattas nedan i kortfattad punktform. Utöver de rena kostnadsfrågorna (bilaga 1) fick de svarande även uppge kostnadsdrivande faktorer och om avbrotten fick andra konsekvenser än kostnader.

2.1 Transportföretag (11 st)

- **Omsättning:** Tiotals eller hundratals miljoner kronor.
- **Kostnader för it-driftavbrott 2016:** Från tiotusentals till hundratusentals kronor, några miljoner kronor i ett fall, inga kostnader alls i ett fall.
- **Antal avbrott 2016:** Enstaka upp till något tiotal, tjugo i ett fall.
- **Totala avbrottstider 2016:** Enstaka upp till tiotals timmar, hundratals timmar i ett enstaka fall.
- **Kostnadsdrivande faktorer:** Typiskt spilltid för anställda och åtgärder för återställning. För de flesta förloras tiotals procent av intäkterna vid avbrott, men flera rapporterar att inga eller bara en mindre del av intäkterna uteblir vid avbrott.
- **Övriga konsekvenser:** Stress och övertid, försämrad ruttplanering för lastbilar, svårigheter att uppfylla åtaganden gentemot kunder, oro för icke-fungerande it, kunder som ej kan boka frakter och därmed kanske väljer konkurrenter istället.

2.2 Livsmedelsföretag (9 st)

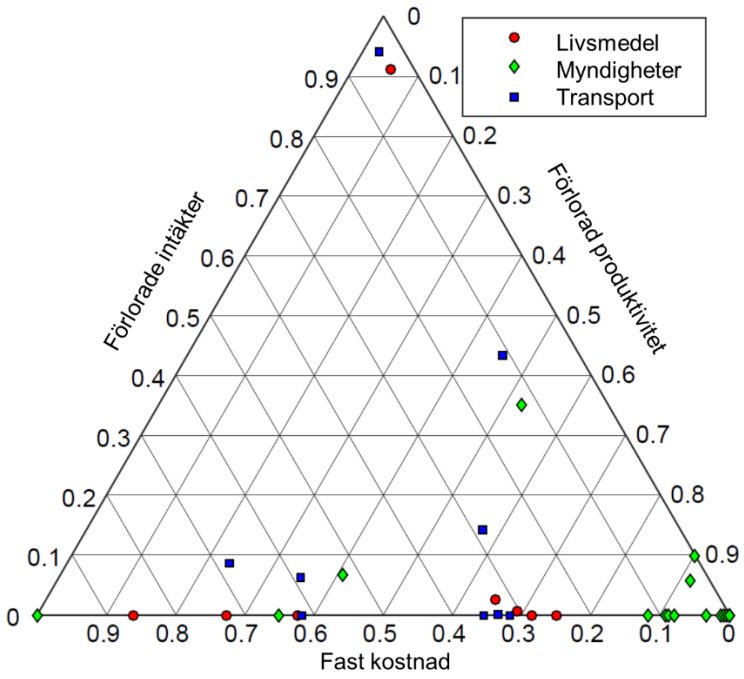
- **Omsättning:** Några hundra miljoner eller några miljarder kronor, i ett enstaka fall under hundra miljoner.
- **Kostnader för IT-driftavbrott 2016:** Från tiotusentals till hundratusentals kronor, inga kostnader alls i ett fall.
- **Antal avbrott 2016:** Enstaka upp till ett tiotal i ett enstaka fall.
- **Totala avbrottstider 2016:** Enstaka upp till tiotals timmar
- **Kostnadsdrivande faktorer:** Typiskt spilltid för anställda och åtgärder för återställning. De flesta rapporterar inga uteblivna intäkter, men enstaka rapporterar att samtliga intäkter uteblir vid avbrott.
- **Exempel på orsaker:** Kryptovirus, kraschad molnserver utan redundans.
- **Övriga konsekvenser:** Vissa avbrott märks ut till kunder som tappar förtroende, vissa märks bara internt och stressar anställda.

2.3 Statliga myndigheter (19 st)

- **Omsättning:** Några hundra miljoner eller några miljarder kronor, i ett enstaka fall tiotals miljarder.
- **Kostnader för IT-driftavbrott 2016:** Från tiotusentals, via hundratusentals, miljontals och upp till tiotals miljoner kronor. Inga kostnader alls i ett enstaka fall.
- **Antal avbrott 2016:** Från enstaka, via tiotals, till hundratals.
- **Totala avbrottstider 2016:** Från enstaka, via tiotals upp till hundratals timmar.
- **Kostnadsdrivande faktorer:** Typiskt spilltid för anställda och åtgärder för återställning, mera sällan uteblivna intäkter.
- **Exempel på orsaker:** Kryptovirus, strömavbrott, leverantörsbyte.
- **Övriga konsekvenser:** I vissa fall har medborgare fått vänta på service och tjänster, i andra fall har avbrotten inte märkts utåt. Stress bland de anställda och irriterade användare.

2.4 Olika kostnadsstrukturer

En viktig iakttagelse är att de olika verksamheterna och i viss mån de olika sektorerna har olika kostnadsstrukturer vid avbrott. Fig. 3 illustrerar fördelningen mellan tre olika kostnadskomponenter: (i) fast kostnad, (ii) förlorad produktivitet och (iii) förlorade intäkter.



Figur 3
Fördelning av avbrottskostnader på tre olika kostnadskomponenter.

Varje verksamhet motsvarar en markör i diagrammet och dess placering motsvarar kostnadsfördelningen för avbrotten. Exempelvis utgjordes avbrottskostnaderna för transportföretaget (□) som ligger ungefär halvvägs uppe i triangeln och något till höger till 11% av fasta kostnader, till 46% av förlorad produktivitet och till 43% av förlorade intäkter. Avbrottskostnaderna för livsmedelsföretaget (○) i triangelns topp utgjordes till 3% av fasta kostnader, till 5% av förlorad produktivitet och till 91% av förlorade intäkter. Som sista exempel utgjordes avbrottskostnaderna för myndigheten (◇) längst ner till vänster i triangelns bas till 100% av fasta kostnader.

Några intressanta iakttagelser kan göras i figuren. För det första finns det en samling myndigheter längst ner till höger vilkas kostnader vid avbrott nästan uteslutande består av förlorad produktivitet – anställda som inte kan arbeta vid avbrott. Däremot har de små eller inga intäktsbortfall eller fasta kostnader för återställning.

För det andra finns det ett stort antal verksamheter med små intäktsbortfall – den stora majoritet som återfinns i diagrammets nedre del.

För det tredje är de verksamheter som har högst andel intäktsbortfall vid avbrott (längst upp i triangelns topp) bägge privata företag.

Övergripande kan man säga att myndigheter i allmänhet knappt drabbas av intäktsbortfall vid driftavbrott. Det har naturligtvis att göra med att många myndigheter är anslagsfinansierade och att anslaget i statsbudgeten inte påverkas av avbrotten. Det finns dock undantag! För en av myndigheterna består 35% av kostnaderna för avbrott av intäktsbortfall.

2.5 Kostnadsstruktur och åtgärder

När är det värt att vidta åtgärder för att minska kostnaderna för avbrott?

Generellt kan man säga att det blir allt svårare och därmed allt dyrare att höja tillgängligheten ju bättre den redan är. Att gå från 99,0% till 99,1% är mycket enklare än att gå från 99,1% till 99,2%. Ju närmare man kommer det ouppnåeliga 100% (inga avbrott alls) desto svårare blir det. Det betyder också att det någonstans går en gräns för när det inte längre lönar sig att höja tillgängligheten. Det gäller oberoende av hur kostnadsstrukturen vid avbrott ser ut.

Om vi kort återvänder till Fig. 1 så kan vi se att det finns två principiellt olika sätt att öka tillgängligheten i en it-tjänst. Antingen så förlänger vi på något sätt tiden som tjänsten i genomsnitt fungerar innan det blir avbrott (MTTF) eller så förkortar vi något sätt tiden som tjänsten i genomsnitt tar att återställa (MTTR). Antingen så blir de övre sträckorna i figuren längre, eller så blir de undre kortare. Något annat sätt att öka tillgängligheten finns inte.

Ett intressant forskningsresultat, som gäller under vissa generella grund-antaganden, är följande: Vilket av de två sätten att öka tillgängligheten som man bör satsa på beror på hur kostnadsstrukturen vid avbrott ser ut. Om man bara har rörliga kostnader (som i diagrammet till höger i Fig. 2) så bör man fördela sin budget mellan att (i) förlänga MTTF och (ii) förkorta MTTR i

proportion till hur effektiva de är. Mer förvånande är kanske att om man bara har fasta kostnader (som i diagrammet till vänster i Fig. 2) så bör man satsa *hela* budgeten på att förlänga MTTF. Däremot finns det inget fall där man bör satsa allt på att förkorta MTTR. Det finns alltså en intressant asymmetri mellan de två typerna av åtgärder.

Ett sätt att förstå resultatet är följande: Om man bara har fasta kostnader så spelar det ingen roll hur långa avbrotten är. En minut eller en timme kostar lika mycket. Då finns det ingen anledning att satsa resurser på att korta reparationstiden ens det minsta lilla. Om man däremot bara har rörliga kostnader så medför varje minuts extra avbrott en extra kostnad. Om man bör undvika en minuts avbrott genom att tjänsten fungerar en minut längre innan den går sönder eller genom att den repareras en minut snabbare beror bara på vilken åtgärd som är billigast.

Naturligtvis är resultatet teoretiskt. Vi har redan konstaterat att de flesta verksamheter har inslag av både fasta och rörliga kostnader. Dessutom är det i praktiken ofta svårt att skilja åtgärder för att förlänga MTTF från åtgärder för att förkorta MTTR ifrån varandra, för att inte tala om att mäta exakt hur effektiva de är. Dessutom tar modellen inte hänsyn till aspekter som förtroende och popularitet hos kunder eller medborgare – ett avbrott kanske bara har fasta kostnader i ett kort tidsperspektiv, men om kunderna inte återvänder efter ett långt avbrott uppstår en rörlig kostnad i ett längre perspektiv.

Ändå är det en insikt som är nyttig även i praktiskt arbete. Det är bra att inse att olika typer av åtgärder är olika önskvärda för olika verksamheter. Fig. 3 visar att olika verksamheter faktiskt kan ha väldigt olika kostnadsprofiler vid avbrott. Det är klokt att låta detta vägleda de investeringar som görs i ökad tillgänglighet.

3. Hur kan man försäkra sig mot it-driftavbrott?

Ett verktyg för ökad säkerhet som har fått mycket uppmärksamhet på senare år är så kallade *cyberförsäkringar*. Lika lite som en hemförsäkring ersätter behovet av ett brandlarm eller en brandsläckare ersätter en cyberförsäkring behovet av andra säkerhetsåtgärder, men i båda fallen kan försäkringen utgöra ett bra och önskvärt komplement.

Något förenklat kan man säga att cyberförsäkringar består av två huvudkomponenter: en skadeförsäkringsdel och en ansvarsförsäkringsdel. *Skadeförsäkringsdelen* täcker exempelvis intäktsbortfall vid it-driftavbrott men även kostnader för återställning och utredning av incidenter, liksom eventuella advokat- och PR-kostnader. *Ansvarsförsäkringsdelen* täcker kostnader vid skadeståndskrav från andra till följd av incidenter, liksom kostnader för att exempelvis meddela alla berörda om dataförlust (exempelvis att meddela alla kunder om att uppgifter ur kundregistret har stulits). Utöver skade- och ansvarsförsäkringarna inkluderar de flesta cyberförsäkringar också en incidenthanteringstjänst, ofta i form av en jurist som tar koordineringsansvaret och kallar in de it-experter, jurister och PR-konsulter som kan behövas för att hantera en incident. Trots att incidenthanteringstjänsten inte är en försäkring i egentlig mening så ingår den nästan alltid och anses viktig av både försäkringsbolag och kunder.

Den svenska cyberförsäkringsmarknaden är fortfarande liten, men växer snabbt. Cyberförsäkringar säljs av ungefär ett dussin försäkringsbolag, varav de flesta är stora multinationella bolag. De säljer i sin tur ofta till storbolagskunder med omsättning på hundratals miljoner eller miljarder kronor. Eftersom typkunden är så pass stor har dessa försäkringsbolag sällan särskilt många kunder i Sverige: det rör sig om några tiotal per försäkringsbolag. Samtidigt finns det försäkringsbolag som vänder sig till ett annat kundsegment – små och medelstora företag med omsättning från enstaka miljoner kronor och uppåt. De årliga premierna på den svenska marknaden ligger någonstans kring 0,5–1% av försäkringsbeloppet, så skyddet kostar mellan fem och tiotusen kronor per miljon i försäkringsbelopp.

Försäkringarna för de olika kundsegmenten skiljer sig åt på flera sätt. En viktig skillnad är teckningsprocessen. I storbolagssegmentet använder kunden nästan alltid en försäkringsmäklare, som förmedlar information om den tilltänkta kunden till försäkringsbolagen och tar in offerterna. Den information som behövs är omfattande: utöver grunduppgifter om företagets storlek, bransch och internationella engagemang handlar det främst om mognaden i informations- och IT-säkerhetsarbetet. Denna bedöms dels med hjälp av omfattande frågeformulär, dels med hjälp av intervjuer där försäkringsbolaget träffar nyckelpersoner hos den tilltänkta kunden. Dessutom tar man ibland hjälp av ytterligare specialister, exempelvis it-revisorer som bedömer mognaden i arbetsprocesser och rutiner eller penetrationstestare som försöker

ta sig in i kundens system för att förstå hur säkra, eller osäkra, de är. Hela arbetet, med mäklararbete, informationsinsamling och offertframtagning tar inte sällan ungefär ett år. Kontrasten är slående i jämförelse med cyberförsäkringsprodukter som riktar sig till småbolag. Här liknar processen mer försäkringsförsäljning till privatpersoner. I de enklaste fallen matar man bara in företagets organisationsnummer för att få en prisuppgift.

Skillnaderna avspeglar de värden som står på spel. Att försäkra ett multinationellt bolag med omsättning på många miljarder kronor upp till ett försäkringsbelopp om kanske 100 miljoner vågar man inte göra hursomhelst. Det är högst begripligt att försäkringsbolagen vill göra en omfattande riskbedömning innan de vågar ingå ett sådant avtal. Processen har jämförts med aktivt förvaltade fonder, där förvaltaren inte köper vilka bolag som helst, utan letar upp dem man vill verkligen tror på och vill investera i.

Småbolagsmarknaden fungerar annorlunda. Att försäkra ett litet bolag med bara några miljoner kronor i omsättning upp till ett försäkringsbelopp om någon enstaka miljon är inte lika farligt. Strategin för de försäkringsbolag som huvudsakligen agerar i det här kundsegmentet är istället att försäkra så många små kunder som möjligt och räkna med att deras genomsnitt utgör en acceptabel risknivå. Själva försäkringarna är också mindre omfattande. Skydd mot incidenter som beror på sådana orsaker till avbrott som vi diskuterade i kapitel 1 snarare än på direkta angrepp utifrån täcks exempelvis ytterst sällan. Därigenom minskas försäkringsbolagens risk.

Frågan om riskernas storlek är central i diskussionen om cyberförsäkringar. Ett exempel kan hjälpa oss att förstå varför: Om ett försäkringsbolag försäkrar 100 hus på en och samma ö i Stockholms skärgård och inga andra så blir man väldigt känslig för olycksutfall. Oavsett om det är inbrott, stormar, översvämningar eller bränder som drabbar de försäkrade så är risken stor att många drabbas samtidigt och att försäkringsbolaget då får svårt att betala ut ersättning till alla på en gång. I praktiken arbetar därför alla försäkringsbolag med att sprida sina risker: om man försäkrar 100 hus på 100 olika platser så är risken mycket liten att många drabbas på en gång. Problemet är att det är mycket svårt att uppnå tillförlitlig riskspridning av cyberrisker.

Det är svårt av två skäl. För det första är många verksamheter beroende av *samma* it-tjänster och produkter. Nya säkerhetshål i operativsystemet Windows eller i TLS-krypteringen hos webbplatser slår mot många försäkringstagare på en gång, även om försäkringsbolaget har försökt att sprida riskera genom att försäkra bolag på olika platser och i olika branscher. För det andra är många verksamheter beroende av *varandra*. Ett driftstopp i en stor molntjänst drabbar alla dess kunder – som i sin tur kan återfinnas varsomhelst både geografiskt och verksamhetsmässigt.

De flesta är överens om att detta är viktiga svårigheter för cyberförsäkringar. Samtidigt finns det ett stort intresse av hur cyberförsäkringar – med brister och förtjänster – kan bidra till högre säkerhet och mer robusthet i samhället. Organisationer som OECD, World Economic Forum och EU:s myndighet för nätverks- och informationssäkerhet (ENISA) arbetar alla på policynivå med dessa frågor.

4. It-driftavbrott och avtal

Att it-tjänster i många verksamheter är beroende av varandra har vi redan berört i både kapitel 1 och 3. Dessa beroenden hanterar man efter bästa förmåga med hjälp av avtal. Sådana så kallade *Service Level Agreements* (SLA) innehåller ofta krav på exempelvis prestanda (som en svarstid på maximalt 100 millisekunder), tillgänglighet (som 99,98% av tiden) och underhållstider (som schemalagt underhåll mellan klockan 03 och 04 första tisdagen i månaden) för de tjänster som köps. Genom att ställa den här sortens krav på de tjänster som ens verksamhet är beroende av minskar man sin egen risk och bidrar till högre kvalitet i den egna verksamheten.

Ur ett avbrottsperspektiv är det viktigt att notera skillnaden mellan planerade och oplanerade avbrott. Planerade avbrott, till exempel för att ta ny mjukvara i drift, behöver man göra då och då i de flesta tjänster. Just eftersom de är planerade brukar de förläggas till sådana tidpunkter när tjänsten efterfrågas så lite som möjligt. Oplanerade avbrott däremot, som är vårt fokus här, kan inträffa lite närsomhelst. Ett ambitiöst SLA kan ändå ställa krav på hur de ska hanteras. Exempelvis kan man kräva att det bara får förekomma ett visst antal oplanerade avbrott under en avtalsperiod eller att återställning måste ske inom en viss tid. Sådana kvalitetskrav är återigen ett sätt att minska risken. För att säkra efterlevnaden kan man också inkludera vitesbelopp som ska betalas om leverantören inte lever upp till de ställda kraven.

Att teckna ett bra SLA är svårt. I korthet kan man säga att ett bra avtal kräver en god förståelse för verksamhetens behov och riskprofil, tydliga definitioner av nyckelbegrepp som ”tjänst”, ”fel”, ”underhåll” etc., tydliga beskrivningar av den aktuella it-miljön samt en tydlig ansvarsfördelning mellan avtalsparterna. Fallgroparna är många. Med otydliga definitioner får man kanske inte vad man ville ha. Med ett ofullständigt avtal fyller köplagen ut det som saknas – kanske med oönskade konsekvenser. Med stora viten kanske man missar chansen till ett välfungerande partnerskap med leverantören som hade kunnat uppnås med positiva istället för negativa incitament.

4.1 Exempel: Detaljhandel

Detaljhandeln är ett bra exempel som illustrerar både generella principer och konkreta praktiska problem.

Svenska butiker idag är nästan helt beroende av sina kortbetalningssystem. Kontantanvändningen har minskat kraftigt på senare år och nästan alla köp sker elektroniskt. Det faller sig alltså naturligt att ställa höga tillgänglighetskrav på kortbetalningssystemen. Men räcker det att kräva en procentsiffra som 99,9%? För en tjänst som ska vara tillgänglig 24 timmar om dygnet året om motsvarar 99,9% ungefär 9 timmars avbrott. Men hur fördelas dessa nio timmar? Det är stor skillnad på ett enda långt niotimmarsavbrott och hundra femminutersavbrott. För en butik kan ett niotimmarsavbrott vid fel tillfälle – som i julhandeln – äta upp hela årets vinst. Hundra femminutersavbrott

kanske knappt märks. Om butiken kunde så skulle man nog helst ställa krav på en kort återställningstid.

Vilka avtalsvillkor man kan få är emellertid en förhandlingsfråga. De stora kortbetalningstjänsteleverantörerna har standardavtal som knappast går att omförhandla. De gör sitt bästa för att hålla god tillgänglighet och de lyckas nästan alltid. Men man behöver inte gå längre än till medierapporteringen för att hitta ständigt nya exempel på kortare och längre avbrott i kortbetalningstjänster. Eftersom avtalen med kortbetalningstjänsteleverantörerna inte ger några bindande garantier och inte heller någon ersättning för uteblivna intäkter vid avbrott får butiksinnehavarna snarare teckna en försäkring om de vill minska sin risk.

4.2 Checklista: Försäkring mot avbrott

Projektet DRISTIG har som en liten fallstudie studerat just detta problem i skärningen mellan avtal och cyberförsäkring. Vilket skydd mot driftavbrott i kortbetalningstjänster kan man få om man tecknar en försäkring?

Det korta svaret är att man mycket väl kan få ersättning för intäktsbortfall, såsom beskrivs i kapitel 3. Som med andra försäkringar finns det ett högsta försäkringsbelopp. Det finns också självrisk: dels i form av ett belopp, dels i form av en väntetid innan försäkringen träder i kraft. Med en väntetid på exempelvis 8 timmar ersätts inget intäktsbortfall för avbrott som är kortare än så. Utöver dessa generella ramar så finns det dock ytterligare fyra aspekter i försäkringsvillkoren som är värda att titta närmare på:

- **Icke-antagonistiska incidenter** – händelser som inte beror på angrepp – täcks inte alltid. Som vi noterade i kapitel 3 gäller detta särskilt cyberförsäkringar riktade mot mindre bolag. I praktiken betyder det att försäkringen kan täcka ett avbrott orsakat av att någon hackar kortterminalen i butiken, men inte ett avbrott orsakat av en misslyckad mjukvaruuppdatering hos kortbetalningstjänsteleverantören.
- **Storskaliga fel i elförsörjning** eller annan infrastruktur såsom telekommunikation täcks aldrig av försäkringarna.
- **Avbrott hos kortbetalningstjänsteleverantören** undantas inte sällan eftersom detta anses vara externa tjänster som inte är en del av den försäkrade it-miljön. Här kan man som köpare behöva omförhandla villkoren, köpa tilläggstjänster eller byta försäkringsbolag för att få skydd. Vissa försäkringsbolag vill ha en lista på vilka externa tjänster man är beroende av för att de ska ingå i försäkringen, vilket ställer krav på god förståelse för kortbetalningstjänstens it-arkitektur.
- **Beräkningen av intäktsbortfallet** varierar mellan försäkringsbolagen. En viss beräkningsprincip kan vara att föredra framför en annan beroende på de egna omständigheterna.

5. Framtida utveckling

Samhället kommer knappast att bli mindre beroende av fungerande it-tjänster i framtiden. Det finns all anledning att tro att frågeställningarna om driftavbrott kommer att vara högst relevanta för lång tid framöver.

Av de resultat som projektet DRISTIG har levererat finns det två som är särskilt intressanta att utveckla vidare ur ett praktiskt perspektiv:

- **Metoden för att uppskatta kostnader** för driftavbrott i it-tjänster (kapitel 2 och bilaga 1) skulle kunna utvecklas ytterligare för att användas i exempelvis risk- och sårbarhetsanalyser. Sådana görs regelmässigt i många verksamheter. Välunderbyggda kostnadssiffror väger ofta tungt när risker ska kommuniceras.
- **Den kunskap om cyberförsäkringar** som har tagits fram kan användas i policyutveckling. Som framgår av kapitel 3 finns det ett stort internationellt intresse för hur cyberförsäkringar kan bidra till högre säkerhet och mer robusthet i samhället.

Ur ett vetenskapligt perspektiv finns det också flera intressanta framtida forskningsfrågor, exempelvis följande:

- **Systematiska kostnadsundersökningar** med hjälp av exempelvis SCB skulle kunna sprida mer ljus över kostnaderna för it-driftavbrott i Sverige. Den i projektet vidareutvecklade metoden kan utgöra grund.
- **Vilka risker som bör täckas av cyberförsäkringar** respektive vilka som bör täckas av andra försäkringar blir allt viktigare i takt med att samhällets it-beroende ökar. Hur ska gränserna dras? OECD bedömer att en oklar gränsdragning mot andra försäkringar hämmar användningen av cyberförsäkringar och det finns forskning som tyder på att kunderna känner sig osäkra på vad som egentligen täcks.
- **Vilka krav bör försäkringsgivare ställa** på de försäkrade? De flesta cyberförsäkringar idag innehåller grundläggande säkerhetskrav. Många har dessutom incitament där premien sänks om kunden vidtar vissa säkerhetsåtgärder. Men det är farligt om likartade krav gör alla försäkrade sårbara för samma sorts angrepp eller misstag. Kanske bör kraven vara på en annan nivå, exempelvis krav på kompetenser och befattningar i försäkringstagarens organisation?
- **Hur hanteras digitala risker** i små kunskapsintensiva företag? Idag genomgår vissa branscher en rask digitalisering. I exempelvis revisions- och juridikbranscherna övertas alltfler arbetsuppgifter av smarta algoritmer. Vad betyder det för företagets riskprofil? Hur kan man överblicka följdverkningarna av it-incidenter i dessa sammanhang? Går det att skydda sig med försäkringar eller smarta SLA?

6. Mer läsning

- Ross Anderson & Tyler Moore. The economics of information security. *Science*, 314(5799):610–613, 2006. DOI: 10.1126/science.1130992
- Martin Eling & Werner Schnell. What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance* 17(5), 474-491, 2016. DOI: 10.1108/JRF-09-2016-0122
- Ulrik Franke. Cyber insurance against electronic payment service outages. *14th International Workshop on Security and Trust Management*. Springer, 2018. Under tryckning.
- Ulrik Franke. The cyber insurance market in Sweden. *Computers & Security*, 68:130–144, 2017. DOI: 10.1016/j.cose.2017.04.010
- Ulrik Franke & Markus Buschle. Experimental evidence on decision-making in availability service level agreements. *IEEE Transactions on Network and Service Management*, 13(1):58–70, 2016. DOI: 10.1109/TNSM.2015.2510080
- Ulrik Franke. Availability of IS/IT. I Phillip A. Laplante (red.) *Encyclopedia of Information Systems and Technology*. CRC Press/Taylor & Francis, 2015. ISBN 9781466560772. DOI: 10.1081/E-EIST-120053881
- Ulrik Franke, Hannes Holm & Johan König. The distribution of time to recovery of enterprise IT services. *IEEE Transactions on Reliability*, 63(4):858–867, December 2014. DOI: 10.1109/TR.2014.2336051
- Ulrik Franke. Optimal IT Service Availability: Shorter Outages, or Fewer? *IEEE Transactions on Network and Service Management*, 9(1):22–33, March 2012. DOI: 10.1109/TNSM.2011.110811.110122
- OECD. *Enhancing the Role of Insurance in Cyber Risk Management*, 2017. DOI: 10.1787/9789264282148-en
- Per Håkon Meland, Inger Anne Tøndel & Bjørnar Solhaug. Mitigating risk with cyberinsurance. *IEEE Security & Privacy* 13(6):38-43, 2015. DOI: 10.1109/MSP.2015.137
- David A. Patterson. A simple way to estimate the cost of downtime. *Proc. 16th USENIX conference on System administration*, ss. 185–188, 2002.

Bilaga 1: Exempel på kostnadsuppskattning för it-driftavbrott

Genom att besvara följande frågor erhålls en uppskattning av de totala kostnaderna för it-driftavbrott under ett år.

Oplanerad it-nertid

Antal avbrott under året:
Exempel: 7

Antal timmar oplanerade IT-driftavbrott under året:
Exempel: De 7 avbrotten summerar till 235 timmar nertid

Fasta kostnader

Kostnad för återställning per avbrott (genomsnitt):
Exempel: Övertid, krishantering, extrauppgifter och konsultkostnader summerar till 10 000 kronor per avbrott

Rörliga kostnader

Timpris för en anställd inklusive sociala avgifter, exklusive overhead (genomsnitt):
Exempel: 250 kronor

Antal (ekvivalenter) anställda som påverkas av driftavbrott (genomsnitt):
Exempel: 5 anställda som inte kan göra något alls ger svaret 5. 10 anställda som kan jobba med halv produktivitet ger ekvivalenten 5. 5 anställda som inte kan göra något alls och 2 anställda som lämnade ordinarie verksamhet ger svaret 7.

Intäkter per timme (genomsnitt):
Exempel: 100 butiker som säljer för 10 000 kronor i timmen ger 1 000 000 kronor

Andel av intäkterna som påverkas av driftavbrott (genomsnitt):
Exempel: Om 100 butiker är lika stora och en enda butik drabbas av stopp i kassasystemet ger det 1 %

Summering

Uppskattad totalkostnad 2016 för IT-driftavbrott
*Exempel: 7 avbrott * 10 000 kronor per avbrott +*
*235 timmar * (250 kronor per anställd och timme * 5 anställda +*
*1 000 000 kronor per timme * 1% av intäkterna) =* ***2 713 750 kronor***

Myndigheten för samhällsskydd och beredskap
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB1281 – oktober 2018 ISBN 978-91-7383-877-1