FSPOS

Finansiella Sektorns Privat-
Offentliga Samverkan

Vägledning för robust elektronisk kommunikation inom finansiell sektor

FSPOS AG Kritisk Infrastruktur
Datum för publicering: 2012-11-29

Rapporten finns att ladda ner på www.fspos.se.

SAMMANFATTNING

Syftet med *Vägledning för robust elektronisk kommunikation inom finansiell sektor* är att tillhandahålla ett stöd till finansiella aktörer i kravställning vid anskaffning och förvaltning av elektronisk kommunikation. Genom denna vägledning erbjuds finansiella aktörer stöd i arbetet med analys av beroenden samt kravställning mot leverantörer, med målsättningen att öka robustheten i de samhällsviktiga finansiella tjänster som baseras på elektronisk kommunikation. Vägledningen är tänkt att kunna användas av den som är involverad i processen för anskaffning och förvaltning av elektronisk kommunikation.

Vägledningen är indelad i fyra avsnitt. Utöver en beskrivande text finns för respektive avsnitt en checklista som kan användas i det praktiska arbetet. Nedan beskrivs innehåll och kortfattade rekommendationer från varje avsnitt.

- **BEROENDEANALYS GENOM KONTINUITETSHANTERING**

  Kontinuitetshantering är ett sätt att analysera verksamheten och identifiera dess kritiska beroenden för att utifrån detta underlag kunna göra en medveten kravställning mot leverantörer.

  Syftet med kontinuitetshantering är att identifiera kritiska delar av verksamheten och därefter skapa och säkerställa robusthet i dessa delar, med målsättningen att säkra leveransförmågan. Sedan våren 2012 finns en internationell standard inom kontinuitetshantering (ISO 22301:2012), vilken används i denna vägledning som föreslagen metod. Ett systematiskt arbete med kontinuitetshantering gör det möjligt för organisationen att optimera sina investeringar i robusthet för elektronisk kommunikation.

- **ANSLUTNINGSFORMER**

  Det finns ett brett utbud av anslutningsformer, både fasta och trådlösa, för elektronisk kommunikation över internet. Den vanligaste anslutningsformen för aktörerna i den finansiella sektorn är fast anslutning via kabel.

  Samtliga anslutningsformer har för- och nackdelar och dessa måste vägas noga mot varandra vid val av anslutningsform. För att möjliggöra genomtänkta val krävs vidare noggranna analyser av anslutningsformerna i relation till det behov och användningsområde verksamheten har. Tack vare ett brett utbud av leverantörer av elektroniska kommunikationer har finansiella aktörer stora möjligheter att välja den/de leverantörer som bäst passar behoven.

  Viktigt att tänka på vid val av anslutningsform är bland annat att definiera antalet tjänster så tydligt som möjligt samt att beakta de typer av risker som finns för de olika anslutningsformerna. Därefter görs avvägningar för respektive tjänst, redundanskrav ställs och behov av flexibilitet definieras utifrån varje tjänsts behov.

ROBUSTHET

I detta avsnitt beskrivs olika sätt att ställa krav på leverantörens redundans, frågeställningar kring gränsdragning mellan kundens och leverantörens ansvar samt aktiviteter för att öka redundansen för att säkerställa robusthet. Med robusthet menas här förmågan att motstå störningar och avbrott samt förmågan att minimera konsekvenser om de ändå inträffar.

Lagen om elektronisk kommunikation (LEK) erbjuder visst stöd i kravställning mot leverantörer av elektronisk kommunikation, de finansiella aktörerna kan och bör dock gå längre i sin kravställning och i sina robusthetshöjande aktiviteter. Exempelvis bör krav på robust utrustning och skalskydd ställas på leverantörerna. De finansiella aktörerna bör också begära att få ta del av leverantörernas egna risk- och/eller kontinuitetsanalyser eller liknande samt ställa krav på regelbundna övningar, tester och revisioner.

Slutligen kan de finansiella aktörerna välja olika strategier för antal leverantörer och anslutningar (ex. flera anslutningar från en och samma leverantör eller flera anslutningar från flera olika leverantörer). Det viktigaste är att kravställa att anslutningarna inte har någon single-point-of-failure.

SERVICE OCH TILLGÄNGLIGHET

I detta avsnitt beskrivs parametrar som bör ses över för att säkerställa tillgängligheten i de tjänster som ska anskaffas och som ska täckas av avtalen. Med service menas i detta avsnitt de olika former och olika grad av leveransstöd som ges av leverantören. Tillgänglighet uttrycks i procent och innebär den grad till vilken beställaren kan förvänta sig att kunna använda en tjänst. Den del av leverantörsavtalet som specificerar servicenivå per tjänst och vilken service respektive servicenivå innehåller, benämns Service Level Agreement (SLA).

Det är rimligt att definiera olika servicenivåer för system/processer (baserat på deras prioritet hos beställaren) för att maximera nyttan av den tjänst som köps och för att undvika under- respektive överinvestering. Leverantörers erbjudanden innehåller ofta olika typer av servicenivåer, men dessa utgår inte ifrån någon universell standard och det är därför viktigt att göra jämförelser mellan olika leverantörers servicepaket.

Servicenivåer kan mätas enligt olika parametrar. Några av de vanligaste är tillgänglighet, maximalt antal fel, servicetid, åtgärdstider och kvalitet/prestanda. Viktigt att tänka på vid avtalsskrivning med leverantörer är att tydliggöra hur dessa parametrar definieras och mäts.

INNEHÅLLSFÖRTECKNING

1. INLEDNING

1.1 Bakgrund

Finansiella Sektorns Privat-Offentliga Samverkan (FSPOS) vision är att samhällsviktiga finansiella tjänster alltid fungerar. FSPOS inkluderar medlemmar från både offentlig och privat sektor och det löpande arbetet bedrivs i regel i mindre arbetsgrupper.

FSPOS Arbetsgrupp Kritisk Infrastruktur (AG KI) har i tidigare genomförda analyser identifierat att många finansiella aktörer upplevde ett behov av stöd vid kravställning gällande elektronisk kommunikation. Med utgångspunkt i detta har *Vägledning för robust elektronisk kommunikation inom finansiell sektor* tagits fram.

1.2 Syfte och mål

Syftet med denna vägledning är att tillhandahålla ett stöd till finansiella aktörer i kravställning vid anskaffning och förvaltning av elektronisk kommunikation. Vägledningen erbjuder stöd i genomförande av beroendeanalys för att skapa ett behovsunderlag, men ger också vägledning för val av anslutningsform samt för kravställning av tillgänglighet och service. Målsättningen är att öka robustheten i de samhällsviktiga finansiella tjänster som baseras på elektronisk kommunikation.

1.3 Målgrupp

Målgrupp för vägledningen är samtliga aktörer inom finansiella sektorn, såväl företag som myndigheter, stora som små. Vägledningen är tänkt att kunna användas av samtliga som är involverade i processen för anskaffning och förvaltning av elektronisk kommunikation. Vägledningen vänder sig således till exempelvis verksamhetsansvariga, säkerhetsansvariga, ansvariga för kontinuitetsarbete och genomförande av beroendeanalys, men även till de som ansvarar för upphandling av tjänster samt formulering av avtal. De olika avsnitten är utformade så att de kan läsas separat beroende på inom vilket område läsaren önskar vägledning.

Vägledningen täcker såväl anskaffning som förvaltning av tjänster och kan på så sätt användas både vid tecknande av nya avtal och vid översyn av befintliga.

1.4 Avgränsning

Vägledningen tar utgångspunkt i lagen om elektronisk kommunikation (2003:389), LEK, gällande definition av begreppet elektronisk kommunikation. LEK trädde i kraft 25 juli 2003 och ersatte telelagen och lagen om radiokommunikation. I LEK omfattas begreppet elektronisk kommunikation av alla typer av elektroniska kommunikationsnät som telenätet, internet och kabel-TV-nätet. I LEK anges inte närmare vilka tjänster eller nät som omfattas, utan de generella begreppen elektronisk kommunikationstjänst[1] och elektroniskt kommunikationsnät[2] används.

Vägledningen omfattar den elektroniska kommunikation som finansiella aktörer använder för att tillhandahålla finansiella tjänster. Även trådlösa anslutningsformer beskrivs i korthet.

Utgångspunkt för vägledningen är den infrastruktur inom elektronisk kommunikation som identifierats inom ramen för nulägesanalysen ”Riskbild Stockholm”, det vill säga den infrastruktur som krävs för att genomföra utvalda finansiella transaktioner:

- Avveckling i RIX
- Nettning i Dataclearingen
- Köp med bankkort
- Bekräftelse om utförd avveckling till utländsk bank
- ATM-uttag
- Köporder för värdepappershandel

Urvalet av transaktioner gjordes av FSPOS Arbetsgrupp Betalningsförmedling (AG Betalning)[3], och utgångspunkten var att transaktionsflödena skulle vara viktiga ur ett kundperspektiv samt att de skulle skildra olika typer av flöden mellan olika aktörer i sektorn.

Denna vägledning behandlar elektronisk kommunikation över internet. Elektronisk kommunikation via telenätet inkluderas endast i de fall då dessa nät används för åtkomst till internet. Såväl trådbunden (koppar och fiber) som mobil kommunikation inkluderas. Det finns ett antal olika accessformer till både trådbunden och mobil kommunikation, dessa beskrivs mer i detalj i avsnitt 3. *Anslutningsformer*.

---

1 En elektronisk kommunikationstjänst definieras i LEK som en tjänst som vanligen tillhandahålls mot ersättning och som helt eller huvudsakligen utgörs av överföring av signaler i elektroniska kommunikationsnät (7 § 6 st.).

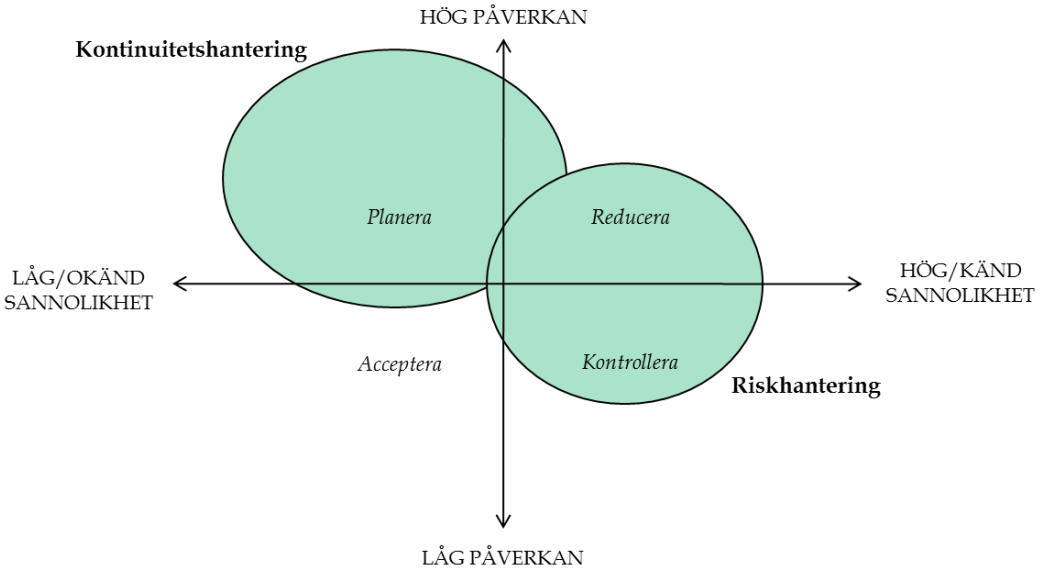
2 Elektroniska kommunikationsnät definieras i LEK som ett system för överföring och i tillämpliga fall utrustning för koppling eller dirigering samt andra resurser som medger överföring av signaler, via tråd eller radiovågor, på optisk väg eller via andra elektromagnetiska överföringsmedier oberoende av vilken typ av information som överförs (7 § 7st.).

3 Svenska Betalningsflöden – Så funkar det, FSPOS AG Betalningsförmedling

2. BEROENDEANALYS GENOM KONTINUITETSHANTERING

För att kunna göra en medveten kravställning mot leverantörer är det viktigt att ha kunskap om verksamhetens behov och hur beroendet till elektronisk kommunikation ser ut. Ett sätt att analysera verksamheten och identifiera dess kritiska beroenden är att använda metodiken för kontinuitetshantering. Detta avsnitt ger en introduktion till kontinuitetshantering och hur det kan kopplas till kravställning gällande elektronisk kommunikation. För en djupare kunskap finns även en steg-för-steg-beskrivning av processen för kontinuitetshantering i bilaga A.

Traditionell riskhantering fokuserar normalt på kända hot vilket gör att händelser med låg eller okänd sannolikhet tenderar att förbises. Kontinuitetshantering utgår ifrån det som är skyddsvärt (istället för hotet/orsaken) och analyserar sedan vilka åtgärder som behöver vidtas för att säkerställa robusthet hos det skyddsvärda, t.ex. ett kritiskt system eller en server. Genom detta synsätt kan även okända hot hanteras bättre, se figur 1 nedan.



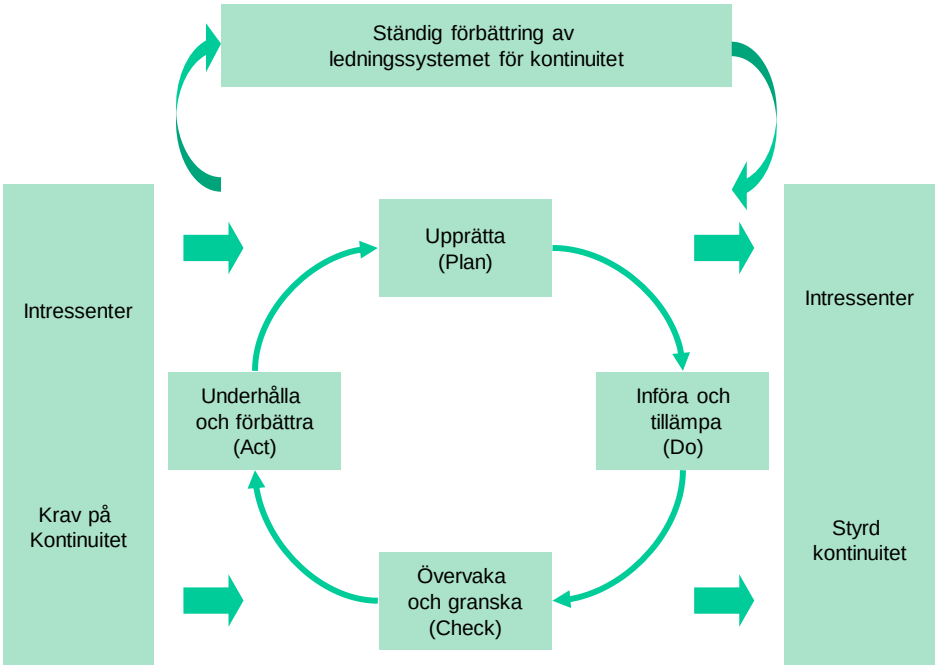
Figur 1: Fokusområden för riskhantering och kontinuitetshantering[4]

En nyckel till ett framgångsrikt arbete med kontinuitetshantering är att säkerställa lämplig organisation, processer, system och kultur för kontinuitetshantering. Det kan exempelvis handla om att säkerställa att personer med rätt kompetens, t.ex. kontinuitetsmetodik, IT och avtalsskrivning, involveras i arbetet.

4 Good Practice Guidelines, Business Continuity Institute

2.1 Syftet med kontinuitetshantering

Syftet med kontinuitetshantering är att identifiera kritiska delar av verksamheten och därefter skapa och säkerställa robusthet i dessa delar, med målsättningen att säkra leveransförmågan. Det finns ett antal modeller och verktyg som kan användas som stöd för en organisations kontinuitetshantering, sedan våren 2012 finns även en internationell standard; *ISO 22301:2012 - Societal security - Business continuity management systems (ISO 22301)*. I bilaga A, *Processen för kontinuitetshantering*, beskrivs processen för kontinuitetshantering steg-för steg, med utgångspunkt i den process och de begrepp som används i ISO-standarden.



Figur 2: PDCA[5]-cykel för kontinuitetshantering enligt ISO 22301

2.2 Kostnad-Nyttoanalys

Ett systematiskt arbete med kontinuitetshantering gör det möjligt för organisationen att optimera sina investeringar i robusthet för den affärskritiska verksamheten. En systematisk analys av de affärskritiska processerna och de aktiviteter och resurser som de är beroende av kan identifiera redundans- och säkerhetsbrister. En sådan analys kan även identifiera resurser där redundansen är oproportionerligt hög jämfört med hur kritiska de är för verksamheten. Kontinuitetshantering möjliggör att insatser för ökad robusthet optimeras mot bakgrund av vad som är affärskritiskt för verksamheten.

---

5 Plan, Do, Check, Act (PDCA)

Samtliga identifierade kontinuitetslösningar bör utvärderas mot bakgrund av hur kostnadseffektiva de är.

Bedömningen kan göras genom att jämföra lösningens reducering av återhämtningskostnad[6] med den totala investeringskostnaden för lösningen. På detta sätt kan ett ROI-värde (return on investment) beräknas, vilket ger ett bra beslutsunderlag för att prioritera identifierade kontinuitetslösningar. När det gäller händelser som har en mycket låg sannolikhet bör ROI-värdet ses som ett sätt att värdera alternativa lösningar jämfört med varandra, och inte tolkas bokstavligen.

Genom att arbeta systematiskt med kontinuitetshantering kan kontinuitet säkerställas i de affärskritiska processerna. Arbetet ger även fördelar i form av:[7]

- **TRYGGHET** – ett systemetiskt tillvägagångssätt minskar risken för att missa viktiga detaljer
- **EFFEKTIVITET** – investeringar i säkerhet och kontinuitet optimeras i förhållande till hur viktig en process är för verksamheten i stort
- **TRANSPARENS** – ledningen tvingas fatta beslut och kommunicera organisationens riskbenägenhet, det vill säga viljan att ta risker
- **ANSVAR** – genom ett strukturerat arbete tydliggörs avsvaret för kritiska delar av verksamheten

6 Reduktionen i kostnaden för ett avbrott, från det att avbrottet inträffar till dess att full normal verksamhet är återtagen tack vare kontinuitetslösningen.

7 Kontinuitetsplanering – en introduktion, MSB

3. ANSLUTNINGSFORMER

Det finns ett brett utbud av anslutningsformer, både fasta och trådlösa, för elektronisk kommunikation över internet. För att möjliggöra väl genomtänkta val krävs noggranna analyser av dessa anslutningsformer i relation till det behov och användningsområde man har. I detta avsnitt beskrivs olika anslutningsformer, för- och nackdelar med de olika alternativen samt stöd vid val av leverantör.

Det finns ett stort antal anslutningsformer för elektronisk kommunikation att välja mellan. Anslutningsformerna möjliggör olika typer av elektronisk kommunikation såsom telefonitjänster, meddelandehantering och internetåtkomst. I denna vägledning är avgränsningen den elektroniska kommunikation som finansiella aktörer använder för att tillhandahålla finansiella tjänster (se avsnitt *1.4 Avgränsning*). Dessa anslutningsformer behandlas i detta kapitel.

3.1 Anslutningsformer

Den finansiella sektorn har under lång tid arbetat med robusthet i internetanvändning och säkra internetanslutningar. Vanligaste anslutningsformen är fast anslutning, exempelvis fiber (vanligast) eller kabel, de flesta aktörerna har dock utöver detta även mobil anslutning.[8]

Uppringda anslutningsformer

En uppringd anslutning möjliggörs genom uppringning (dial-up) till internetleverantör via modem och det publika telefonnätets ledningar. Dial-up är den mest långsamma typen av internetanslutning men fungerar om avsikten endast är att skicka lite information. Anslutningsformen begränsar också användandet av den telefonlinje som används för uppringningen.

Fasta anslutningsformer

xDSL

xDSL är en samling av tekniker för överföring av stora mängder data över telefonledningar av koppar. Vilken typ av teknik som används för överföringen av information framgår av den bokstav som ersätter x.[9] Vid användning av xDSL-anslutning kan vanlig telefon fortfarande användas, till skillnad från en uppringd anslutning via ett analogt modem. För anslutningen krävs dels ett xDSL-modem och dels att den lokala telefonstationen är förberedd för tjänsten. I Sverige erbjuder idag flera operatörer xDSL till slutkund.

---

8 www.scb.se (Företagens användning av IT 2011)

9 Exempel på beteckningar: ADSL = Asymmetric Digital Subscriber Line, SDSL = Symmetric Digital Subscriber Line, HDSL = High-data-rate Digital Subscriber Line, VDSL = Very high-rate Digital Subscriber Line

xDSL-förbindelsen är på korta avstånd betydligt snabbare än förbindelser med analoga modem. Kopparledningens bandbredd sjunker dock snabbt med avstånd vilket gör att xDSL endast kan användas över korta distanser.

Optisk fiber

I över 30 år har optisk fiber använts för att transportera information, men det är först under 2000-talet det kommit i allmänt bruk och erbjudits till privatpersoner och organisationer för snabba internetanslutningar. Själva fibern har en kärna av glasfiber som kan transportera ljusimpulser med data.[10]

Fiberoptiskt nät är idag i särklass den snabbaste tekniken för överföring av data. Andra fördelar med fiber är att den kan transportera enorma mängder information. Två stycken optiska fibrer kan transportera samma informationsmängd som hela Sveriges kopparnät gör idag. Fiber ses därför som en framtidssäker lösning eftersom kapaciteten (åtminstone i dagens mått mätt) är nästintill obegränsad. Fibern är inte heller beroende av avstånd utan kvaliteten på informationen som överförs via nätet är densamma överallt. En annan fördel med fiber är att den inte avger något elektromagnetiskt fält vilket gör att den är okänslig för åska och svår att avlyssna.[11] Majoriteten av de finansiella aktörerna använder denna typ av anslutning.

Till skillnad från exempelvis xDSL kräver fiberanslutningar att ny infrastruktur byggs (fiberkablar dras). Fibernätet i till exempel Stockholm är redan idag väl utbyggt och under fortsatt utveckling och utbyggnad av nätägarna, där den största aktören är Stokab. Stokabs nät är operatörsneutralt vilket innebär att Stokab hyr ut fiberförbindelser till operatörer och tjänsteleverantörer till företag och offentlig verksamhet.[12]

Trådlösa anslutningsformer

Användningen av trådlösa förbindelser som anslutningsform ökar snabbt. Mobila anslutningsformer använder radiovågor och det finns olika tekniker för detta; 2G, 3G och nu 4G. År 1991 lanserades 2G-nätet (det så kallade GSM-nätet), vilket erbjöd hastigheter upp till 53,6 Kbit/sek. År 2001 lanserades 3G-nätet (främst anslutning via teknikerna HSPA eller CDMA) vilket erbjuder hastigheter upp till 25 Mbit/sek. 4G-nätet är i Sverige under uppbyggnad och syftet är att göra mobilt bredband (främst via LTE-teknik) mycket snabbare och stabilare. Hastigheter på uppemot 100 Mbit/sek kan uppmätas och med framtida 4G-nät beräknas hastigheten öka ytterligare. Generellt har trådlösa anslutningsformer lägre hastigheter än fasta.

---

10 www.skanova.se (Om fiber)
11 www.skanova.se (Om fiber)
12 www.stokab.se (Stokabmodellen)

Två olika tekniker för 4G-anslutning finns i dagsläget; WiMax och LTE. WiMax erbjuds endast lokalt och har därmed relativt låg täckningsgrad och nyttjandegrad.[13]

ATT TÄNKA PÅ I AVTAL:

- Välj anslutningsform utifrån användningsområde och dess krav
- Säkerställ att leverantörens mobila täckning är tillräcklig för de platser där organisationen är verksam

Regelbunden förändring och utveckling av anslutningsformer

Utvecklingen av olika anslutningsformer går snabbt och det är svårt att skapa en heltäckande och ständigt aktuell lista. En snabb och pålitlig anslutning krävs för samtliga aktörer på den finansiella marknaden. Ovanstående anslutningsformer är de som främst används i dagsläget, men nya alternativ utvecklas.

Nuvarande telenät, bestående av kopplarkablar (vissa så gamla som från 30-talet) är utnyttjat till vad dagens tekniska utveckling tillåter. Nätet blir dessutom stegvis svagare eftersom många förbindelser kopplas bort på grund av åldersskador. Rent tekniskt går det inte att få ut mer kapacitet än vad som görs med dagens xDSL. Kopparkabel har länge varit den huvudsakliga anslutningsformen, men optisk fiber har många fördelar och har till stor del tagit över marknaden/är på väg att ta över som det mest utbredda alternativet. Nätet av kopparkablar kommer inte heller att bytas ut i takt med att det åldras utan snarare ersättas av andra, snabbare, lösningar, såsom fiber och/eller trådlösa lösningar.[14] Regeringens mål är att år 2020 ska 90 % av alla företag och hushåll ha tillgång till bredband om minst 100 Mbit/sek. Detta kräver en utbyggnad av fasta (fiberbaserade och kabel-TV-nät) och mobila nät. För de mobila näten krävs utbyggnad med ny teknik.[15]

DNS

DNS (domännamnsystemet) är en funktion i internets infrastruktur. Det är en globalt distribuerad databas av poster med domännamn vilka är kopplade till en eller flera IP-adresser med lagring i miljontals servrar.[16] Det är DNS som gör att datorer kan hitta till varandra på internet genom att alla utrustningar anslutna till internet identifieras med hjälp av en unik IP-adress.

---

13 www.pts.se (Mobilt bredband)
14 www.fibert.se (Varför fiber?)
15 Bredbandsstrategi för Sverige, Näringsdepartementet
16 Robust Elektronisk Kommunikation – vägledning för användare vid anskaffning, PTS

För att vara säker på att man dirigeras till den korrekta IP-adressen för den förväntade servern bör man se till att ställa krav på stöd för DNSSEC (DNS Security Extensions) som är en standardiserad metod för att hantera detta.

ATT TÄNKA PÅ I AVTAL:

- Vid intern drift av namnservrar, tillse att drift av en del sekundära namnservrar driftas hos en eller flera externa DNS-operatörer
- Tillse att namnservrar är placerade i olika internetoperatörers nät
- Ställ krav på stöd för DNSSEC

3.2 Strategi vid val av anslutningsform

Olika anslutningsformer innebär olika nivåer av risktagande. Vid fasta anslutningar är man exponerad för risker under längre tid och inkräktare kan därmed få möjlighet att ladda ned större mängd filer. Vidare är en dator med fast anslutning mer attraktiv att göra intrång i för att via den kunna utföra vidare attacker. [17] Trådbundna anslutningar kan till stor del skyddas genom fysiska hinder, exempelvis brandväggar.

Säkerhetsrisker vid trådlös anslutning är generellt sett större än vid fast anslutning. I trådlösa nätverk finns i princip inga fysiska hinder för att en obehörig angripare ska kunna ta sig in på nätverket.[18] Här måste man istället använda sig av säkerhet i mjukvaror och de tjänster som används, exempelvis genom krypterings- och autentiseringslösningar.

Genom att kartlägga verksamhetens kritiska arbetsprocesser och tjänster och analysera hur beroende till olika typer av elektronisk kommunikation ser ut (exempelvis enligt metod beskriven i bilaga *A. Processen för kontinuitetshantering*) skapas en grund för valet av leverantör(er) och anslutningsform(er). Tack vare det breda utbudet av leverantörer av elektroniska kommunikationer har de finansiella aktörerna stora möjligheter att välja den/de leverantörer som bäst passar behoven och också ställa relevanta krav på olika nivåer på robusthet.

ATT TÄNKA PÅ I AVTAL:

- Definiera antalet tjänster så tydligt som möjligt
- Beakta de typer av risker som olika tjänster medför och gör en avvägning vid val av tjänst
- Ställ krav på redundans utifrån varje tjänsts behov samt definiera behov av flexibilitet för respektive tjänst

17 www.pts.se (Anslutningsformer)
18 www.pts.se (Anslutningsformer)

4. ROBUSTHET

Detta kapitel beskriver olika sätt att ställa krav på leverantörens redundans. Här beskrivs även frågeställningar kring gränsdragning mellan kundens och leverantörens ansvar samt aktiviteter för att öka redundansen för att säkerställa utlovad robusthet såsom krav på gemensamma övningar.

Vissa tjänster är mer utsatta och sårbara för hot och risker. Det kan gälla såväl fysiska som logiska delar av tjänster och dessas infrastruktur. Som ett resultat av genomförd beroendeanalys kan också ett antal tjänster/processer identifieras som mer kritiska än andra för verksamhetens funktion.

För ovanstående tjänster är det viktigt att ställa särskilda krav på robusthet. Med robusthet menas här förmågan att motstå störningar och avbrott samt förmågan att minimera konsekvenser om de ändå inträffar.

4.1 Leverantörers redundans

Liksom den finansiella sektorns intressenter ställer krav på en robust leverans av finansiella tjänster, bör också aktörerna i den finansiella sektorn ställa krav på robusthet i leveransen av kritisk infrastruktur, såsom elektronisk kommunikation.

Leverantörer av elektronisk kommunikation är bundna enligt lag (LEK, 5 kap, 6b §) att *"vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att verksamheten uppfyller rimliga krav på driftsäkerhet. De åtgärder som vidtas ska vara ägnade att skapa en säkerhetsnivå som, med beaktande av tillgänglig teknik och kostnaderna för att genomföra åtgärderna, är anpassad till risken för störningar och avbrott"*. Lagen erbjuder dock inte stöd i hur robustheten kan mätas eller ställer krav på olika nivåer av robusthet. Som leverantör av samhällsviktiga tjänster bör den finansiella sektorn därför ställa specifika krav på robusthet till sina leverantörer av elektronisk kommunikation.

4.2 Ansvarsfördelning

LEK reglerar det ansvar och de skyldigheter leverantörer av elektronisk kommunikation har. Syftet med lagen är att *enskilda och myndigheter skall få tillgång till säkra och effektiva elektroniska kommunikationer (*LEK 1 kap. 1§).

För att leverantörerna ska kunna upprätthålla robusthet i sina tjänster och därmed kunna leverera det de åtagit sig att leverera krävs dock också att de finansiella aktörerna själva förbinder sig att bland annat:

- utse kontaktpersoner och ange kontaktinformation till dessa
- ge tillträde till lokaler när detta behov finns

- säkerställa tillräckligt skydd för utrustning i egna lokaler, exempelvis genom brandskydd[19] och begränsad åtkomst för obehöriga
- informera leverantörer om händelser som kan påverka tjänsten

Post- och telestyrelsen (PTS), som är tillsynsmyndighet för LEK, skall ha tillsyn över efterlevnaden av lagen och har rätt att få tillträde till områden där verksamhet som omfattas av LEK bedrivs. Skulle PTS finna skäl att misstänka att lagen inte efterlevs skall myndigheten underrätta den som bedriver verksamheten om detta och ge denne möjlighet att yttra sig. Följs inte detta får leverantören ett föreläggande eller förbud att leverera tjänsten.

ATT TÄNKA PÅ I AVTAL:

- Använd LEK som stöd och inspiration vid organisationens egen kravställning inom redundans och tillhandahållande av uppgifter
- Använd LEK som stöd och inspiration vid kravställning på leverantörerna avseende redundans och tillhandahållande av uppgifter

4.3 Aktiviteter för ökad redundans

För att öka redundansen på leveransen av elektroniska kommunikationer kan, och bör, aktörerna på den finansiella marknaden ställa krav på sina leverantörer. Samarbete/dialog med leverantörer kan ske på flera olika nivåer: strategisk, taktisk och operativ. Nedan följer förslag på områden att kravställa inom.

Krav på robust utrustning och skalskydd

Ett av de viktigaste kraven är att leverantörer av elektronisk kommunikation garanterar robusthet och hög kvalitet på utrustning och service av denna, exempelvis genom regelbunden service av utrustning och skydd av serverhallar. Krav bör också ställas på att redundant utrustning finns, exempelvis alternativt driftställe med speglad server och redundant ledningsnät.

19 Lagen (2003:778) om skydd mot olyckor

ATT TÄNKA PÅ I AVTAL:

- Ställ krav på att leverantören garanterar regelbunden service av utrustning och skydd av serverhallar.
- Ställ krav på att redundant utrustning finns, exempel alternativt driftsställe med speglad server, redundant ledningsnät och reservkraft.

Flera aktörer hanterar inte sitt eget driftsställe utan har outsourcat funktionen till en eller flera leverantörer. En avvägning här är hur långt tillbaka i leverantörskedjan som de finansiella aktörerna kan ställa krav. I dessa fall ställs vanligtvis krav på att leverantörerna ska ha höga SLA-nivåer gentemot sina leverantörer för att kunna garantera leverans i så stor utsträckning som möjligt. Snarare än att ställa krav på leverantörernas leverantörer regleras robusthet och redundans genom avtal med den egna leverantören där påföljder för misslyckande att leverera utlovad tjänst beskrivs (se mer under avsnitt *5. Service och tillgänglighet*).

Krav på IP- adresser

Antalet IP-adresser av den adresseringsstandard som används idag, IPv4, är på väg att ta slut. Därför har IPv6 utvecklats och är den senaste versionen av IP-adresser. IPv4 och IPv6 kan inte kommunicera med varandra och organisationer behöver därför ställa krav på att leverantören även kan erbjuda stöd för IPv6.[20]

Användning av molntjänster

Molntjänster, s.k. Cloud Computing, möjliggör användning av serverbaserade applikationer över internet.[21] En typ av molntjänst kallas Software as a service (SaaS). Normalt ansvarar en organisation själv för installation och drift av sina applikationer på en egen server. Med denna typ av molntjänst outsourcas detta till en leverantör som istället installerar applikationen på sina servrar och därmed står för drift och underhåll. Molntjänster föredras av många organisationer på grund av skalbarhet och effektivitet, medan det för andra organisationer är olämpligt på grund av exempelvis krav på tillgänglighet, integritet och konfidentialitet.

20 www.pts.se (Robust kommunikation)
21 Robust Elektronisk Kommunikation – vägledning för användare vid anskaffning, PTS

ATT TÄNKA PÅ I AVTAL:

- Säkerställ prestanda och tillgänglighet på förbindelsen till leverantörens datacenter
- Säkerställ redundans och robusthet för molntjänstleverantörens servrar
- Ställ krav på skydd av konfidentiell och hemlig information

Delgivning av analyser

Det får antas att samtliga leverantörer av elektronisk kommunikation regelbundet följer upp och analyserar sitt risk- och säkerhetsarbete. De finansiella aktörerna bör begära att få ta del av dessa sammanställningar, vanligtvis i form av resultat av leverantörens riskanalyser, revision av kontinuitetshanteringsarbetet eller liknande. På detta sätt kan de finansiella aktörerna aktivt påverka sina leverantörer inom områden där riskarbetet inte är tillräckligt.

De finansiella aktörerna bör också kravställa att leverantören regelbundet delger en skriftlig beskrivning av hur de hanterar säkerhetsarbetet i enlighet med de krav som ställts på leverans av respektive tjänst.

Sektorsmyndigheten PTS genomför årligen en risk- och sårbarhetsanalys för hela sektorn elektronisk kommunikation. Denna rapport är också relevant ur ett kravställningsperspektiv eftersom de finansiella aktörerna bör begära att leverantörerna aktivt följer upp analysen och i möjlig mån åtgärdar identifierade sårbarheter.

Övningar, tester och revision

Att lära genom egna erfarenheter är värdefullt och genom övningar och tester kan avtal och reservlösningar prövas. Aktörerna inom den finansiella sektorn bör ställa krav på att leverantörer av elektronisk kommunikation regelbundet genomför övningar, tester och revision av sina system. Övningar, tester och revision kan genomföras på flera olika nivåer, bland annat genom:

- Övning av personal för att säkerställa kompetens och öka erfarenheter

- Skarpa tester för att testa leverantörens kritiska system, processer och beroenden och utröna hur länge leverantören kan klara sig utan dessa utan att det påverkar de finansiella aktörerna i större omfattning. Detta kan göras till exempel genom test av alternativt driftställe samtidigt som ordinarie verksamhet fortgår på ordinarie plats eller genom test av reservkraft för att säkerställa att diesel räcker enligt utlovat

- Genomgång av checklistor och rutiner
- Revision genomförd av den egna organisationen eller av tredje part

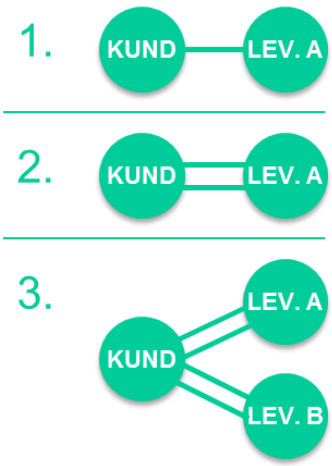
De finansiella aktörerna kan också ställa krav på att gemensamma övningar ska genomföras, det vill säga övningar där både finansiella aktörer och leverantörer av elektronisk kommunikation deltar. Detta för att testa bland annat samverkan, kommunikationsvägar och informationsspridning. Vidare bör de finansiella aktörerna ställa krav på att leverantörerna av elektronisk kommunikation deltar vid de stora, sektorsgemensamma övningar som anordnas, bland annat FSKLÖ (anordnas av FSPOS), Telö (anordnas av PTS) och Samö (anordnas av MSB). Krav kan ställas på att beställare får genomföra revisioner av leverantörens system, processer, rutiner, eller leverantörens uppfyllnad av andra delar av avtalet. En sådan revision kan antingen genomföras av beställaren eller av en tredje part som är betrodd av både leverantören och beställaren.

Användning av redundanta anslutningar

Det finns flera olika strategier för val av anslutning. Det är hos aktörerna i den finansiella sektorn lika vanligt att välja flera leverantörer för en och samma tjänst, som att välja endast en leverantör.[22] Om man, i tron att man skapar sig en redundant lösning, väljer att köpa samma tjänst från två olika leverantörer riskerar man att ledningarna går i samma tunnlar. Om något inträffar längs denna väg finns en risk att båda leverantörernas nät fallerar. Det som är viktigast att kravställa om, oavsett om man använder sig av en eller av flera leverantörer, är att det nät som används är redundant, det vill säga att det inte finns någon ”single-point-of-failure”. En redundant lösning innebär att det finns flera vägar för den elektroniska kommunikationen att ta på sin väg från internetleverantören till slutkunden, och att dessa vägar är geografiskt åtskilda.

Det mest redundanta alternativet är att använda sig av flera leverantörer och ställa tydliga krav till dessa avseende redundanta nät, exempelvis i form av dubbla linor hos respektive leverantör. En avvägning måste dock göras avseende kostnad i relation till nytta med denna lösning. Beroende på hur redundant lösning man anser sig behöva, kan alternativet med en leverantör och flera geografiskt åtskilda förbindelser ofta vara tillräckligt redundant. Med denna leverantör kan man skapa en djup relation och därmed öppna för rakare dialog om önskemål från kundens sida och tillgängliga eller nya alternativ från leverantörens sida.

22 Resultat av intervjustudie – genomförd av FSPOS, FSPOS AG KI under 2012



Figur 3: Alternativa lösningar för att säkerställa redundans i leveransen; 1. En leverantör – singellina, 2. En leverantör – dubbellina, 3. Två leverantörer – dubbellinor.

Som beskrivits ovan finns det olika sätt att säkerställa robusthet i den fysiska infrastrukturen. En annan aspekt som är viktig är den logiska infrastrukturen såsom protokoll, operativsystem och tillämpningar för växlar och routrar. Den logiska infrastrukturen kan i många fall ändras även på avstånd via nätet, och behöver skyddas mot hot i form av intrång, överbelastning och manipulation. Beställaren bör föra en dialog med leverantören gällande krav på logisk redundans, exempelvis möjlighet att leda om datatrafiken.

ATT TÄNKA PÅ I AVTAL:

- Avtala om att leverantören ska delge resultat av sina riskanalyser och annat riskarbete
- Avtala om att leverantören informerar om incidenter som påverkar leverans
- Krav kan specificeras på redundant utrustning och relevant skalskydd hos leverantören
- Krav kan specificeras på relevanta övningar, både enskilt av leverantören och gemensamt med leverantören
- Krav kan specificeras på logisk redundans, t.ex. möjlighet att leda om datatrafik
- Beakta risken för Single-points-of-failure, även då flera leverantörer används

Prioritering

I dagsläget finns ingen lagstadgad prioritering av samhällsviktiga verksamheter avseende vilka som får tillgång till elektronisk kommunikation i en krissituation som berör dessa nät. PTS utreder för närvarande möjligheten att införa ett sådant system, likt Styrel för prioritering av samhällsviktiga elanvändare[23], vilket också de finansiella aktörerna ställer sig positiva till.[24] Leverantörer av elektronisk kommunikation har dock redan idag den tekniska möjligheten att prioritera IP-trafik, exempelvis att i en krissituation se till att blåljusmyndigheters IP-trafik går före allmänhetens IP-trafik.

Som beställare är det viktigt att ha en dialog med leverantören om hur man som kund prioriteras i en krissituation samt vilka möjligheter det finns att påverka denna prioritering. Leverantörer har ofta en prioritetsordning bland sina kunder, denna är dock sällan öppen och hur leverantören prioriterar framkommer först i en krissituation.

Oavsett om det kommer lagstadgas om ett system för prioritering enligt ovan behöver aktörerna själva se till att avtal med leverantörer innefattar SLA:er gällande sanktioner som indirekt leder till att de prioriteras, för att säkerställa en robust leverans av elektronisk kommunikation och snabba åtgärder vid avbrott.

Samverkan med andra beställare

Genom att använda befintliga samverkansforum inom den finansiella sektorn kan aktörerna tillsammans utbyta idéer och frågor kring olika typer av lösningar och på detta sätt skaffa sig referenspunkter inför dialog med leverantörer. De finansiella aktörerna tillsammans är en viktig och stor kundgrupp och gemensamma krav från dessa torde väga tungt för leverantörerna.

23 www.energimyndigheten.se (Styrel - prioritering av samhällsviktiga elanvändare vid kortvarig elbrist)
24 Resultat av intervjustudie, FSPOS Arbetsgrupp Kritisk Infrastruktur

5. SERVICE OCH TILLGÄNGLIGHET

I detta avsnitt beskrivs parametrar som bör ses över för att säkerställa tillgängligheten i de tjänster som ska anskaffas och som ska täckas av avtalen. Här beskrivs kategorier för de egna funktionerna gällande exempelvis kvalitet och redundans. Avsnittet innehåller även beskrivning av hur krav kan ställas på löpande stöd och support från leverantören, samt löpande uppföljning av hur tillgänglighetskrav uppfylls.

Avsnittet redogör även för de olika parametrar som normalt ingår ett avtals tjänstenivåer. Avslutningsvis presenteras ett antal frågor som bör beaktas i framtagande av avtalet, gällande bland annat monitorering och sanktioner.

Med service menas i detta avsnitt de olika former och olika grad av leveransstöd som ges av leverantören. Detta innefattar således såväl löpande stöd och support som olika nivåer av tillgänglighet och kvalitet hos de erbjudna tjänsterna. Tillgängligheten uttrycks i procent och innebär den grad till vilken en beställare kan förvänta sig att kunna använda en tjänst.

I detta avsnitt beskrivs hur olika nivåer används för att dela in beställarens tjänster för att säkerställa rätt service och prioritet. Val av nivå för beställarens tjänster utgår alltid från behov för den berörda tjänsten och vilken kostnad en viss tjänstenivå medför. Den del av avtalet som specificerar tjänstenivå per tjänst och vilken service respektive nivå innehåller, benämns Service Level Agreement (SLA).[25]

Dessa SLA:er ingår oftast som ett delavsnitt i det övergripande avtalet och är ett bra sätt för beställare att optimera de egna systemens service utifrån behov, men de tydliggör samtidigt för leverantören vilka mål de har att förhålla sig till och är därför ett viktigt underlag för deras kvalitetsarbete. SLA:er bör följas och utvärderas av såväl beställare som leverantör och misslyckanden av leverantören att uppfylla de olika servicenivåerna bör kopplas till sanktioner i någon form.

5.1 Val av servicenivå

Den beroendeanalys som beskrivits i tidigare avsnitt (se avsnitt *2. Beroendeanalys genom kontinuitetshantering*) av denna vägledning kartlägger hur kritiska de egna systemen är. För att maximera nyttan av den service som köps och för att undvika under- respektive överinvestering i servicen, är det därför rimligt att definiera olika servicenivåer för respektive system. Exempelvis kan mindre kritiska system täckas av en grundnivå och

25 Andra begrepp som ibland förekommer i samband med fastställande av SLA är Service Level Specification (SLS) och Service Level Objective (SLO), som båda utgör delar av ett SLA. SLS är den operativa/tekniska vägledningen för att uppnå den önskade servicenivån, medan SLO är en vägledning som beskriver de mätbara mål som ska uppnås genom servicenivån.

de mest kritiska av en prioriterad nivå. Ofta är dock behoven av de egna systemen så pass olika att fler servicenivåer än två behövs.

En högre servicenivå medför samtidigt en högre kostnad och vid val av servicenivå bör alltid en avvägning göras mellan den nytta som förväntas ges av en nivå och den kostnad det skulle innebära. Kostnaden avser här vad beställaren betalar för en viss servicenivå. Nyttan är den kostnad för exempelvis ett avbrott som kan undvikas genom den valda servicenivån.

Leverantörer specificerar ofta färdiga erbjudanden med olika servicenivåer, inte sällan benämnda ”guld”, ”silver”, ”brons”, etc. Sådana benämningar utgår dock inte från någon universell standard och vad som inkluderas i ett ”guld”-erbjudande för en leverantör är därför inte per definition samma för en annan. Beställare bör därför göra en noggrann jämförelse mellan vad som innefattas i respektive leverantörs servicepaket.

I ett SLA definieras varje tjänstenivå utifrån ett antal parametrar. Vilka parametrar som inkluderas kan skilja sig från fall till fall och bör styras av vilka behov beställaren har inom de tjänster som anskaffas. Nedan presenteras några av de vanligaste parametrarna som täcks av leverantörers tjänstenivåer. Därefter presenteras ett antal övriga tjänster, som beställare kan överväga att inkludera i avtalet, exempelvis inom uppföljning och sanktioner.

5.2 Parametrar som kan inkluderas

Tillgänglighet

Tillgängligheten hos en tjänst beskrivs ofta av leverantörer uttryckt i procent, där 90 % tillgänglighet exempelvis innebär att systemet förväntas vara fritt från avbrott 90 % av tiden. Detta kan även uttryckas inverterat som otillgänglighet eller som *avbrottstider*, detta används bland annat i Kammarkollegiets ramavtal. Tillgänglighet och otillgängliget uttryckt som procent av total kalendertid kan beskrivas som i nedanstående tabell.

Tillgänglighet	Otillgänglighet (per år)	Otillgänglighet (per månad)
90 %	876 timmar	73 timmar
99 %	87,6 timmar	7 timmar 18 minuter
99,9 %	8,76 timmar	43 minuter 48 sekunder
99,99 %	52 minuter 33 sekunder	4 minuter 22 sekunder
99,999 %	5 minuter 15 sekunder	26 sekunder

Vilken tid tillgängligheten mäts mot är inte alltid tydligt i leverantörernas erbjudande. I vissa fall är den baserad på ett kalenderår och i andra fall på ett kvartal. Därutöver kan tillgängligheten ibland baseras på heldagar, medan den i andra fall utgår från den servicetid den aktuella tjänsten har.

Det kan i vissa fall även vara lämpligt att ställa mer specifika krav än de i exemplet ovan. Exempelvis kan krav ställas på högre tillgänglighet särskilda dagar i månaden, vissa dagar på året, eller under vissa tider på dygnet, då verksamheten är särskilt känslig för avbrott. Det kan även vara av relevans att ha en dialog med leverantören om möjlighet att ställa krav på skydd mot överbelastningsattacker.

Beställare bör i dialog med leverantören tydliggöra hur tillgänglighetstiden räknas ut samt kräva att få se historiska siffror på tillgänglighet innan avtal skrivs på.

Maximalt antal fel

För vissa tjänster är det lämpligt att ställa krav på maximalt antal fel. Ibland är just frekvensen av avbrott mer viktig än hur långa avbrotten är. Konsekvenserna av ett avbrott för en viss tjänst kan exempelvis vara lika stora oavsett om de avhjälps inom 2 eller 10 timmar och det är då rimligt att fokusera på denna parameter. Beställare bör säkerställa att de tjänster som är särskilt känsliga för antalet avbrott garanteras en servicenivå med maximalt antal fel som kan accepteras.

Maximalt antal fel bör precis som tillgänglighet även specificera vilken tidsperiod som gäller och det är en betydande skillnad om detta gäller per år, månad eller vecka. Sett till ett helt år skulle acceptansnivån kunna vara så vitt skild som 2, 24 eller 104 fel. Det är därför av stor vikt att leverantören tydliggör vilka tider som antalet mäts emot. Precis som för tillgänglighet, bör leverantörer kunna uppvisa historiska siffror på antal fel hos den berörda tjänsten, och beställare bör alltid kräva att få ta del av sådan statistik.

Det är viktigt att säkerställa att beställare och leverantör har samma definition av begreppet fel och att denna definition finns med i avtalet, gärna med förtydligande exempel.

Servicetid

Servicetid är den tid som leverantören kan förväntas vara tillgänglig för att åtgärda eventuella fel, dvs. under vilka timmar som leverantören finns tillhanda för support för en viss tjänst. För mer kritiska tjänster, som har en högre servicenivå, är det vanligt och ofta lämpligt att ha servicetid dygnet runt alla dagar i veckan. Leverantörer benämner ibland detta som 24h-service, eller liknande.

För mindre kritiska tjänster, som har en lägre servicenivå, är det vanligt och ofta lämpligt att ha en mer begränsad servicetid. En lägre servicenivå innebär en lägre kostnad och för att undvika överinvestering kan det accepteras att support endast kan ges under exempelvis timmarna 08-18 måndag till fredag.

Åtgärdstider

Åtgärdstid är den tid som passerar från det tillfälle då felet anmäls eller upptäcks av leverantören, till dess att det är åtgärdat och tjänsten är återställd till normalläge.

Beställare bör se till att detta är tydliggjort i det avtal som upprättas, samt att åtgärdstider tillgodoser de krav som den egna verksamheten har.

Krav på åtgärdstid kan exempelvis formuleras som *"Maximal åtgärdstid per fel under servicetid (timmar)"*. Beställare bör, precis som för tillgänglighet, även se till att avtal tydligt anger om åtgärdstiden utgår från hela dygn eller om de endast gäller för den servicetid som gäller för den aktuella servicenivån.

Kvalitet/prestanda

Även kvalitetsparametrar kan täckas av leverantörens servicenivåer. Detta kan exempelvis inkludera kvalitet för förbindelser inom tal-, video- och datatjänster, som kan vara av stor vikt för IP- och internetbaserade tjänster. Några exempel på kvalitetsparametrar[26]:

- *Trafikprioritet*: möjliggör prioritering av datatrafik då bandbredden är begränsad
- *Fördröjning* (latency): den tid det tar för ett IP-paket att transporteras från sändare till mottagare
- *Variation i fördröjning i nätet* (jitter)
- *Paketförlust (*packet loss*)*: andelen IP-paket som inte når mottagaren

Kraven för dessa kvalitetsparametrar kan variera avsevärt mellan olika tjänster. Beställare bör säkerställa att de tjänster som köps får rätt servicenivå och de egna tjänsterna tilldelas en prioritet, precis som för exempelvis tillgänglighet. Beställaren kan ställa krav på leverantören att uppvisa garanterad kvalitet. Sådant krav finns exempelvis i Kammarkollegiets ramavtal.

Underhåll och servicefönster

Alla system kommer att behöva underhåll. Som beställare är det viktigt att veta under vilka tider servicefönster ligger. Beställare bör säkerställa att underhåll sker på fasta tider så att verksamheten kan tillgodose planerade avbrott och så att den egna verksamheten inte påverkas av dessa underhåll.[27] Vid mer akuta fall bör klargöras i avtal hur leverantören informerar beställaren om när och hur underhåll ska ske.

Särskild servicenivå vid kritiska fel/krisläge

Det är vanligt att servicenivåer som anges i avtal avser drift i normalläge. Vid extraordinära händelser eller krisläge kan därför särskilda SLA-krav specificeras för parametrarna som diskuterats ovan. Det är dock viktigt att avtalet tydligt anger vad en extraordinär händelse eller krisläge innebär, samt huruvida det är leverantören, beställaren eller båda två som kan avgöra om en sådan händelse föreligger. Sanktioner

---

26 Robust Elektronisk Kommunikation – vägledning för användare vid anskaffning, PTS
27 http://natverk.dfs.se/ (Frågor att beakta inom infrastruktur vid anskaffning av molntjänster)

vid åsidosättande av SLA-krav, som behandlas nedan, kan också definieras särskilt för krisläge.

Kommunikation med leverantören vid avbrott

Finansiella aktörer bör begära att erhålla regelbundna uppdateringar avseende leverans av de elektroniska kommunikationerna, särskilt vid incidenter och händelser som förväntas påverka leveransen. Det är leverantörernas skyldighet att omedelbart rapportera till exempel brister i skyddet av utrustning eller angrepp mot tjänsten till kunden.

Avtal bör även tydligt definiera vid vilken grad av störning beställaren informeras, hur informationen förmedlas och till vem, samt vilken information som ska delges. I det senare kan avtalet exempelvis stipulera att leverantören ska delge vilka tjänster som har drabbats eller vad prognosen för avhjälpning är.

Ibland kan kravet på information definieras i termer av löpande statusrapporter, exempelvis dagligen eller varannan timme. För mindre kritiska tjänster kan det räcka med en rapportering vid avbrott och en rapportering vid det slutgiltiga återställandet av tjänsten. Krav kan ställas på muntlig kommunikation men kan även behöva ställas på tillhandahållande av driftstatistik och mer eller mindre omfattande incidentrapporter i form av på förhand fastställda dokument.

Beställare bör tillsammans med leverantören ta fram en rutin för eskalering. I Kammarkollegiets ramavtal finns krav på gemensamt framtagen eskaleringsrutin. Där kravställs även att två separata eskaleringar ska användas, en teknisk och en på managementnivå. Beställare bör även säkerställa att leverantören alltid har en kontaktperson som handlägger inkomna ärenden. Lämpligen bör kontaktpersonen ha befogenhet att fatta bindande beslut för den part kontaktpersonen företräder. Felanmälan ska kunna göras dygnet runt, alla dagar på året. Avtalen bör också möjliggöra att såväl leverantören som beställaren kan påkalla eskalering.[28]

ATT TÄNKA PÅ I AVTAL:

- Tydliggör hur tider räknas ut för exempelvis tillgänglighet, antal fel och åtgärder vid avbrott
- Krav kan ställas på leverantören att uppvisa garanterad kvalitet
- Specificera särskilda krav för krisläge, vad som innebär krisläge, samt tillhörande sanktioner vid avbrott
- Specificera särskilda villkor för kommunikation med leverantören vid såväl planerade som oplanerade avbrott

28 Ramavtalsupphandling – Datakommunikation, nätverk och telefoni, Kammarkollegiet

5.3 Uppdatering, uppföljning och sanktioner

Uppdatering av avtal

Leverantörers erbjudanden medför ofta långa bindningstider och/eller uppsägningstider. Sådana villkor gör det därför svårt att byta leverantör eller omförhandla befintliga avtal. Eftersom tjänster inom elektronisk kommunikation kännetecknas av snabba teknikförändringar, är risken stor att det avtal som tecknats hinner bli inaktuellt gällande de tjänster de omfattar eller de villkor som reglerar de inkluderade tjänsterna.

Beställare bör därför säkerställa att avtalet inte utgör ett hinder för byte av leverantör inom en rimlig tidsperiod, genom att noga utvärdera de bindningstider och uppsägningstider/villkor som erbjuds. Ett alternativ är också att avtalet stipulerar att båda parter träffas inom bestämda intervall för att diskutera och omförhandla avtal. En skrivelse i avtal kan exempelvis reglera att omförhandling av avtal görs en gång per år eller en gång vartannat år.

Uppföljning av SLA

För att säkerställa att SLA-kraven efterlevs på önskvärt sätt och för att möjliggöra sanktioner vid leverantörens åsidosättande av krav, är det viktigt att uppfyllnad mäts på ett effektivt sätt och att detta görs kontinuerligt. Verktyg eller infrastruktur för uppföljning kan tillhandahållas av den egna organisationen, av leverantören eller av en betrodd tredje part. Beställare kan ställa krav på leverantören att presentera en metod för mätning av exempelvis prestanda och tillgänglighet. Sådana krav finns exempelvis i Kammarkollegiets ramavtal.[29]

Avtalet bör klargöra hur uppföljningen sker och hur ofta avstämningar görs. Exempelvis kan avtalet stipulera att denna ska göras löpande med månatliga avstämningar. Genom kontinuerliga avstämningar kan eventuella åtgärder tas och sanktioner vidtas då rätt servicenivå inte uppnåtts.

Sanktioner vid åsidosättande av SLA

För att skydda beställaren och för att motivera leverantören att uppfylla de servicenivåer som avtalet täcker, är det viktigt att avtalet specificerar villkoren för händelser då leverantören misslyckas att uppfylla SLA-kraven.

Åsidosättande av SLA kan ha många olika orsaker och ta sig uttryck på många olika sätt. Det är därför viktigt att beställare i dialog med leverantören tydligt klargör vad som innebär ett åsidosättande av avtal. Den typ av verktyg eller infrastruktur som används för monitorering är dessutom av stor vikt för att kunna avgöra om åsidosättande har skett.

---

29 Ramavtalsupphandling – Datakommunikation, nätverk och telefoni, Kammarkollegiet

I vissa fall hänvisar leverantörer till så kallade ”force majeure”-klausuler, som skyddar dem vid ett avbrott. Det är viktigt att beställare i avtalsförhandling tydliggör vilka fall som avser ”force majeure” och vilka som inte gör det, samt att detta tydligt framkommer i avtalet. Leverantörer har ett incitament att definiera detta begrepp så brett som möjligt, medan en så tydlig definition som möjligt ligger i beställarens intresse.[30] Även här är monitoreringen av yttersta vikt för att kunna avgöra om en sådan situation föreligger, då en effektiv övervakning ofta kan klargöra om felet ligger hos leverantören eller om det ligger utom dennes kontroll.

Sanktioner vid åsidosättande kan definieras på flera olika sätt, exempelvis genom en sänkning av kostnaden för tjänsten under berörd period, dvs. en direkt finansiell sanktion. Andra typer av sanktioner är till exempel en prissänkning eller krediter för framtida leveranser av den berörda tjänsten.[31]

Ersättningen bör spegla den kostnad som beställaren skulle drabbas av vid ett avbrott. Vid ett avbrott kan det emellertid vara svårt att påvisa vilken skada som åsamkats. Därför är det en god idé att på förhand definiera vilka sanktioner som bör gälla. Ett värdefullt underlag för förhandling med leverantören ges av den beroendeanalys som genomförts för det aktuella systemet/verksamheten.

I vissa fall kan det även vara motiverat att bryta avtalet helt med leverantören. Detta kan exempelvis vara aktuellt vid längre avbrott, som drabbar särskilt kritiska system och som inte åtgärdas av leverantören. Därför kan man som beställare vilja definiera vilka villkor som ska gälla för att avtalet kan brytas helt och då avtal kan tecknas med en ny leverantör. Exempelvis kan avtalet ge respektive part friheten att bryta avtalet då motparten ”grovt åsidosatt sina åtaganden”. Viktigt är då att avtalet även definierar vilka händelser som detta inkluderar.

ATT TÄNKA PÅ I AVTAL:

- Specificera villkor för omförhandling och uppdatering av avtal
- Tydliggör vilka fall då avbrott undantas från sanktioner, t.ex. ”force majeure”
- Förhandla på förhand om de kostnader av avbrott som gäller för sanktioner
- Definiera de sanktioner som ska gälla vid åsidosättande av SLA
- Definiera vid vilka villkor avtalet kan brytas helt

30 www.outsourcing-center.com (Negotiating Effective Service Level Agreements)
31 www.iids.org (Managing Violations In Service Level Agreements)

BILAGA A - PROCESS FÖR KONTINUITETSHANTERING

Program för kontinuitetshantering

Kontinuitetshantering skapar en grundläggande medvetenhet om de affärskritiska processerna och resurserna samt dess tolerans mot störningar, liksom vilka risker och sårbarheter verksamheten är exponerad mot. Denna kunskap är viktig för att kunna ta genomtänkta och avvägda beslut gällande lösningar för elektronisk kommunikation.

Eftersom omvärlden ständigt förändras är det nödvändigt att kontinuitetsarbetet regelbundet revideras. För att säkerställa detta behöver ett program för kontinuitetshantering utvecklas, implementeras och hållas levande. Kontinuitetshanteringsprogrammet är den löpande process för ledning och styrning som stöds av den högsta ledningen och tilldelas tillräckliga resurser för att implementera och upprätthålla kontinuitetshantering. För ett lyckat kontinuitetsarbete finns ett antal framgångsfaktorer:

- Förståelse för hur organisationens beroende av andra kan påverka den egna förmågan att leverera tjänster och produkter, samt för hur ett avbrott i den egna verksamheten kan påverka andra organisationer och funktioner i samhället.
- Ledningen visar sitt engagemang, exempelvis genom att etablera interna nyckeltal kopplade till framsteg inom kontinuitetsarbetet.
- Kontinuitetshantering är en naturlig del av organisationskulturen och är en process som involverar och engagerar hela organisationen.
- Börja enkelt och öka sedan ambitionsnivån, gällande både omfång och djup, ju skickligare man blir.

Det är viktigt att det finns en gemensam syn på verksamhetens riskbenägenhet, det vill säga var gränsen går för vilka konsekvenser som är acceptabla. Detta kan definieras genom en kriteriemodell där olika konsekvenskategorier (t.ex. ekonomi, rykte/varumärke) och konsekvensnivåer (obetydlig, märkbar, allvarlig) definieras, därefter beskrivs var gränsen för vad som är acceptabelt går. I exemplet nedan är gränsen för vad som är acceptabelt angiven med den svarta linjen mellan nivåerna märkbar och allvarlig. Med detta menas att konsekvenser inom ekonomi och rykte/varumärke är accepterbara upp till det som beskrivs inom nivån märkbar. Konsekvenserna inom nivån allvarlig bedöms inte som accepterbara.

	Obetydlig	Märkbar	Allvarlig
Ekonomi	Förlust < 500 000	Förlust < 5 000 000	Förlust > 5 000 000
Rykte/ varumärke	Ingen förlust av kunder	Förlust av låg andel kunder	Förlust av stor andel kunder

Figur 4: Exempel på kriteriemodell - konsekvenskategorier och konsekvensnivåer

I exemplet används tre konsekvensnivåer. Kriteriemodellen skulle även kunna använda ett större annat antal nivåer om det skulle anses lämpligt att segmentera analysen ytterligare, exempelvis genom att använda nivåerna *obetydlig*, *märkbar*, *allvarlig* och *katastrofal*. På ett liknande sätt kan fler konsekvenskategorier än ekonomi och rykte/varumärke läggas till i kriteriemodellen, baserat på vilka områden organisationen anser lämpliga.

I det inledande arbetet formuleras även initiala kontinuitetsstrategier som beskriver hur organisationen på en övergripande nivå tänker sig att uppnå kontinuitet. Exempelvis kan kontinuitetsstrategin för ett nyckelpersonsberoende vara kompetensspridning. Ett beroende till externa IT-system kan exempelvis ha en kontinuitetsstrategi om manuella rutiner och en kontinuitetsstrategi kopplat till lokaler kan vara att avtala om reservarbetsplatser hos ett partnerföretag. Dessa initiala strategier kan komma att behöva revideras efter att mer detaljerade analyser av processer, resurser och beroenden har genomförts.

Identifiering av affärskritiska processer

Ett av de första stegen i kontinuitetshanteringsarbetet är att identifiera affärskritiska processer, för att sedan genom det fortsatta arbetet säkerställa att de alltid kan levereras. Identifieringen görs med utgångspunkt i vilka processer som är viktiga för att organisationen ska kunna uppnå sina verksamhetsmål samt eventuella legala krav som organisationen har för sin verksamhet.

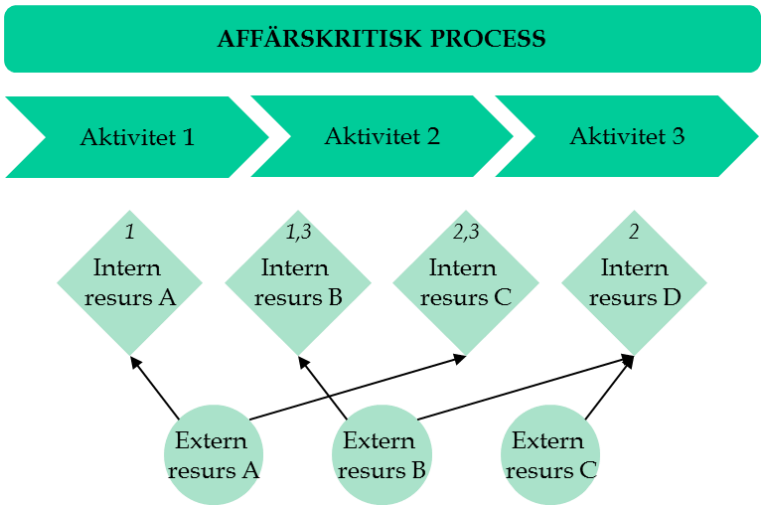
I detta arbete är det bra att inventera eventuellt arbete som tidigare gjorts inom detta område inom organisationen, t.ex. processkartläggningar eller återstartsrutiner för kritiska IT-system.

Analys av beroenden

Affärskonsekvensanalys är ett verktyg för att få en fördjupad kunskap om de aktiviteter samt interna och externa resurser som behövs för att leverera de affärskritiska processerna. Kunskap om hur kritiska resurser kan påverka verksamhetens förmåga att utföra en aktivitet är central.

Första steget i affärskonsekvensanalysen är att identifiera vilka kritiska aktiviteter som måste kunna utföras för att säkerställa att de affärskritiska processerna fungerar. Detta görs genom att analysera varje affärskritisk process och identifiera kritiska aktiviteter.

För att kunna utföra de identifierade kritiska aktiviteterna krävs i sin tur både interna och externa resurser i form av personal, system, lokaler, leverantörer etc. För varje aktivitet identifieras därmed de interna och externa resurser som behövs för att utföra respektive aktivitet. Detta illustreras i figur 4 nedan.



Figur 5: Exempel på dokumentation av en affärskritisk process, dess kritiska aktiviteter samt beroendet av interna och externa resurser

När kritiska aktiviteter samt interna och externa resurser identifierats för varje affärskritisk process är nästa steg att definiera den maximalt tolerabla avbrottstiden för varje aktivitet.

För att definiera maximal tolerabel avbrottstid (MTPD[32]) för en aktivitet används den tidigare utvecklade kriteriemodellen som definierar organisationens riskbenägenhet. Den längsta tid som ett avbrott kan fortgå, utan att konsekvenserna blir så allvarliga att de enligt kriteriemodellen definieras som oacceptabla, är den tid som är aktivitetens maximalt tolerabla avbrottstid.

En aktivitets maximalt tolerabla avbrottstid avgör sedan vilket krav på återhämtningstid (RTO[33]) som ställs på respektive resurs. Med detta menas den tid inom vilken resursen måste kunna återgå till normal funktion efter ett avbrott. Ofta sätts krav på återhämtningstid med en säkerhetsmarginal i förhållande till den maximalt tolerabla avbrottstiden. I de fall där resursen har att göra med lagring av data

[32] *Maximum tolerable period of disruption (ISO 22301)*
[33] *Recovery time objective (ISO 22301)*

är det också relevant att definiera krav på återhämtningspunkt (RPO[34]) vilket innebär krav på hur gammal data maximalt får vara för att medge funktionalitet i den kritiska aktiviteten.

Olika typer av elektronisk kommunikation är vanligtvis en av de viktigaste resurserna för finansiella aktörer, och det handlar då ofta om beroenden till externa leverantörer. Det är viktigt att ha en dialog med leverantörer för att få en bild av robustheten i leveransen av de tjänster som är kritiska för den egna verksamheten. Vissa delar av kontinuitetsplanerna kan behöva synkroniseras med leverantörens kontinuitetsplaner och det är även viktigt att komma överens om gemensamma skyddsnivåer (mer om detta i avsnitt *4. Robusthet*). Kravställning på tillgänglighet och service regleras genom att specificera Service Level Agreements (SLA) i avtal (mer om detta i avsnitt *5. Service och tillgänglighet*).

ATT TÄNKA PÅ I AVTAL:

- Synkronisera organisationens kontinuitetsplaner med leverantörens
- Kom överens om gemensamma skyddsnivåer
- Ställ krav på tillgänglighet och service (SLA)

Slutligen görs en riskvärdering för att få en djupare förståelse för risker och hot som är kopplade till de resurser som stödjer affärskritiska processer. Detta för att avgöra om befintliga lösningar är tillräckliga för att säkerställa leverans i nivå med behoven.

I en riskvärdering inom ramen för kontinuitetshantering läggs fokus på den konsekvens en störning eller ett avbrott har, och framförallt på att analysera hur sannolikt det är att avbrottet överskrider resursens krav på återhämtningstid.

Konsekvens	**Exempel på frågor att ställa sig**
Normala arbetsplatser utslagna (helt eller delvis)	*Var ska vi arbeta?*
Uteblivet IT-stöd (verksamhetskritiska system)	*Har vi tekniska eller manuella reservrutiner?*
Utslagen kommunikation (telefoni, internet etc.)	*Har vi alternativa kommunikationsvägar?*

[34] *Recovery point objective (ISO 22301)*

Förlust eller frånvaro av nyckel-personer eller stora personalgrupper	➢	*Har vi nyckelpersoner och hur ska vi möta nyckelpersonsberoendet?*
Utslagning av kritiska leverantörer eller motparter	➢	*Vad har motparterna för krisberedskap och hur påverkar det oss?* *Har vi alternativa leverantörer?*

Figur 6: Exempel på övergripande konsekvenser som bör beaktas i arbetet[35]

Utifrån riskvärderingen tas sedan beslut om vilka risker som måste minskas för att säkerställa att de maximalt tolerabla avbrottstiderna för kritiska aktiviteter inte överskrids. Riskvärderingen kan även identifiera risker där den befintliga redundansen är onödigt hög.

Identifiering av kontinuitetslösningar

Utifrån resultatet av riskvärderingen tas beslut om eventuella förstärkningar och/eller förändringar av befintliga kontinuitetslösningar. Lösningarna kan bland annat delas upp i de tre kategorierna personal, lokaler och system och kan exempelvis omfatta:

- Organisationsutveckling t.ex. omorganisering av en enhet
- Reservlösningar t.ex. investering i ett reservalternativ till ett kritiskt IT-system
- Upphandling av alternativa leverantörer
- Etablering av reservanläggning dit delar av organisationen kan flytta vid behov

Om en reservlösning till exempel är att flytta delar av verksamheten till en reservbyggnad behövs en plan upprättas som beskriver hur flytten dit ska ske och om det är några speciella rutiner som gäller i nya lokalen (t.ex. inpassering). Även återflytt till ordinarie lokaler behöver förberedas.

En kontinuitetsplan beskriver alla åtgärder som organisationen förberett för att upprätthålla de affärskritiska processerna i enlighet med krav på maximalt tolerabel avbrottstid. Kontinuitetsplanerna innehåller identifierade kontinuitetslösningar samt reserv- och återgångsrutiner ofta i form av ett antal checklistor samt beskrivning av roller, ansvar och befogenheter. Förslag på innehåll i kontinuitetsplanen återfinns i checklistan 6.*1 Beroendeanalys genom kontinuitetshantering*. Kontinuitetsplanerna aktiveras vid behov för att kunna upprätthålla en kritisk aktivitet och möjliggöra för en snabb återgång till normal verksamhet.

35 Vägledning vid kontinuitetsplanering, Finansinspektionen

Utvärdering och revidering

Omvärlden och organisationer är i ständig förändring, det är därför av vikt att regelbundet revidera kontinuitetsarbetet för att säkerställa att kontinuitetsstrategier, -lösningar och -planer fortfarande är tillämpliga. Även vid större förändringar i verksamheten, som t.ex. nya IT-system, organisationsförändringar eller byte av leverantörer, bör en revidering göras.

Det är utöver revidering även viktigt att regelbundet öva och testa de implementerade kontinuitetsplanerna för att säkerställa att befintliga kontinuitetslösningar är tillräckliga så att maximalt tolerabla avbrottstider för affärskritiska processer ej överskrids. Omfattning och frekvens av test och övning bör kopplas till hur kritisk en process eller resurs är för verksamheten. Genom att kontinuitetslösningar för de mest kritiska resurserna testas mer frekvent och omfattande än de mindre kritiska, kan testresurserna optimeras.

BILAGA B - CHECKLISTOR

Beroendeanalys genom kontinuitetshantering

- ☐ Säkerställ att rätt kompetenser inkluderas i arbetet med beroendeanalysen
- ☐ Upprätta ett program för kontinuitetshantering som säkerställer att arbetet utvecklas, implementeras och upprätthålls
- ☐ Ta stöd av befintlig kompetens och tidigare utfört arbete inom risk- och kontinuitetshantering, samt övrigt säkerhetsarbete
- ☐ Specificera organisationens riskbenägenhet genom en kriteriemodell, med relevanta konsekvenskategorier
- ☐ Formulera kontinuitetsstrategier för hur organisationen generellt tänker sig uppnå kontinuitet
- ☐ Identifiera den egna organisationens affärskritiska processer, baserat på verksamhetsmål och legala krav
- ☐ Identifiera kritiska aktiviteter som måste fungera för att upprätthålla organisationens affärskritiska processer
- ☐ Identifiera interna och externa resurser som är kritiska för att utföra de kritiska aktiviteterna
- ☐ Fastställ maximalt tolerabla avbrottstider för de kritiska aktiviteterna, den tid som maximalt får passera innan oacceptabla konsekvenser uppstår (baserat på riskbenägenheten)
- ☐ Fastställ krav på återhämtningstid för de kritiska resurserna och vid behov även krav på återhämtningspunkt
- ☐ Utför riskvärdering för de kritiska resurserna och besluta om riskbehandling
- ☐ Identifiera kontinuitetslösningar baserat på tidigare steg i kontinuitetsarbetet. Dessa är mer specifika åtgärder för att säkerställa kontinuitet och kan exempelvis delas in i kategorier som personal, lokaler och system
- ☐ Upprätta kontinuitetsplaner för respektive identifierad affärkritisk process/funktion/system. Kontinuitetsplanerna ska täcka in åtgärder och rutiner, checklistor, roller och ansvar, etc. Förslag på innehåll:
  - Introduktion
  - Mål, syfte och omfattning (Vilka kritiska processer och resurser omfattas?)
  - Roller, individer och ansvar
  - Kontinuitetslösningar för kritiska resurser (Hur, när och av vem aktiveras dessa?)
- ☐ Beakta att kontinuitetsarbetet bör synkroniseras med leverantörens planer, för att säkerställa robusthet i nästa led

- Kontinuitetsarbetet ligger till grund för vilka tjänster som bör anskaffas och bör därför utvärderas utifrån kostnad och nytta. Ett värde för return of investment (ROI) kan exempelvis tas fram

Anslutningsformer

- Krav på karta över ledningsnätet, ledningsnätets ålder etc.
- Avtala om relevant grad av anslutning för respektive tjänst och med den leverantör som bäst tillfredsställer tjänsternas behov, baserat på beroendeanalysen och priset för tjänsten. Beakta bland annat:
  - Anslutningshastighet baserat på uppskattat trafikvolym
  - Mobiltäckning för trådlösa anslutningar
- Vid behov av redundans kan uppringning (dial-up) användas om övriga anslutningar är otillgängliga
- För fast anslutning är fiberoptiskt nät snabbast men mobila tekniker finns för 4G-nätet, med hög hastighet
- Beakta anslutningars vädersäkerhet. Fiberoptiskt nät är exempelvis inte påverkat av åska
- Beakta att olika anslutningar ger olika skydd mot intrång, bland annat:
  - Fibern avger inte något elektromagnetiskt fält vilket gör att den är okänslig för åska och svår att avlyssna.
  - Fasta anslutningar exponerar användaren mot risker under längre tid och möjliggör därför för inkräktare att ladda ner större mängder – brandväggar kan ge skydd mot dessa angrepp
  - Mobila nät är exponerade mot större risker och kräver krypterings- och autentiseringslösningar
  - Definiera behovet av flexibilitet för de tjänster som köps
  - Definiera antalet tjänster tydligt i antalet
- Säkerställ att leverantörer erbjuder tillräcklig bandbredd för den typ av tjänster som utförs
- Säkerställ tillgänglighet till domännamnsystemet (DNS)
- Säkerställ tillräcklig anslutningshastighet baserat på uppskattad maximal trafikvolym (föregås av trafikanalys)

Robusthet

- Formulera specifika krav på robusthet, exempelvis:
  - Regelbunden och tillräcklig service av utrustning
  - Skalskydd som säkerställer att obehöriga inte har tillgång till exempelvis serverhallar och utrustning

- Lokaler med god miljö, gällande exempelvis temperatur, el, luftfuktighet, etc.
- Säkerhet mot störningar i eltillförseln bör t.ex. finnas på plats.
- Lokaler och utrustning ska övervakas, så att avvikelser kan identifieras och avhjälpas
- Systemansvariga med tydligt ansvar bör finnas för samtliga berörda tjänster och dess utrustning
- Redundans för relevant utrustning eller speglade servrar på alternativt driftställe
- Redundant ledningsnät
- Redundans i leveransen av elektronisk kommunikation hela vägen fram till byggnaden, så kallad ”Last mile-redundans”

- Avtalet ska tydligt klargöra var gränsen går mellan leverantörens och beställarens ansvar
- Krav på systematiskt kvalitets- och säkerhetsarbete hos leverantören (t.ex. ISO 9001, ISO 22301, ISO/IEC 27001)
- Säkerställ att leverantören uppfyller krav för brandskydd, enligt lagen (2003:778) om skydd mot olyckor
- Säkerställ att leverantör erbjuder fullt stöd för både IPv4 och IPv6 så att alla kan nå fram, oavsett IP-version
- Vid nyanskaffning av exempelvis brandväggar, routrar, switchar, servrar etc. säkerställ IPv6-stöd.
- Vid användning av molntjänster, säkerställ tillräckligt höga krav på fungerande externa anslutningar
- Krav på redogörelse av leverantörers leverantörer
- Använd LEK 5 kap. 15§ som stöd vid kravställning mot leverantörer. Lagtexten innehåller bestämmelser till skydd för konsumenter och andra slutanvändare:

  ”Ett avtal mellan en konsument och den som tillhandahåller ett allmänt kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster ska innehålla tydliga, heltäckande och lättillgängliga uppgifter om:

  1. *leverantörens namn och adress,*
  2. *de tjänster som tillhandahålls,*
  3. *tillgången till nödsamtal och tillhandahållandet av lokaliseringsuppgifter,*
  4. *villkor som begränsar tillgången till eller användningen av andra tjänster och tillämpningar än som avses i 3,*
  5. *den lägsta kvalitetsnivå som erbjuds,*
  6. *leveranstiden,*
  7. *de åtgärder som vidtagits för att mäta och styra trafiken i syfte att undvika överbelastning av nätet och hur åtgärderna kan påverka tjänsternas kvalitet,*
  8. *de underhålls- och kundstödstjänster som erbjuds,*
  9. *begränsningar när det gäller användningen av terminalutrustning,*

10. *abonnentens valmöjligheter när det gäller att föra in sina personuppgifter i en abonnentförteckning,*
11. *detaljerade priser och taxor,*
12. *hur betalning kan ske och prisskillnaden mellan olika betalningssätt samt hur information om gällande taxor och underhållsavgifter kan erhållas,*
13. *avtalets löptid,*
14. *villkoren för förlängning och upphörande av tjänsten,*
15. *villkoren för förlängning och uppsägning av avtalet,*
16. *vilka åtgärder som kan komma att vidtas vid säkerhetsbrister,*
17. *villkoren för ersättning om tjänster inte tillhandahålls enligt avtalet, och*
18. *hur ett tvistlösningsförfarande för konsumenter utanför domstol inleds."*

- Krav kan ställas om att leverantören ska öva individuellt eller gemensamt med beställaren, med fokus på exempelvis:
  - Kompetens och erfarenhet hos personalen
  - Test av system, processer, beroenden, alternativa driftställen
  - Genomgång av checklistor och rutiner
  - Samverkan och kommunikation
- Ställ krav på hur leverantören rapporterar om eget arbete med robusthet (Operativt – taktiskt – strategiskt), exempelvis att avtala om att få ta del av resultat av leverantörens riskanalyser och annat kontinuitets- och säkerhetsarbete
- Ställ krav på att leverantören regelbundet delger en skriftlig beskrivning av hur de hanterar säkerhetsarbetet i enlighet med de krav som ställts på leverans av respektive tjänst
- Beakta att flera leverantörer inte nödvändigtvis innebär full redundans, då det kan finnas single-points-of-failure. Redundans uppnås när anslutningar är geografiskt åtskilda antingen för en enskild leverantör eller för två leverantörer där vägarna är fysiskt avskilda
- För dialog med leverantören gällande krav på logisk redundans, exempelvis möjlighet att leda om datatrafiken
- För dialog med leverantören om hur er leverans prioriteras i en krissituation samt vilka möjligheter det finns att påverka denna prioritering
- För dialog med leverantören om möjlighet att ställa krav på skydd mot överbelastningsattacker
- Avtala om att leverantören ska ha en utsedd kontaktperson dedikerad till beställaren
- Upprätta dialog med andra aktörer för utbyte av idéer och för gemensam kravställning
  - Krav på lokaler, strömförsörjning mm.
  - Krav på riskhantering
  - Ägar- och ansvarsdelning (när är det kundens ansvar och när är det leverantörens?)

- Krav på gemensamma övningar
- Krav på leverantörers redundans
- Krav på leverantörers risk- och sårbarhetsanalyser/kontinuitetsplaner

Service och tillgänglighet

- Säkerställ att beställda tjänster inkluderas i ett SLA, där respektive tjänst får en tjänstenivå som uppfyller dess krav (baserat på beroendeanalysen). Beakta parametrar som:
  - Tillgänglighet/avbrottstid
  - Maximalt antal fel (definition av begreppet fel)
  - Åtgärdstider vid avbrott
  - Kvalitet/prestanda
  - Servicetid
  - Underhåll och servicefönster
  - Kommunikation med leverantören vid avbrott. Avtala om när avbrott ska kommuniceras, hur det ska kommuniceras och vad som ska kommuniceras
- Avtala om särskilda servicenivåer vid krisläge. Särskilda nivåer bestäms för parametrarna som inkluderas i SLA, med särskilda nivåer och villkor för sanktioner
- Vid val av servicenivå, väg alltid kostnaden mot nyttan, för att undvika över- och underinvestering
- Inkludera tydliggöranden om hur servicenivåerna räknas ut, för att undvika missförstånd eller tvister vid avbrott, exempelvis gällande tider eller antal fel är räknade per månad, kvartal eller år
- Tydliggör i avtalet när ett avbrott anses ha inträffat, exempelvis när det faktiskt har inträffat, när det upptäcks eller när det har anmälts
- Se över historiska siffror på leverantörens tjänster, gällande exempelvis avbrott eller antal fel
- Avtala om villkor för omförhandling och uppdatering av avtal, samt när ett avtal kan brytas på grund av åsidosättande från någon av parterna
- Tillse att leverantören har dokumenterade rutiner för övervakning, felhantering, uppdateringar och övrigt relaterat till drift och förvaltning
- Säkerställ att efterlevnad av SLA uppfylls genom strukturerad och mätbar monitorering, samt att avstämningar görs kontinuerligt på bestämda tider för driftsstatistik och svarstid för kundtjänst
- Avtala om vilka sanktioner som gäller då leverantören inte lyckas uppfylla SLA-kraven. Sanktioner kan bestämmas exempelvis genom:
  - Sänkt kostnad för tjänsten under den berörda perioden
  - Prissänkning eller kredit på framtida leveranser av tjänsten

- Motivera sanktioner med den kostnad som ett avbrott skulle medföra. Då detta kan vara svårt att påvisa vid en incident bör dessa kostnader specificeras i avtalet i förväg
- Klargör i avtalet vilka händelser som undantar leverantören från sanktioner, exempelvis vid ”force majeure”, där det tydligt framgår vad som inkluderas i detta

BILAGA C: ORDLISTA[36]

Ord/ förkortning	Förklaring
Avbrottstid	Se Tillgänglighet
CDMA	Code Division Multiple Access - teknik för mobil anslutning inom tredje generationens mobiltelefoni, 3G
Dataclearingen	Dataclearingen är ett masstransaktionssystem som i huvudsak används för konto till konto-överföringar som inte utnyttjar bankgironummer. Systemet baseras på att deltagarna utväxlar standardiserad information om en kunds transaktion så att det blir möjligt att utföra denna mellan bankerna.
DNS	Domain Name System, domännamnsystemet
DNSSEC	IETF-standarden DNS Security Extensions (DNSSEC) ger möjlighet att kryptografiskt verifiera om DNS-uppslagningen är korrekt och på så vis kunna detektera och avvisa en attack.
Domän	En nivå i domännamnshierarkin
Domännamn	Ett unikt namn, sammansatt av namndelar, där en i domännamnssystemet lägre placerad domän står före en högre placerad domän, t.ex. pts.se.
Force majeure	Händelse som står utom leverantörens makt och som man inte hade kunnat räkna med. Används ibland i avtalsklausul för att friskriva leverantören från oförutsedda incidenter.
HSPA	High Speed Packet Access - teknik för mobil anslutning inom tredje generationens mobiltelefoni, 3G
IP	Internet Protocol, kommunikationsprotokoll som handhar adressering, vägval och överföring av IP-paket på internet på det som kallas nätverksnivån. IPv4 och IPv6 är adresseringsstandarder.
IP-adress	Numerisk adress till en dator eller annan utrustning i ett IPnät. Adressen skrivs i version 4 (IPv4) vanligen som fyra heltal åtskiljda med punkter (t.ex. 123.45.67.8). I version 6 (IPv6) skrivs adressen i grundformen som åtta block med vardera 16 binära siffror i hexadecimal notation åtskilda med kolon t.ex. 3ffe:ffff:0100:f101:0210:a4ff:fee3:9566.
IPv4	Internet Protocol, version 4 (32-bitars IP-adress).

[36] *Förklaring av tekniska begrepp är baserade på, Robust elektronisk kommunikation – vägledning för användare vid anskaffning, PTS*

IPv6	Internet Protocol, version 6 (128-bitars IP-adress).
Jitter	Variation i fördröjning i nätet.
Latency	Benämns även *fördröjning* och avser den tid det tar för ett IP-paket att transporteras från sändare till mottagare.
LTE	Long Term Evolution – mobil anslutning inom nästa mobiltelefonigeneration, 4G
Molntjänster	Molntjänster, s.k. Cloud Computing, möjliggör användning av serverbaserade applikationer över internet.
MSB	Myndigheten för samhällsskydd och beredskap vars uppgift är att utveckla och stödja samhällets förmåga att hantera olyckor och kriser.
Nettning	Nettning innebär att motstående förpliktelser kvittas. Vid nettning sammanförs motstående betalnings- eller leveransförpliktelser mellan två eller flera avtalsparter enligt förfallodagen till en betalningsförpliktelse eller en leveransförpliktelse som gäller investeringsobjekt av samma art.
Packet loss	Benämns även paketförlust och avser andelen IP-paket som inte når mottagaren.
Redundans	Reservkapacitet t.ex. en dubblerad extern anslutning.
RIX	Banker som har konton i Riksbanken kan göra betalningar till och från varandra genom Riksbankens betalningssystem för stora betalningar, RIX. Via det tekniska systemet avvecklas betalningar i svenska kronor.
Robusthet	Med robusthet menas i detta sammanhang förmågan att motstå störningar och avbrott samt förmågan att minimera konsekvenserna om de ändå inträffar
Servicetid	Den tid, uttryckt i timmar på dygnet och dagar i veckan, som leverantören är tillgänglig för att åtgärda fel.
SLA	(Service Level Agreement) serviceåtagande i form av ett avtal där t.ex. ett företag som tillhandahåller en internettjänst åtar sig att upprätthålla en viss kvalitet på sin tjänst med ersättningsskyldighet om tjänstetillhandahållaren inte uppfyller avtalade krav som avtalats.
Styrel	Styrel är ett landsomfattande planeringssystem för prioritering av samhällsviktiga elanvändare vid en förutsedd eller plötsligt uppkommen kortvarig elbrist.
Tillgänglighet	Den grad en beställare kan använda en tjänst och uttrycks i procent. Kan även uttryckas inverterat som otillgänglighet eller *avbrottstid*, uttryckt i tid då tjänsten inte är tillgänglig för beställaren.

xDSL	Tekniker för överföring av stora datamängder over telefonledningar av koppar. Tekniken som används anges av den bokstav som ersätter x i xDSL: ADSL (Asymmetric Digital Subscriber Line), SDSL (Symmetric Digital Subscriber Line), HDSL (High-data-rate Digital Subscriber Line), VDSL (Very-high-rate Digital Subscriber Line)
WiMax	Worldwide Interoperability for Microwave Access – ett protokoll för fast och mobil trådlös kommunikation.
Åtgärdstid	Den tid som passerar från det tillfälle ett fel anmäls eller upptäcks av leverantören, till dess att felet är åtgärdat.

BILAGA D: REFERENSER

Lagtext

SFS	Namn	Förkortning
2003:389	Lagen om elektronisk kommunikation	LEK
2003:778	Lagen om skydd mot olyckor	LSO

Textdokument

Titel	Utgivare	Version
Robust elektronisk kommunikation - vägledning för användare vid anskaffning	PTS	PTS-ER-201116
Ramavtalsupphandling – Datakommunikation, nätverk och telefoni	Kammarkollegiet	DNR 2008-9
Svenska Betalningsflöden – Så funkar det	FSPOS Arbetsgrupp Betalningsförmedling	Juli 2009
Good Practice Guidelines	Business Continuity Institute	2008
Quality management systems — Requirements	International Organization for Standardization	ISO 9001:2008
Societal security - Business continuity management systems	International Organization for Standardization	ISO 22301:2012
Information technology - Security techniques - Information security management systems - Requirements	International Organization for Standardization /International Electrotechnical Commission	ISO/IEC 27001:2005
Vägledning vid kontinuitetsplanering	Finansinspektionen	2005
Kontinuitetsplanering – en introduktion	MSB	2006
Bredbandsstrategi för Sverige	Näringsdepartementet	N2009/8317/ITP
Resultat av intervjustudie	FSPOS Arbetsgrupp Kritisk Infrastruktur	2012

Webbplatser

Webbplats	Innehåll
Post- och telestyrelsen www.pts.se	*Mobilt bredband* *Anslutningsformer* *Robust kommunikation*
Skanova www.skanova.se	*Om fiber*
Stokab www.stokab.se	*Stokabmodellen*
Fibert (ekonomisk förening) www.fibert.se	*Varför fiber?*
Energimyndigheten www.energimyndigheten.se	*Styrel - prioritering av samhällsviktiga elanvändare vid kortvarig elbrist*
Dataföreningen natverk.dfs.se	*Frågor att beakta inom infrastruktur vid anskaffning av molntjänster*
Outsourcing Center www.outsourcing-center.com	*Negotiating Effective Service Level Agreements*
Intelligent Interactive Distributed Systems www.iids.org	*Managing Violations In Service Level Agreements*
Statistiska centralbyrån www.scb.se	*Företagens användning av IT 2011*