

Robust elektronisk kommunikation

- vägledning för användare vid anskaffning**

Robust elektronisk kommunikation - vägledning för användare vid anskaffning

Rapportnummer

PTS-ER-2011:16

Diarienummer 10-8756

ISSN

1650-9862

Författare

Anders Rafting, NS2

Post- och telestyrelsen

Box 5398

102 49 Stockholm

08-678 55 00

pts@pts.se

www.pts.se

Förord

Samhällets behov av robust elektronisk kommunikation är idag mycket stort och kommer att öka i framtiden. Utifrån sin myndighetsroll att arbeta med robust kommunikation har Post- och telestyrelsen tagit fram denna vägledning.

Med robusthet menas i detta sammanhang förmågan att motstå störningar och avbrott samt förmågan att minimera konsekvenserna om de ändå inträffar. Företag, myndigheter, offentlig förvaltning och andra organisationer liksom enskilda medborgare är idag i hög grad beroende av att elektronisk kommunikation dvs. fast och mobil telefoni, datakommunikation samt internet finns tillgänglig och fungerar på ett tillfredsställande sätt.

Syftet med denna vägledning är att, till personer som anskaffar elektroniska kommunikationstjänster, ge stöd för att kunna ställa relevanta krav på tillgänglighet i avtal med berörda leverantörer. Målet är att tjänster och information som baseras på elektronisk kommunikation ska kunna tillhandahållas på ett robust och tillförlitligt sätt.

Stockholm 2011-06-15

Catarina Wretman,

Ställföreträdande generaldirektör

Innehåll

Robust elektronisk kommunikation	1
- vägledning för användare vid anskaffning	1
Förord	3
Sammanfattning	6
Abstract	7
1 Checklistor	8
1.1 Checklista med krav för IP-/internetanslutning och tillhörande tjänster	8
1.2 Checklista med krav på DNS	9
1.3 Checklista med krav för telefoni	9
1.4 Checklista för krav på lokaler, strömförsörjning mm.	10
1.5 Checklista för riskhantering	10
1.6 Checklista för att teckna avtal med leverantör av elektronisk kommunikation	11
2 Behov av robust elektronisk kommunikation	13
2.1 Inledning	13
2.2 Syfte och mål med vägledningen	13
2.3 Målgrupp	13
2.4 Omfattning och avgränsning	13
2.5 Läsanvisningar	14
2.6 Förankring/granskning	15
3 Roller och ansvar för robusthet inom sektorn för elektronisk kommunikation	16
3.1 Operatörernas ansvar	16
3.2 Statens ansvar	16
3.3 Ditt ansvar som köpare och användare av elektronisk kommunikation	17
4 Hantering av risker i verksamhetskritiska funktioner	18
4.1 Riskanalys är grundläggande för säkerhetsarbetet	18
4.2 Metoder för riskanalys	19
4.3 Vad är verksamhetskritiskt och vilka är hoten	20
4.3.1 <i>Alternativ metod – omvänd målsökning</i>	21
4.4 Reducering av risker	21
4.5 Upprätta en kontinuitetsplan	21
5 Anslutning för extern elektronisk kommunikation	23
5.1 Olika accessformer	23
5.2 Begreppet bredband	26
5.3 Anslutning för telefoni	28
5.3.1 <i>Traditionell abonnentanslutning (ISDN)</i>	29
5.3.2 <i>VoIP/IP-telefoni</i>	29
5.3.3 <i>Internetbaserad telefoni</i>	29
6 Krav på tillgänglighet för extern anslutning och berörda tjänster	30
6.1 Tillgänglighet genom redundans i olika servicenivåer	30
6.1.1 <i>Servicenivå 1 – för normal tillgänglighet</i>	30
6.1.2 <i>Servicenivå 2 – specificerar högre grad av robusthet</i>	31
6.1.3 <i>Servicenivå 3 – ger skydd även mot svårare påfrestningar</i>	31
6.2 Krav på kapacitet och kvalitet för IP- och internetbaserade tjänster	32
6.2.1 <i>Dimensionering av kapacitet i elektroniska kommunikationstjänster</i>	32
6.2.2 <i>Kvalitetsparametrar för olika tjänster</i>	33

6.2.3	Ställ krav på IPv6	35
6.2.4	Virtual Private Networks	35
6.3	Krav för webbtjänster	36
6.3.1	Krav för skydd av kommunikation mellan webbserver och klient	37
6.4	Krav för DNS-tjänster	37
6.4.1	Ställ krav på stöd för DNSSEC	38
6.5	Krav för e-posttjänster	39
6.5.1	Tillgängligheten till e-postservrar måste garanteras	39
6.5.2	Skydd mot obehörig läsning av e-post	39
6.5.3	Hantering av oönskad e-post	39
6.5.4	Skydd av e-postservrar	40
6.6	Krav på tillgänglighet för fast telefoni	40
6.7	Krav på täckning, kapacitet och elförsörjning i mobiltelefoninät	41
6.8	Krav på tillgång till svensk spårbar tid	41
7	Avtal med leverantör av elektronisk kommunikation	43
7.1	Avtal för önskad grad av tillgänglighet	43
7.1	Viktigt att ange vad som ska omfattas av avtalet	43
7.2	Vilka avbrottstider är acceptabla?	44
7.2.1	Tillgänglighet i procent av total kalendertid	44
7.2.2	Tillgänglighet i timmar	45
7.3	Avtal om fast telefoni – kretskopplad eller paketförmedlande	47
7.4	Avtal om mobiltelefoni	47
7.4.1	Avbrottsinformation	47
7.4.2	Åtgärder som kan vidtas för att höja tillgängligheten till mobiltelefoni	48
7.5	Avtal om information från operatören	48
7.5.1	Information vid avbrott och störningar	48
7.5.2	Avtal om information om driftsstatistik	48
7.6	Vad bör beaktas vid avtal om molntjänster?	49
7.7	Övriga avtalsvillkor	50
7.8	Stöd för incidenthantering	50
Bilaga - 1	Infrastrukturen för elektronisk kommunikation	52
	Viktigt med robusthet på infrastrukturnivå	52
	Vad ingår i infrastrukturen för elektronisk kommunikation?	53
	<i>Fysiska delar av infrastrukturen</i>	53
	<i>Logiska delar av infrastrukturen</i>	53
	Infrastrukturens säkerhet – hot och skydd	54
	<i>Tillgänglighet genom redundans</i>	55
Bilaga 2	Tryggad tillgång till adresser genom IPv6	56
Bilaga 3	Branschstandard för DNS-tjänst med kvalitet	58
Bilaga 4	Internet Governance	61
Bilaga 5	Ordlista och förkortningar	64
Litteratur		68
Källhänvisningar		68
Länkar till ramavtal inom offentlig förvaltning		68

Sammanfattning

Syftet med vägledningen är att ge stöd vid anskaffning av extern elektronisk kommunikation, exempelvis internetanslutning och telefoni. Målet är att tjänster och information som baseras på elektronisk kommunikation ska kunna tillhandahållas på ett robust och tillförlitligt sätt. Den primära målgruppen för vägledningen är personer på företag, myndigheter och organisationer som anskaffar och/eller förvaltar system och tjänster som är beroende av extern elektronisk kommunikation.

Det finns ett brett utbud av anslutningsformer att välja mellan med ett flertal trådbundna och trådlösa tekniker för extern anslutning. Avgörande för att kunna välja lämplig accessform och att kunna ställa adekvata krav vid anskaffningen, är att en risk- och sårbarhetsanalys genomförs för varje funktion som identifierats som kritisk för verksamheten. Viktiga frågor i riskanalysen är exempelvis: vilka är hoten, hur stor är sannolikheten för ett avbrott, vilka är konsekvenserna av ett avbrott för verksamheten, hur långa avbrott tål verksamheten, vilka kostnader skulle det medföra att minska konsekvensen av ett avbrott, vilka tjänster ska prioriteras i en katastrofsituation, etc.

Baserat på de krav som verksamheten ställer, exempelvis uttryckt i acceptabla avbrottstider, kan tillgängligheten definieras i avtal med olika servicenivåer. I vissa fall kan det vara relevant att teckna avtal med villkor för högre robusthet och tillförlitlighet än vad leverantörernas standardavtal erbjuder. Ett sådant avtal utgör, tillsammans med tillförlitligheten i egen berörd utrustning, grunden för tillgänglighet till extern elektronisk kommunikation. Förutom avtal om krav på tillgänglighet och åtgärdsstid etc. bör även avtalet omfatta krav på information från operatörer vid störningar och avbrott.

Vid användning av molntjänster är det bland annat viktigt att ta reda på hur prestanda och tillgänglighet för förbindelsen till molntjänstleverantörens datacenter garanteras samt beakta hur konfidentiell och hemlig information skyddas.

För hantering av IT-angrepp av olika slag, kan det vara tillrådligt att i förväg ha etablerat ett samarbete med en organisation för incidenthantering.

Abstract

The purpose of this guide, is to provide support to people dealing with procurement of external electronic communication, for example Internet access and telephony. The aim is for organizations to provide services and information in a robust and reliable way. The target audience is persons at companies, authorities and organizations responsible for procurement and administration of system and services that depend on external electronic communication.

There is a huge choice of wired and wireless technologies for external communication. To be able to choose the most appropriate access method and to put adequate demands, it's crucial to perform a risk and vulnerability analysis for each function that has been identified as business critical. Important questions to put are for example: what are the threats, how big is the probability for a breakdown, what are the consequences if an outage occurs, how long can the business tolerate to be offline, what are the costs to lessen the consequences, what services should be prioritized in a state of disaster, etc.

Based upon the requirements from the business, for example expressed in acceptable maximum time for a disruption, the availability for services and information can be defined in different service levels. In certain cases it might be relevant to sign agreements with stronger requirements for robustness and reliability than what is usually the case. That type of agreement forms, together with own equipment, the basis for availability to external electronic communication. Except for requirements regarding availability and service time, the agreement should also contain a requirement to get information from the service provider/operator on disturbances and disruptions.

If cloud computing is used it's important to get information on how performance and availability to the connection to the datacenter for the cloud computing company is safeguarded and take into consideration how confidentiality and privacy is protected.

In order to be able to handle cyber attacks, it would be advisable to establish a kind of co-operation with a computer incident response team.

1 Checklistor

1.1 Checklista med krav för IP-/internetanslutning och tillhörande tjänster

- Relevant grad av tillgänglighet och kvalitet för externa anslutningar baserad på riskanalys.
- Tillgänglighet kan anges i exempelvis tre servicenivåer för externa anslutningar
 1. Enkel anslutning till operatör med en (1) fysisk förbindelse.
 2. Anslutning som dubbleras genom två fysiskt åtskilda framföringsvägar till en och samma operatör där förbindelserna är *separerade bortom en punkt i nätet där redundans finns* t.ex. knutpunkt/nod/stamnät.
 3. Anslutning till två olika operatörer där man försäkrat sig om att *anslutningarna till respektive operatörs nät har fysiskt åtskilda framföringsvägar*.
- Information vid inträffade avbrott och störningar
- Policy för e-posttjänster för att undgå obeställd e-postreklam (spam) och nätfiske (phishing)
- Fullt stöd för IPv6 så att även de som enbart har IPv6 kan nå fram
- Tillfredsställande kvalitet på tjänster som tal, video, TV
- Tillräcklig anslutningshastighet baserat på uppskattad maximal trafikvolym
- Dokumenterade rutiner för övervakning, felhantering, uppdateringar och övrigt relaterat till drift och förvaltning
- Säkerställd tillgänglighet till domännamnssystemet (DNS) – se checklista nedan

1.2 Checklista med krav på DNS

- DNS-data för en zon bör ligga på minst två separata namnservrar. Dessa ska vara logiskt och fysiskt separerade genom anslutning till olika operatörsnät, i olika autonoma system (AS).
- DNS-data för en zon bör vara DNSSEC-signerade.
- De NS-poster som listas i den överliggande zonen (.se eller motsvarande) för att peka ut (delegera) en viss domän skall samtliga finnas införda i den underliggande zonen.
- Samtliga namnservrar som listats med NS-poster i en delegerad zon skall svara auktoritativt för domänen.
- Samtliga namnservrar som listats med NS-poster i den delegerade zonen skall svara med samma serienummer i SOA-posten för domänen.
- Zonkontaktadressen i SOA-posten skall vara nåbar.
- Alla NS-poster i den underliggande zonen ska vara nåbara för DNS-trafik från internet.
- Fullt stöd för DNS Security Extension (DNSSEC) ska finnas i samtliga auktoritativa namnservrar.

1.3 Checklista med krav för telefoni

- Tillsammans med telefonileverantören genomföra åtgärder för att förstärka den egna verksamhetens möjligheter att kommunicera med omvärlden
- Få information om täckning, kapacitet, elförsörjning samt var tjänsteservrar är placerade
- Skaffa reservabonnemang hos alternativ operatör. Ha en strategi för hur dessa ska användas och hur nummer ska spridas.

- Vid övergång till mobil Centrex, behåll ett antal fasta telefoner på kontoret.
- Skaffa ett eller flera reservtelefonnummer till växeln, som endast används då huvudnumret är satt ur funktion.
- Skaffa separata telefonabonnemang som kopplas till den egna telefonväxeln för att skapa reservväg då ordinarie förbindelser inte fungerar.
- Komplettera den fasta telefonin med en internetbaserad lösning.
- Vid IP-telefoni bör krav ställas på kryptering av SIP-signalering och mediaströmmar.

1.4 Checklista för krav på lokaler, strömförsörjning mm.

- Lokaler för IT-system ska ha en tillräckligt god miljö vad avser temperatur, luftfuktighet och el.
- Lokaler för IT-system ska ha ett skalskydd som gör att endast behörig personal har tillträde.
- Det ska finnas skydd mot störningar och avbrott i strömförsörjningen.
- Utrymmen och utrustning ska övervakas för att möjliggöra tidig upptäckt och identifiering av avvikelser, störningar och fel så att snabba korrigerande åtgärder kan vidtas för att minimera konsekvenserna.
- Systemansvariga bör finnas för samtliga delar med tydligt beskrivna ansvarsområden.

1.5 Checklista för riskhantering

- Hur stor är sannolikheten att ett avbrott inträffar?
- Vilka konsekvenser får ett avbrott för verksamheten?

- Hur länge kan ett avbrott vara utan att det får orimliga konsekvenser för verksamheten?
- Vilka kostnader skulle det medföra att minska konsekvensen av ett avbrott eller minska sannolikheten för att ett avbrott inträffar?
- Vilka tjänster ska prioriteras i en katastrofsituation?
- Var bör den lägsta nivån på en tjänst ligga i en katastrofsituation?
- Måste man erbjuda samma kontinuitet av service till alla kunder, eller kan man ha olika servicenivåer?
- Måste alla lokaler vara inkluderade i en kontinuitetsplan eller är vissa mer verksamhets-/affärskritiska än andra?

1.6 Checklista för att teckna avtal med leverantör av elektronisk kommunikation

- Tjänster ska tillhandahållas på ett robust sätt så att fel och avbrott inom operatörens nät har minimal påverkan på tjänstens tillgänglighet och kvalitet.
- Om avbrott och fel ändå inträffar ska avtalet innehålla villkor så att återställande sker inom för verksamheten nödvändig tid.
- Villkoren i övrigt ska vara sådana att om kraven inte uppfylls, ska ersättningen utgå enligt avtal
- Det ska entydigt framgå av avtalet vad operatören ska leverera.
- Kunden bör i sitt avtal med operatören reglera information om tidpunkt, omfattning och tidpunkt för inträffade såväl avsiktliga som oavsiktliga störningar och avbrott.
- Avtala om **när**, dvs. vid vilken grad av störning som information ska ges
- Avtala om **hur**, dvs. i vilken form störningsinformationen ska förmedlas och till vem
- Avtala om **vad** störningsinformationen ska omfatta, t.ex. påverkan på avtalade tjänster, prognoser för färdigtidpunkt, faktisk färdigtidpunkt och när återgång kan ske till normalläge

- Ställ krav på information om driftsstatistik och svarstider för kundtjänst
- Det ska tydligt anges vilka nätdelar som omfattas av avtalet och var gränsen går mellan operatörens ansvar och abonnentens ansvar.
- Tillgänglighetskravet ska vara utformat så att det uppfyller verksamhetens behov.
- Det ska framgå hur operatören garanterar efterfrågad tillgänglighet.
- Det ska anges hur alternativa vägval dvs. redundans garanteras vid spärr och fel.
- Avtalet ska ta hänsyn till verksamhetens krav på tillgänglighet till operatörens kundtjänst.
- Hur säkerställer man prestanda och tillgänglighet på förbindelsen till molntjänstleverantörens datacenter?
- För molntjänster:
 - Hur redundant och robust är molntjänstleverantörens servrar anslutna till internet?
 - Hur förhindrar man inlåsning till leverantör av molntjänster?
 - Hur skyddas konfidentiell och hemlig information?
 - Hur skyddas integriteten?

2 Behov av robust elektronisk kommunikation

2.1 Inledning

Företag, myndigheter och organisationer i är idag mer eller mindre beroende av att kunna kommunicera elektroniskt. Störningar och avbrott i kommunikationen kan orsaka allt från irritation till svåra följder för verksamheten.

För många organisationer kan det därför vara relevant att teckna avtal med villkor för högre robusthet för och tillgänglighet till extern kommunikation än vad leverantörernas standardavtal erbjuder. Ett sådant avtal utgör, tillsammans med tillförlitligheten i berörd utrustning, grunden för tillgänglighet till extern elektronisk kommunikation för en organisation. I avtalet kan Service Level Agreement (SLA) tecknas gällande tillgängligheten för i avtalet ingående tjänster. Med robusthet menas i detta sammanhang förmågan att motstå störningar och avbrott samt förmågan att minimera konsekvenserna om de ändå inträffar – se figur 1 nedan.

2.2 Syfte och mål med vägledningen

Syftet är att ge stöd vid anskaffning av extern elektronisk kommunikation, exempelvis internetanslutning och telefoni.

Målet är att tjänster och information som baseras på elektronisk kommunikation ska kunna såväl tillhandahållas som konsumeras på ett robust och tillförlitligt sätt.

2.3 Målgrupp

Den primära målgruppen för vägledningen är personer på företag, myndigheter och organisationer som anskaffar och/eller förvaltar system och tjänster som är beroende av extern elektronisk kommunikation.

Vägledningen kan även användas av till exempel verksamhets-, säkerhetsansvariga och systemägare för IT-system för att få ökad förståelse för robusthet i elektronisk kommunikation.

2.4 Omfattning och avgränsning

Vägledningen ska:

- ge stöd för att för att genomföra riskanalys,
- baserat på resultatet från riskanalysen kunna ställa de krav på tillförlitlighet som motsvarar verksamhetens behov,
- ge stöd för att kunna föra en dialog med leverantörer i att värdera olika lösningsförslag som ska kunna uppfylla kraven
- öka medvetenheten om att tillförlitlighet påverkas av berörd utrustningen och genom avtal med leverantörer av extern elektronisk kommunikation,
- beskriva kraven på exempelvis fysisk säkerhet, strömförsörjning och driftsmiljö på en övergripande nivå.

Vägledningen behandlar inte metoder för upphandling.

2.5 Läsanvisningar

Kapitel 1 innehåller checklistor som kan vara till stöd vid anskaffning av elektronisk kommunikation och tillhörande tjänster.

Kapitel 2 handlar om syfte och mål, målgrupp och omfattning.

Kapitel 3 talar om vilket ansvar staten respektive operatörerna har för robusthet i elektronisk kommunikation samt vad du själv ansvarar för som anskaffare och användare i detta avseende.

Kapitel 4 handlar om betydelsen av riskhantering, metoder för riskanalys, identifiering av verksamhetskritiska system, hot och hur risker kan reduceras.

Kapitel 5 handlar om olika accessformer för extern kommunikation.

Kapitel 6 behandlar olika servicenivåer för redundans i externa anslutningar och om kapacitet och kvalitet för IP-baserade tjänster.

Kapitel 7 diskuterar hur avtal tecknas med krav på tillgänglighet i procent, krav på åtgärdstid, krav för fast och mobil telefoni, krav på information från operatörer vid störningar och avbrott, vad som bör beaktas vid molntjänster samt orientering om incidenthantering.

2.6 Förankring/granskning

PTS vill rikta ett varmt tack till de personer från olika organisationer inom branschen och sektorn för elektronisk kommunikation som granskat rapporten och lämnat värdefulla synpunkter och förslag till ändringar och tillägg.

3 Roller och ansvar för robusthet inom sektorn för elektronisk kommunikation

3.1 Operatörernas ansvar

I lagen om elektronisk kommunikation (LEK) finns bestämmelser om att operatörerna har ett ansvar för att uppfylla **rimliga krav på god funktion och teknisk säkerhet samt på uthållighet och tillgänglighet vid extraordinära händelser i fredstid**. Dessa krav gäller för alla tillhandahållare av allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster. PTS utgav i maj 2007 ett allmänt råd (PTSFS 2007:2) som beskriver hur dessa bestämmelser kan följas. Lagen och det allmänna rådet kan sägas lägga en grund för robusthet, som alla operatörer bör använda. Dock finns inga värden angivna för exempelvis maximala avbrottstider eller motsvarande .

3.2 Statens ansvar

Investeringar för robusthet i den infrastruktur för elektronisk kommunikation som operatörerna förvaltar, görs i huvudsak utifrån strikt affärsmässiga bedömningar. Detta kan innebära att påfrestningar utöver det normala inte kan hanteras med bibehållen tillgänglighet till nätet och dess tjänster, vilket beställare av elektronisk kommunikation bör känna till.

I de fall marknaden inte själv kan uppnå en nivå på robusthet som klarar extrema påfrestningar, ingriper staten genom PTS med regler, styrning och upphandling av åtgärder.

PTS är sektorsmyndighet för elektronisk kommunikation och arbetar på många olika sätt för att stärka robustheten i infrastrukturen för allmänt tillgänglig elektronisk kommunikation, bland annat genom:

- insatser för att öka förståelsen hos operatörer att använda robusthet som ett konkurrensmedel för att kunna ge kunderna ökad tillgänglighet
- upphandling av robusthetshöjande åtgärder i operatörernas nät,
- samarbete och partnerskap mellan PTS och operatörerna avseende krishantering samt,
- författningsreglering som exempelvis tillsyn av operatörer och att utge allmänna råd och föreskrifter

3.3 Ditt ansvar som köpare och användare av elektronisk kommunikation

Denna vägledning syftar inte i första hand till att beskriva krav på en organisations interna arbete och utrustning. Det är dock viktigt att förstå att förutsättningarna för tillförlitligheten hos organisationens elektroniska kommunikation beror såväl på externa avtal som på egna system och den egna organisationens kompetens inom området.

Avgörande för att kunna genomföra anskaffning med relevant nivå på tillgänglighet är att en risk- och sårbarhetsanalys genomförs för varje kritisk del av verksamheten. Risken för en oönskad händelse, kan minimeras exempelvis genom adekvata avtal med leverantörer av elektronisk kommunikation.

Nedan ges övergripande några exempel på vad som i övrigt ingår i organisationens ansvar när det gäller förutsättningar för tillförlitlig elektronisk kommunikation.

Lokaler

- Utrymmen för verksamhetskritisk utrustning ska ha en tillräckligt god miljö vad avser temperatur, luftfuktighet och el, och
- ska ha ett skydd som gör att endast behörig personal har tillträde.

Strömförsörjning

- Utrustningen ska ha system för skydd mot störningar och avbrott i strömförsörjningen.

Övervakning

- Utrymmen och utrustningar ska övervakas för att möjliggöra tidig upptäckt och identifiering av avvikelser, störningar och fel så att snabba korrigerande åtgärder kan vidtas för att minimera konsekvenserna.

Ansvarsfördelning

- Systemansvariga bör finnas för samtliga verksamhetskritiska delar med tydligt beskrivna ansvarsområden.

4 Hantering av risker i verksamhetskritiska funktioner

4.1 Riskanalys är grundläggande för säkerhetsarbetet

Riskanalys är en grundförutsättning för ett kontinuerligt och systematiskt säkerhetsarbete eftersom det innebär att klargöra och analysera de risker en verksamhet är utsatt för. Riskanalyser inriktas ofta på det som är konkret, i första hand infrastruktur som nätverk, förbindelser, servrar, olika nätverkselement m.m. Den tekniska infrastrukturen är viktig men faktorer som organisation, personaltillgång, nyckelpersonberoende, ansvar, kompetens, rutiner och processer bör också ingå i riskanalysen.

Olika verksamhetskritiska funktioner och tillämpningar baserade på elektronisk kommunikation kräver olika grad av tillgänglighet. Riskanalys är här ett viktigt redskap för att kunna bedöma en organisations samlade behov av åtgärder för att säkerställa tillgänglighet till elektronisk kommunikation. Viktiga frågor i riskanalysen är:

- Vilka konsekvenser får ett avbrott för verksamheten?
- Hur länge kan ett avbrott vara utan att det får orimliga konsekvenser för verksamheten?
- Vilka kostnader skulle det medföra att minska konsekvensen av ett avbrott eller minska sannolikheten för att ett avbrott inträffar?
- Hur stor är sannolikheten att ett avbrott inträffar?

Riskanalys kan genomföras genom att identifiera scenarier och bedöma konsekvenser i form av kostnader, förlorade intäkter, förseningar, försämrad service, bad will etc.

Riskanalys bör göras regelbundet och alltid vid förändringar av arbetssätt samt vid införande av nya rutiner. Riskanalyser bör även genomföras vid nya affärsrelationer, nya tekniska lösningar, nya tillämpningar, i samband med åtgärder för ökad prestanda, ökat skydd eller föranlett av störningar och avbrott.

Inom ramen för riskanalysen bör upprättade rutiner och handlingsplaner, resultat och bedömningar dokumenteras och hållas uppdaterade. Avsaknad av dokumenterade rutiner kan leda till en otydlighet gällande vilka

säkerhetsåtgärder som bör vidtas, vad som ska uppnås, vem som beslutar om åtgärder, vem som ansvarar för genomförande och hur uppföljning ska göras.

Ett sätt att arbeta med riskhantering är att kvantifiera risker i ekonomiska termer. Genom att kvantifiera på detta sätt kan beslutsfattandet förenklas eftersom det går att bedöma nyttan av att genomföra en säkerhetsåtgärd för att eliminera eller begränsa risken.

4.2 Metoder för riskanalys

Det finns ett flertal olika metoder som du kan använda dig av för att genomföra riskanalys. Det finns såväl enkla som mer omfattande varav många är branschspecifika. En viktig faktor att beakta vid val av riskanalysmetod är att den ska kunna gå att tillämpa på såväl små som stora objekt eller företeelser.

En av de enklaste modellerna för analys av risk är den s.k. miniriskmetoden. Denna modell utgör något av en miniminivå för hur risker bör bedömas. I miniriskmetoden beräknas ett s.k. riskvärde utifrån en uppskattad sannolikhet och konsekvens om risken inträffar. För att bedöma sannolikhet (S) och konsekvens (K) kan en enkel, relativ skala från 1-5 användas, där 1 innebär låg och 5 innebär hög. Riskvärdet (R) beräknas genom att multiplicera S och K. För risker med högt riskvärde vidtas normalt olika åtgärder.

För ytterligare information om hur man genomför en riskanalys, se exempelvis ISO/IEC 27001 - Ledningssystem för informationssäkerhet (LIS) som är en ISO-standard. Statliga myndigheter ska numera tillämpa LIS på sin verksamhet.

Även MSB:s rekommendationer Basnivå för informationssäkerhet (BITS) innehåller en metod för riskanalys på IT-system. BITS vänder sig till såväl privat som offentlig verksamhet.

Exempel på andra metoder för risk och sårbarhetsanalys är följande:

- SBA (Sårbarhetsanalys)¹.
- FMEA (Failure Mode Effect Analysis) och Ishikawadiagram (fiskbensdiagram)².

¹ se t.ex. <http://www.dfs.se/products/sba/>

² se t.ex. <http://www.sis.se/upload/632905563861067870.pdf>

- Octave (Operationally Critical Threat, Asset and Vulnerability Evaluation)³.

4.3 Vad är verksamhetskritiskt och vilka är hoten

Det är nödvändigt att först identifiera vilka funktioner som är kritiska för den egna verksamheten och vilka hoten är. För varje funktion görs en bedömning om verksamheten är beroende av att den fungerar tillfredsställande. Den anses i så fall vara kritisk och blir föremål för vidare analys.

I nedanstående lista ges exempel på hot mot elektronisk kommunikation som kan vara bra för en organisation att känna till vid dialog med operatörer.

- elavbrott,
- kabelbrott pga. exempelvis grävarbeten,
- fel och störningar i samband med uppgradering av nät och tjänster,
- tekniska fel t.ex. hård- eller mjukvarufel,
- naturfenomen (storm/översvämning/nedisning etc),
- sabotage genom t.ex.fysisk åverkan, anlagd brand, sprängattentat,
- stöld av t.ex. kopparkablar,
- riktad överbelastning ((Distributed) Denial of Service, (D)DoS),
- angrepp mot logiska funktioner t.ex. domännamnssystemet (DNS), intern och extern rouing, DHCP-servrar, SIP-servrar,
- angrepp mot övervakningssystem,
- organisation (resursbrist, insiderbrott),
- attacker mot tillämpningar t.ex. postsystem, banktjänster, samhällsservice, handel,
- avlyssning, manipulering och stöld av känslig information

³ se t.ex. <http://www.cert.org/octave/>

4.3.1 Alternativ metod – omvänd målsökning

Erfarenheter visar att om man bara fokuserar på kända hot, missas ofta det som är mest skyddsvärt, samtidigt som det vidtas skyddsåtgärder för det som inte behöver det. För att undvika detta, finns en metod som kallas omvänd målsökning, som fokuserar på målet dvs. det som är skyddsvärt istället för på hotet i form av en angripare/aktör. Detta synsätt sätter värdet först, därefter studerar man vad som behöver göras för att säkerställa att det som har högst värde skyddas. Genom detta synsätt kan även okända hot hanteras.

4.4 Reducering av risker

För att strukturera riskanalysarbetet kan det vara bra att genomföra en klassificering och någon form av prioritering. Det finns flera exempel på hur olika typer av risker kan klassificeras, som t.ex.

- tekniska system och lösningar,
- risker som rör interna processer (t.ex. metoder, styrparametrar, uppföljning),
- ekonomiska/finansiella risker ,
- humankapital (t.ex. personal, kompetens och kultur) ,
- risker av legal, politisk eller marknadsmässig karaktär
- risker för konfidentialitetsbrott t.ex. röjande av hemlig information

När väl en risk har beräknats, kan åtgärder vidtas för att minska eller eliminera risken genom att mildra, förebygga eller föregripa den. Det kan ske genom att undvika risken, överföra den genom exempelvis försäkringar, eller genom att reducera hotet, sårbarheten eller den möjliga påverkan (skadan). Det kan också ske genom att upptäcka oönskade händelser, reagera på dem och sedan återställa förhållandena till sitt ursprungsläge.

4.5 Upprätta en kontinuitetsplan

Det mest kostnadseffektiva och därför vanligaste sättet att hantera risk för driftavbrott, särskilt inom organisationer som lever efter marknadsmässiga

principer, är att upprätta en kontinuitetsplan. Här ingår endast de mest kritiska processerna. Planen bör omfatta rutiner vid inträffade avbrott för degraderad reservdrift istället för full normaldrift. Detta kan också utgöra en av parametrarna som grund för val av servicenivå och som metod att reducera sårbarheten.

Det är viktigt att i förväg göra prioriteringar av vad som är mest kritiskt för verksamheten. Med det som grund kan beslut tas i vilken ordning degradering av system/tjänster ska göras. Exempel på frågor man kan ställa sig:

- Vilka tjänster ska prioriteras i en katastrofsituation?
- Var bör den lägsta nivån på en tjänst ligga i en katastrofsituation?
- Måste man erbjuda samma kontinuitet av service till alla kunder, eller kan man ha olika servicenivåer?
- Måste alla lokaler vara inkluderade i en kontinuitetsplan eller är vissa mer verksamhets-/affärskritiska än andra?

Degraderad reservdrift kan behöva genomföras i flera steg, och då är det bra om man har bestämt hur det ska gå till i förväg. Hela denna rutin ska vara väl dokumenterad och förankrad hos alla inblandade.

5 Anslutning för extern elektronisk kommunikation

5.1 Olika accessformer

Idag finns det ett flertal trådbundna och trådlösa tekniker som erbjuder för extern anslutning till exempelvis internet och för telefoni. Nedan ges exempel på de vanligaste.

xDSL (Digital Subscriber Line)

xDSL är en samlingsbeteckning på en familj av tekniker där digitala modem används på det vanliga fasta telefonnätet. Vilken typ av digitalt system som sänds över ledningen framgår av den bokstav som ersätter x. Exempel på beteckningar är ADSL, SDSL och VDSL. A står för Asymmetric, vilket innebär att hastigheten för mottagning, nedlänken, är avsevärt högre än hastigheten för sändning, upplänken.

Vid ADSL går det att ringa som vanligt med den fasta telefonen samtidigt som internetanslutningen via ADSL är igång. För att kunna använda ADSL-anslutning krävs dels ett ADSL-modem, dels att den lokala telefonstationen är förberedd för tjänsten.

Om behov finns av snabbare upplänk för att sända data kan SDSL väljas där S i vid mening står för Symmetric och är en variant av DSL som är symmetriskt vilket betyder att bandbredden är lika både uppströms och nedströms. SDSL använder koppartrådens hela frekvensband och kan därför inte samtidigt användas för vanlig fast telefoni.

VDSL, där V står för Very high speed, är en höghastighetsanslutning för data. VDSL är dyrare och åtkomligt för betydligt färre än ADSL. Liksom SDSL använder VDSL koppartrådens hela frekvensband och kan därför inte samtidigt användas för vanlig fast telefoni.

Mobil access

Med mobil access via 3G- eller 4G-näten ges möjlighet till internetåtkomst med varierande täckning och kapacitet beroende på var ansluten enhet befinner sig. Detta måste beaktas när krav ställs på verksamhetens

tillgänglighet. Olika abonnemang passar olika behov och krav. Ofta innebär avtal debitering efter mängden datatrafik, vilket kan göra denna accessform minde lämplig för anslutning av servrar och liknande.

WLAN (Wireless Local Area Network)

LAN är en form av trådlöst lokalt nätverk (även kallat WiFi) som använder radiovågor i stället för dragna kablar. WLAN används inom begränsade geografiska områden för lokal kommunikation och ger vanligen även access till internet. WLAN finns exempelvis inom ett företags lokaler, på hotell och på allmänna platser som flygplatser, köpcentra, järnvägsstationer och internet-caféer.

Wimax

Wimax är en IEEE-standard som ger en stabilare förbindelse och större räckvidd än WLAN/WiFi. På grund av den bättre räckvidden är Wimax ofta ett bra alternativ när man bygger trådlösa nätverk, även för mobila användare, som täcker större område, exempelvis hela städer. I de senaste versionerna har tekniken bl.a. blivit bättre på att använda lägre frekvenser vilket gör att Wimax bättre klarar av hinder mellan accesspunkten och enheten som ansluter till accesspunkten. Under optimala förhållande ska Wimax kunna ha en räckvidd på upp till ungefär 11 mil och idealt klara av hastigheter upp till 70 Mbit/s. Wimax har vissa likheter med DSL teknikerna då man får välja mellan att ha en hög hastighet eller en riktigt bra räckvidd. Wimax har vanligen god potential för att kunna användas för tjänster som VoIP (IP-telefoni) eller IPTV.

I Sverige används idag frekvensutrymmet på 3,5 GHz. Detta frekvensutrymme är i Sverige licensbelagt och därför behövs tillstånd från Post och Telestyrelsen för att bygga Wimax nätverk.

Mikrovågslänk

Som alternativ till eller som redundans till anslutning via kabel kan en punkt-till-punktförbindelse via radio användas. De vanligaste radiolänkarna använder mikrovågor. Denna teknik används ofta mellan basstationer för mobiltelefoni

och även mellan sändningsplatser för marksänd rundradio. Radiolänkar kräver inte någon kabelgrävning och kan därför bli billigare och går snabbt att ta i drift. En nackdel med radiolänkar är att det oftast krävs fri sikt mellan sändare och mottagare. Antennerna måste monteras i master och på höga byggnader. Överföringen kan störas vid mycket dåligt väder, speciellt vid sändning på vissa frekvensområden. En annan nackdel är att en radiolänk har lägre kapacitet än till exempel optisk fiber.

För att installera mikrovåglänkar med licensierade frekvenser i Sverige krävs ansökan hos Post & Telestyrelsen.

Kabel-TV

I byggnader med kabelTV kan kabelTV-leverantören vanligen erbjuda bredband via ett kabelmodem som kabel-TV-företaget erbjuder. I vissa fall behövs också ett avtal mellan kabel-TV-företaget och fastighetsägaren som gör det möjligt för den förra att leverera tjänsten.

Optisk fiber

Optisk fiber är en anslutningsform som möjliggör mycket hög överföringshastighet. Investering i fiber anses mycket framtidssäker, eftersom allt högre hastigheter kan uppnås på befintlig fiber, genom att uppgradera ändrustningen allteftersom tekniken utvecklas. För fiberanslutning krävs att ny infrastruktur byggs i form av fiberkablar som består av tunna trådar av glas eller plast. En enda optisk fiber tjock som ett hårstrå kan förmedla 8 000 simultana telefonsamtal upp till 40 km utan signalförstärkning eller för att överföra data med mycket hög hastighet - upp till 100 Gbps och mer. Ett fiberoptiskt överföringssystem består av en sändare som skickar iväg och kodar ljussignaler med olika våglängd genom de optiska fibren, samt av en mottagare som tar emot och avkodar dem.

Fiber är ett lämpligt alternativ för organisationer som har höga krav på tillgänglighet för sina externt exponerade servrar t.ex. webb, e-post etc. Till skillnad från enklare bredbandstjänster som baseras på exempelvis ADSL-teknik, kan operatören på ett säkrare sätt garantera kapaciteten för fiberanslutning mellan exempelvis en myndighets eller ett företags olika arbetsställen och internet. En optisk fiber är okänslig för elektrisk och magnetisk påverkan vilket kan vara en stor fördel i vissa miljöer.

Svart fiber

Den minst förädlade tjänsten baserad på optisk fiber benämns svart fiber. Med detta avses s.k. oförädlad nätkapacitet, dvs. fysiska ledningar utan elektronisk utrustning. Svart fiber används för att producera i princip alla slags elektroniska kommunikationstjänster och kan användas i hela eller delar av ett sammanhängande nät. Främst efterfrågas svart fiber av operatörer som i sin tur förädlar tjänsten vidare till slutkundstjänster. Med beaktande av de allt högre kraven på kapacitetskrävande tjänster och utvecklingen av de framtida IP-baserade näten, har betydelsen av optisk fiber, och därmed efterfrågan på tjänsten svart fiber, ökat. Tjänsten svart fiber ser likadan ut oavsett var i nätet den tillhandahålls och för vilket syfte den köps.

Det är köparen av svart fiber som kopplar på den aktiva utrustningen och därmed bestämmer hur den ska användas. Att köparen själv ansluter den aktiva utrustningen ger ökad kontroll vad gäller teknik t.ex. förändringar vad gäller kapacitet, typer av tjänster, lösningar för tjänster. Det ger även bättre affärsmässig kontroll av priset för att producera tjänster och möjligheter till förändrad paketering av tjänster till kunder. Likaså kan servicenivåer och kontroll av kvaliteten förbättras genom att beroendet minskar av t.ex. den servicenivå och kundtjänst som någon tjänstetillhandahållare av mer förädlade tjänster erbjuder.

5.2 Begreppet bredband

Hastigheten i en extern anslutning, ibland kallad bandbredd, uttrycks i bitar per sekund (bps). På den svenska marknaden saluförs olika accesstekniker under namnet ”bredband”. Detta begrepp är på intet sätt är entydigt. Olika leverantörer hävdar att allt från 0,5 Mbit/s till 2 Mbit/s är minimigränsen för att en förbindelse ska kallas för bredband. PTS genomförde i augusti 2010 en mätning av olika accesstekniker - se figur 1 nedan.

Figur 1: Hastighet och kvalitet för olika accesstekniker, 1-11 augusti 2010

			<i>Uppmätta resultat</i>			
	<i>Teknik</i>	<i>Annonserad hastighet (Mbit/s)</i>	<i>Hastighet vid Uppladdning (Mbit/s)</i>	<i>Hastighet vid Nedladdning (Mbit/s)</i>	<i>Svarstid (Ms)</i>	<i>Antal mätningar</i>
Trådbundet	Koppar (xDSL)	24	1,3	11,3	45	4 671
	KoaxialCTV (Kabel-TV)	50	11,7	48,0	25	2 823
	Fibernät LAN	100	24,9	53,6	23	7 959
Mobilt	HSPA (3G)	7,2	0,6	2,5	158	7 459
	CDMA 2000	3,6	0,4	1,1	128	463

* = Inkluderar abonnemang inom intervallet 50-100 Mbit/s.

Av tabellen framgår att det finns påfallande skillnader mellan den hastighet och svarstid som erbjuds av operatörerna och de uppmätta värdena.⁴ Idag ger exempelvis mobil anslutning via HSPA ca 30 procent av utlovad hastighet i nedlänk. Även svarstiden är påtagligt högre än vad som kan förväntas, vilket indikerar att de mobila accessteknikerna alltfjänt lämpar sig sämre för kvalitetsfordrande tjänster. På samma sätt uppvisar xDSL stora brister vad gäller upplänk, vilket ger stora begränsningar för realtidsinteraktiva tillämpningar som exempelvis videokonferenser.

Den maxhastighet som leverantören marknadsför är en teoretisk maxhastighet som normalt inte går att nå. Hastigheten kan påverkas av fler parametrar, bland annat fördröjning i nätet orsakad av exempelvis köbildning. De vanligaste faktorerna som leder till att den teoretiska hastigheten är betydligt lägre än den verkliga är:

⁴ Baseras på mätresultat från tjänsten Bredbandskollen - avser perioden 1-11 augusti 2010.

- avståndet mellan din anslutningspunkt och telestationen – gäller för ADSL
- avståndet mellan mobilnätsansluten terminal och basstationen
- hur många som samtidigt använder samma trådlösa anslutning i området – gäller både WLAN (WiFi) och mobil access (3G/4G)
- annan, störande utrustning anslutna till samma trådlösa nätverk
- radiostörningar av andra orsaker (väder, atmosfäriska förhållanden)

5.3 Anslutning för telefoni

Traditionellt har begreppet fast telefoni avsett kretskopplad taltrafik med tillhörande tjänster mellan telefonstation och abonnentväxlar (PBX) över det fasta allmänna telefonnätet (PSTN). I och med utvecklingen inom IP-telefoniområdet är begreppet fast telefoni idag mycket vidare varför telefoni i denna vägledning används både för traditionell fast telefoni och olika typer av IP-baserad telefoni.

Dagens telefonilösningar kan vara uppbyggda med kretskopplad teknik, IP-baserad pakETFörmedlande teknik eller en kombination av dessa, en så kallad hybridlösning. Oavsett teknik kan abonnentväxeln ha anknytningar för analoga, digitala, trådlösa och mobila terminaler samt IP-telefoner och sk. softphones (telefoniapplikation för dator) som terminaler. Ytterligare ett alternativ är att använda mobiltelefoner som kontorstelefoner (mer om detta under 6.4).

Affärsmässigt finns två huvudalternativ att välja mellan

- eget ägande av abonnentväxel
- funktions-/tjänsteköp som realiserar av olika typer av Centrex- och ”Kommunikation som tjänst”-lösningar.

Gränsen mellan abonnentens och operatörens ansvar brukar kallas nätanslutningspunkt (NAP). I affärsmodellen ”eget ägande” ligger nätanslutningspunkten mellan operatörens accessnät och organisationens växel - organisationen köper s.k. nätanslutning. För det egna ägandet är det väsentligt att anslutningen från abonnentväxeln till operatörens accessnät har skett med robusthet i fokus för att få tillfredsställande tillgänglighet för den externa kommunikationen.

Vid funktions-/tjänsteköp är den tekniska utrustningen oftast placerad i operatörens nät men den kan även vara placerad hos abonnenten varvid

nätanslutningspunkten flyttas längre in i organisationen eftersom operatörens ansvar även omfattar växelfunktion. Om tjänstelösningen används är det viktigt att samtliga berörda SLA-nivåer är anpassade till verksamhetens krav. Det är också viktigt att ha en god kännedom om det egna interna nätverket samt skapa ett förtroendefullt samarbete med leverantören.

5.3.1 Traditionell abonnentanslutning (ISDN)

De vanligaste produkterna för anslutning av abonnentväxlar är ISDN PRA (Primary Rate Access) bestående av 30 talkanaler och ISDN BRA (Basic Rate Access) bestående av 2 talkanaler. För väldigt små installationer eller för att skapa reservvägar in och ut från telefonväxeln kan även separata telefonabonnemang användas. Det finns även lösningar för att använda SIP-baserad IP-telefoni på befintlig ISDN-förbindelse. Det medger en enkel övergång till IP utan investeringar i mjuk- eller hårdvara.

5.3.2 VoIP/IP-telefoni

Många operatörer erbjuder nu telefoni som förmedlas via IP som tjänst i nätet de själva har kontroll över dvs. inte det vi kallar internet. Sådan IP-telefoni har motsvarande tjänster och kvalitet som den traditionella kretskopplade tekniken. Idag finns det möjlighet, om än fortfarande ovanligt, att ansluta abonnentväxeln direkt mot ett sådant yttre IP-nät via en s.k. SIP-trunk. Bedömningen är dock att detta med största sannolikhet kommer bli det stora genombrottet för IP-telefonin i form av ökad funktionalitet och tillkomst av nya tjänster.

5.3.3 Internetbaserad telefoni

Många såväl stora som små teleoperatör erbjuder internetbaserade SIP-lösningar numera utöver sina traditionella telefonlösningar (TDM/IP-baserade). Utvecklingen pekar helt klart åt det hållet, framför allt när fler och fler organisationer har insett mervärdet av att exempelvis kunna kommunicera med video end-to-end där internet egentligen är det enda alternativet på sikt.

6 Krav på tillgänglighet för extern anslutning och berörda tjänster

6.1 Tillgänglighet genom redundans i olika servicenivåer

I detta kapitel beskrivs ett flertal faktorer, som baserat på genomförd risk och sårbarhetsanalys samt framtagna kravspecifikation, bestämmer krav på robusthet/tillgänglighet för olika tjänster som IP- och internetbaserad kommunikation via en samt fast och mobil telefoni.

Det är viktigt att komma ihåg att reducerad drift kan vara ett lämpligare sätt att hantera tillgänglighet än att höja servicenivån, vilket ibland ändå är otillräckligt och dessutom kraftigt fördyrar anslutningen

Det är viktigt att en organisation som erbjuder informations- eller e-tjänster ser till att berörda webb- och applikationsservrar alltid är nåbara. Detta åstadkoms bland annat genom att de placeras på ett sådant sätt att de har hög tillgänglighet med god redundans. Detta ger bibehållen extern tillgänglighet i den händelse en av de anlitade operatörernas infrastruktur skulle drabbas av störningar eller avbrott.

Om drift av webb-, epost- och namnservrar,⁵och andra externt exponerade servertjänster görs i egen regi, ligger ansvaret för att skapa nödvändig redundans på internetanslutningen hos organisationen själv.

Beroende på vad resultatet av genomförd riskanalys visar, kan lämplig servicenivå väljas för externa anslutningar på tillgänglighet – se även figur 2 nedan.

6.1.1 Servicenivå 1 – för normal tillgänglighet

Anslutningen för internetbaserad kommunikation via en Internet Service Provider (ISP) är anpassad för ”normal” driftssituation där åtagandet endast sträcker sig till att kunna tillhandahålla ”normala” e-tjänster, exempelvis vissa tjänster för offentlig e-förvaltning som inte har krav på sig att ständigt vara tillgängliga. Anslutningen utgörs av en enda fysisk och logisk förbindelse till internet som kan vara lokaliserad till kundens geografiska placering eller till annan plats i det fall drift av servrar för webb och e-post är utlagd till extern part. Anslutningen upphandlas med avtal s.k. Service Level Agreement (SLA) som ska ligga till grund för att säkerställa den önskade tillgängligheten. Några ytterligare åtgärder för ökad robusthet är inte nödvändigt.

⁵ server som finns hos operatörerna för domännamnuppslagningar i DNS

6.1.2 Servicenivå 2 – specificerar högre grad av robusthet

Organisationer med högre krav på tillgänglighet än den som nivå 1 ger, kan teckna utökat avtal om fler fysiska anslutningar till en och samma operatör. Denna redundans skyddar mot avbrott om t.ex. en förbindelse slutar att fungera på grund av exempelvis en avgrävd kabel. Emellertid ger detta inget skydd mot logiska fel i exempelvis domännamnssystemet eller routing och inte heller mot andra fel i den tjänstetillhandahållande operatörens infrastruktur.

En beställare som kräver nivå 2 bör ställa krav på att få minst två anslutningar till en och samma operatör. Förbindelserna bör anläggas i fysiskt åtskilda kanaler med garanterat åtskilda framföringsvägar. Om driften av tjänsterna är utlokaliserade till annan part bör upphandlad tjänst tillgodose samma krav på tillgänglighet.

6.1.3 Servicenivå 3 – ger skydd även mot svårare påfrestningar

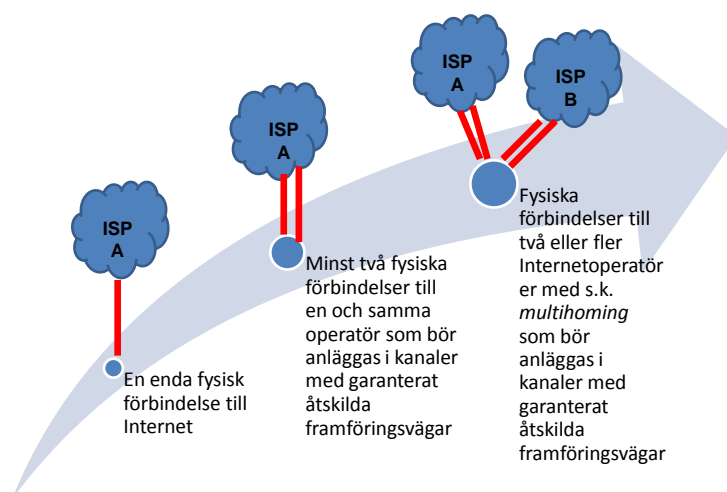
Vissa användarkategorier bedriver verksamheter eller tillhandahåller tjänster som ställer högre krav på tillgänglighet. Dessa ska inte bara klara mindre fel och störningar, utan även vara anpassade för att fungera vid kriser orsakade av svåra påfrestningar. I dessa fall är det omvärldens krav på tillförlitlighet som anger graden av robusthet och vad som krävs för att inte förtroendet ska påverkas negativt. En enskild händelse, exempelvis i form av en överbelastningsattack hos en operatör ska inte kunna leda till att en tjänst blir otillgänglig.

För att uppnå robusthet i nivå 3, bör man ansluta sig till två eller fler internetoperatörer med s.k. multihoming. Detta ger skydd mot att en av de anlitade operatörernas nät av någon anledning upphör att fungera. Den utrustning dvs. routrar som används, måste vid multihoming hantera protokollet Border Gateway Protocol (BGP) för anslutning till internet. Observera att detta också innebär att en organisation som är ansluten via multihoming måste ha tillgång till egen eller externt anlitad kompetens för att hantera BGP-funktionen.

Det är inte alltid som en mer komplex lösning ger ett bättre skydd, särskilt inte vid mindre störningar och fel. Däremot erhålls ett bättre skydd vid större störningar. Samtidigt krävs mer kompetens hos driftspersonalen för att hantera den mer komplexa lösningen i nivå 3, bland annat för att hantera protokollet BGP än vad som krävs för såväl beställare som driftsansvariga för nivå 1 och nivå 2. Nivå 3 använder två eller flera anslutningar till olika operatörer. Eftersom en del av ansvaret flyttas från operatören till kunden, måste denna själv kunna hantera angrepp och incidenter koordinerat med berörd operatör eller köpa denna tjänst från operatören.

I nivå 3 förutsätts kunden tillhandahålla sina resurser över internet med egen IP-adressrymd, s.k. operatörsberoende adresser eller PI-adresser (eng. Provider Independent). Dessutom krävs att man utgör ett eget s.k. autonomt system, AS. Anslutningarna till de olika operatörerna måste liksom för nivå 1 och 2 ha garanterad fysisk redundans. Dessutom måste utrustningen som används vara fysiskt skyddad och placerad i lämplig driftsmiljö. Nivå 3 ger förutom fysisk redundans även logisk redundans då trafiken kan dirigeras en annan väg om en operatör fått problem av något slag, exempelvis drabbats av falsk/felaktig routinginformation, ekonomiska problem etc.

Figur 2: Olika grad av redundans



6.2 Krav på kapacitet och kvalitet för IP- och internetbaserade tjänster

6.2.1 Dimensionering av kapacitet i elektroniska kommunikationstjänster

För att skaffa och upprätthålla god kvalitet i elektroniska kommunikationstjänster, behöver varje organisation uppskatta vilken total trafikvolym som kan förväntas vid olika tidpunkter. Verksamheten behöver vidare uppskatta vilken trafikbelastning som kan genereras vid exempelvis kundkontakter,

uppdateringar från verksamhetssystem, olika slags webbtjänster etc. Vad som också behöver beaktas är om det finns vissa tider eller perioder på året då trafikbelastningen förväntas öka.

Vid dimensionering av kapacitet för förbindelserna krävs att information om verksamhetens trafikmönster hämtas in. Detta sker oftast genom att en trafikmätning utförs. Mätningens resultat ger besked om eventuella trafiktoppar eller andra faktorer att ta hänsyn till och i så fall när detta inträffar. Förutom att anskaffa tillräckligt hög kapacitet baserat på det uppmätta behovet, kan det vara lämpligt att införa *lastbalanseringssystem* för att hantera förväntad maximal trafikbelastning. Räkna med en viss säkerhetsmarginal baserat på trafikmätningen för att undvika oönskade effekter.

6.2.2 Kvalitetsparametrar för olika tjänster

Kvaliteten på förbindelserna som används för förmedling av olika slags tjänster är avgörande för hur väl tal, video, data etc. fungerar. Följande parametrar utgör de med störst påverkan på kvalitén för IP- och internetbaserade tjänster:

- Trafikprioritet (QoS) – möjlighet att prioritera datatrafik, exempelvis mellan olika tjänster då bandbredden är begränsad.
- Fördröjning (latency) – tid som det tar för ett IP-paket att transporteras från sändare till mottagare.
- Variationer i fördröjningen i nätet (jitter).
- Paketförlust (packet loss) – andelen IP-paket som inte når mottagaren.

Kraven på olika parametrar varierar mellan olika tjänster. Exempelvis är telefoni känsligt för fördröjning och jitter. Interaktiva tjänster är mer intoleranta mot paketförluster. Dataöverföring och webbsurfning kräver hög bandbredd. Se figur 3 nedan.

Figur 3: Olika tillämpningars beroende av hastighet och kvalitet

Tillämpning	Bandbredd	Paketfördröjning	Jitter	Paketförlust
Video/TV, IP-baserad telefoni	Medium	Viktig	Viktig	Oviktig
Interaktiva Internettjänster	Låg	Viktig	Oviktig	Viktig
Dataöverföring	Hög	Oviktig	Oviktig	Oviktig
Webbsurfning, Informationssökning	Hög	Oviktig	Oviktig	Oviktig

Om olika tjänster och applikationer nyttjar samma förbindelse är det viktigt att kvalitetsparametrarna beaktar de olika tjänsternas krav. I detta arbete måste olika tjänster vidare värderas utifrån verksamhetens krav på tillgänglighet.

När trafikbelastningen överstiger den kapacitet som organisationen köpt måste den egna utrustningen stödja s.k. trafikprioritet så att den trafik som anses vara viktigast för organisationens verksamhet garanteras tillräcklig bandbredd.

Vad de elektroniska applikationerna och tjänsterna sammantaget indikerar, är att de kräver en miniminivå på ett antal olika parametrar, för att de ska kunna distribueras på ett tillfredsställande sätt. Det räcker inte med att överföringskapaciteten är hög, utan anslutningen måste dessutom vara av acceptabel kvalitet med rimliga svarstider för att leva upp till de förväntningar som användare idag har på nätet. Som betonats ovan bör det särskilt noteras att enskilda aktiviteter som var för sig genererar en blygsam belastning på nätet, snabbt kan aggregeras till en sammantaget mycket hög trafiklast. Det gäller inte minst strömmande högupplöst video som kräver stora mängder dedicerad tillgänglig kapacitet. Vissa aktiviteter som exempelvis videokonferenser, kräver att användaren kan skicka data i samma takt som det tas emot.

6.2.3 Ställ krav på IPv6

Adresserna av den version som dominerar idag, IPv4, är i praktiken slut. Alla slags organisationer bör därför ställa krav på fullt stöd för att kunna kommunicera över IPv6 *utöver* det nuvarande IPv4-protokollet. Kunder/besökare som enbart har IPv6-anslutning kan komma att dyka upp inom en snar framtid. Krav på införande av IPv6 återfinns i EU-kommissionens handlingsplan. Enligt OECD⁶, ISOC⁷ m.fl. borde införande av IPv6 ha påbörjats redan under 2010, med staten som föregångare.

Det är viktigt att på ett tidigt stadium kontrollera ifall berörda internetleverantörer kan tillhandahålla IPv6 och vilken leveranstid som utlovas. Om IPv6 inte kan tillhandahållas och leverantören inte har några planer på att införa detta inom den närmaste tiden, är det lämpligt att vända sig till någon annan internetleverantör. Det är också viktigt att vid nyanskaffning ställa krav på IPv6-stöd i all övrig berörd utrustning t.ex. brandväggar, routrar, switchar, servrar etc.

För att lösa övergången till IPv6, används lämpligen s.k. dual stack där anslutna enheter i nätverket har stöd både för IPv4 och IPv6. Detta är nödvändigt då IPv4 kommer att leva kvar under långt tid framöver på grund av äldre applikationer och utrustning som inte kan hantera IPv6. Många resurser på internet kommer enbart att vara nåbara via IPv4 under ännu ett antal år. Anslutna enheter kommer alltså genom dual stack ha en eller flera IPv4 och IPv6-adresser samtidigt, vilket ger en mer komplex miljö för nätadministration och felsökning av kommunikationsproblem. Se även bilaga2.

6.2.4 Virtual Private Networks

För att uppfylla behovet av att säkerställa kvalitet, flexibilitet och säkerhet i data, röst och videokommunikation har organisationer i mer än ett decennium investerat i s.k. VPN, Virtual Private Network som är logiskt separerat från det publika internet men som använder samma fysiska infrastruktur som internet. I den egna verksamheten ger VPN-lösningar en möjlighet att elektroniskt koppla ihop olika anläggningar/kontor med varandra i olika syften, till exempel för kommunikation maskin-till-maskin, filöverföring, röstkommunikation/telefoni, videodistribution eller en kombination av dessa. En egen VPN-lösning höjer säkerheten i kommunikationen mellan anläggningar/kontor eftersom det handlar om ett kontrollerat nät och inte ett

⁶ "Economic considerations in the management of IPv4 and the deployment of IPv6"
(<http://www.oecd.org/dataoecd/7/1/40605942.pdf>)

⁷ "IPv6 Deployment in the Public Sector"
(https://www.isoc.org/pubpolpillar/issues/ipv6_20090515.shtml)

allmänt tillgängligt. Säkerheten gäller flera olika aspekter, från intrång i kommunikationen till högre tillförlitlighet.

Behovet av kapacitet och tillgänglighet för trafik är sällan jämt fördelat över tid. Möjligheten att genom VPN kunna prioritera trafiken under vissa perioder gör att kommunikationen blir säkrare och att övrig kommunikation inte störs. Ett enkelt exempel kan vara att IP-baserad telefoni bör prioriteras framför datatrafik för att undvika att samtalet blir stört genom eko, fördröjning och hackig överföring.

Allt fler lösningar och processer kan övervakas och få support på distans. Möjligheten som VPN medger att genomföra och samordna övervakning och styrning, likväl som support över nätet, medför betydande besparingar och effektivitetsfördelar för företag, där ett eget VPN ger möjligheten till en säker tillgänglighet till processerna.

6.3 Krav för webbtjänster

Webbservrar bör ha redundant åtkomst till internet och beroende på besöksvolymerna eventuellt ha s.k. lastdelare. De bör även ha rätt dimensionering för trafiktoppar (peakar), exempelvis internetbanker i slutet av månaden och Skatteverket i deklarationstider.

Har en verksamhet alla sina namnservrar för DNS anslutna till en och samma internetoperatör spelar det egentligen ingen roll om man lägger webbservern där också. Får operatören problem med tillgängligheten blir inte bara namnservrarna utan också webbservern onåbar. Den som däremot har sina namnservrar placerade hos två olika operatörer kan också överväga att placera webbservern hos en tredje operatör för att uppnå största möjliga redundans.

För att uppnå och tillhandahålla kontinuerlig tillgänglighet till de tjänster som organisationen tillhandahåller, måste redundanta system med hög serverkapacitet användas. Den vanligaste tekniken för att uppnå detta är att skapa s.k. klustrade system, dvs. att flera servrar kopplas samman. Servrarna innehåller samma information och om en server går ned kan de övriga samarbeta för att ersätta den och klara trafikvolymen. Detta ger dels hög tillgänglighet då last kan fördelas och svarstider hållas nere, dels ett gott skydd mot överbelastningsattacker.

Servrarna kan placeras på internet eller i organisationens nätverk helst på geografiskt åtskilda platser och med IP-topologisk diversitet dvs. i olika operatörers nät.

6.3.1 Krav för skydd av kommunikation mellan webbserver och klient

Trafiken mellan webbserver och externa klienters webbläsare bör skyddas från manipulation och insyn. Med hjälp av certifikat och tillhörande krypteringsnycklar kan en webbläsare upprätta en säker, krypterad kommunikation med den aktuella webbservern. Här används Transport Layer Security (TLS) eller föregångaren Secure Sockets Layer (SSL) för att skapa en säker förbindelse mellan en webbläsare och en webbplats genom protokollet *Hypertext Transfer Protocol Secure (https)* för krypterad transport av data via http-protokollet.

6.4 Krav för DNS-tjänster

En mycket viktig funktion i internets infrastruktur är domännamssystemet (DNS). DNS är en globalt distribuerad databas av poster med domännamn kopplade till en eller flera IP-adresser med lagring i miljontals servrar. Varje till internet ansluten utrustning identifieras med hjälp av en unik IP-adress, som används för att förmedla datapaketet på internet till rätt dator. Det är DNS som gör att vi på ett användarvänligt sätt t.ex. kan "surfa" på internet. DNS är även i praktiken en förutsättning för att kunna skicka och ta emot e-post. En stor fördel med domännamn är att motsvarande IP-adress kan ändras utan att domännamnet berörs.

Verksamheter som är beroende av att vara tillgänglig via internet behöver säkerställa namnservrarnas tillgänglighet, eftersom det är dessa som pekar ut var domäner kan slås upp/finnas. Drift och administration av namnservrarna kan dels skötas av externa DNS-operatörer och dels hanteras i egen regi internt hos företag, myndigheter och andra organisationer. För exempelvis en myndighet som själv sköter driften av sina namnservrar, kan tillgängligheten ökas genom att lägga ut drift av en del sekundära namnservrar hos en eller flera externa DNS-operatörer. För ytterligare robusthet är det viktigt att namnservrarna är placerade i olika internetoperatörers nät dvs. i olika s.k. autonoma system (AS) för att få kontinuitet i DNS-funktionen trots att en av operatörerna slagits ut.

En speciell funktion har de s.k. resolverservrarna, som vanligen hanteras av internetoperatörerna och som på begäran av en enskild dator gör uppslag av domännamn exempelvis www.pts.se mot IP-adress och omvänt.

Namnservrarna bör ha den senaste versionen av DNS programvara med den senaste uppdateringen för att stå mer skyddade från logiska sårbarheter. För att

en domäninnehavare ska kunna kontrollera om den egna domänen är korrekt konfigurerad rekommenderas DNSCHECK⁸ som är ett verktyg som tagits fram och tillhandahålls av .SE (Stiftelsen för internetinfrastruktur).

I samband med att IPv6 introduceras måste man beakta att IPv6 adressernas längd och hexadecimala form gör att de blir svåra att memorera för människor, varför DNS blir en än viktigare funktion i infrastrukturen.

6.4.1 Ställ krav på stöd för DNSSEC

Användare som söker information på webbplatser eller vill använda e-tjänster behöver vara säkra på att de dirigeras till den korrekta IP-adressen för den förväntade ervern och inte någon annanstans. Den standardiserade metod som kan hantera detta kallas DNSSEC (DNS Security Extensions). Den bygger på kryptografi och digitala signaturer och gör att de s.k. resolverna, dvs. de namnservrar som utför namnuppslagningen mot DNS-databasen, kan upptäcka om adresshänvisningen till t ex en viss webbplats har förfalskats. Domännamnshavare bör därför se till att ha ställa krav på stöd för DNSSEC i berörda auktoritativa namnservrar och resolver.

Krav på DNSSEC-stöd bör finnas oavsett om DNS-tjänsterna sköts av extern part genom avtal eller om de administreras i egen regi.

Det är viktigt att den som driver en DNS-tjänst med DNSSEC klart och tydligt redovisar rutinerna för hantering av nycklar och annat material som är säkerhetskritiskt. Behovet av en allmänt känd och transparent säkerhetsnivå för DNSSEC blir därmed fyllt.

Sedan juli 2010 är roten i DNS, dvs. den högsta nivån i DNS-hierarkin, signerad. Detta innebär att hela den s.k. zonfilen för rot med alla toppdomäner, exempelvis .com .se .org har signerats av ICANN⁹ som bland annat har hand om förvaltningen av rotzonen. Det innebär i sin tur att det är möjligt att etablera en tillitskedja från en tjänst som erbjuds i en domän via DNS till en enskild användares resolver.

⁸ <http://dnscheck.iis.se/>

⁹ Internet Corporation for Assigned Names and Numbers, se www.icann.org

6.5 Krav för e-posttjänster

6.5.1 Tillgängligheten till e-postserverar måste garanteras

E-post är centralt i dagens kommunikation mellan myndigheter, företag och organisationer. Allt fler verksamheter är beroende av att e-postserverar levererar prestanda och skalbarhet som står i proportion till behovet. För att förbättra tillgängligheten till e-posttjänster gäller i stort sett samma råd som för webbservrar dvs. de bör vara speglade och klustrade.

6.5.2 Skydd mot obehörig läsning av e-post

För att säkert utbyta information mellan e-postserverar bör ett skydd på transportnivå läggas på kommunikationen. Skydd mot obehörig läsning av e-post upphandlas vanligen inte utan finns färdigt i all modern programvara och kan införas vid behov genom att använda Transport Layer Security (TLS). TLS är en standard som bl.a. kan användas för säker överföring av elektronisk post via det vanliga standardprotokollet SMTP (Simple Mail Transfer Protocol). Detta gör att någon som försöker avlyssna e-posten på vägen mellan e-postserverarna (postkontoren) inte kan läsa det som skickas. För att enkelt initiera TLS, kan kommandot/nyckelordet StartTLS användas.

För att ytterligare öka säkerheten, kan e-posten krypteras hela vägen mellan sändare och mottagare på applikationsnivå. De två vanligaste metoderna för denna typ av kryptering är PGP (Pretty Good Privacy) och S/MIME (Secure Multipurpose internet Mail Extensions).

6.5.3 Hantering av oönskad e-post

E-postoperatörer ska lämna information om och stöd för att bekämpa oönskad e-post. Ett effektivt sätt att förbättra säkerheten är att ha en policy för e-posttjänster som stipulerar att organisationen ska använda sig av metoder som syftar till att motverka spridning av oönskad e-postreklam och nätfiske (phishing). Nätfiske är en sorts skräppost med falsk avsändare som ofta har som mål att lura internetanvändare att lämna ifrån sig känslig information. Båda dessa fenomen kan bekämpas med olika metoder för att upptäcka e-post som skickas med falsk avsändaradress.

Standardprotokollet för att skicka e-post, SMTP, gör det möjligt att skicka meddelanden med valfri domän som avsändaradress. En rekommenderad metod för skydd mot e-post med falsk avsändare är Domain Keys Identified Mail (DKIM) som bygger på kryptografiska signaturer. Detta realiserar genom att avsändarens postkontor signerar all utgående post varefter mottagarna i sin tur kan validera signaturerna. Genom att använda Author Domain Signing Practices (ADSP) i kombination med DKIM för att validera signaturerna, fås

underlag för filtrering av e-postmeddelanden. DKIM och ADSP är relativt nya standarder som väntas få stor spridning.

Senders Policy Framework (SPF) är en annan äldre standard som ger domäninnehavaren en möjlighet att i DNS publicera regler som anger från vilka datoradresser e-post från domänen ska komma. Om meddelandet kommer från en sändande server som inte är publicerad i reglerna, tolkas det av den mottagande servern som att allt inte står rätt till. Däremot säger inte standarden något om vad som ska hända med e-post som filtreras bort. SPF används i mycket liten utsträckning för närvarande.

6.5.4 Skydd av e-postserverar

När användningen av e-post och mängden utbytt information ökar, blir företag mer sårbara för skadlig kod som sprids snabbt och som kan få interna rutiner och affärsprocesser att kraftigt störas på bara några minuter. I värsta fall kan dolda, riktade attacker inträffa som har utformats särskilt för att stjäla lösenord eller känslig information. Det är därför viktigt att ha produkter installerade som ger ett fullgott realtidsskydd mot kända och okända virus, maskar, trojaner, spionprogram och andra hot mot e-postserverar. Även proaktivt skydd mot snabbt uppkomna hot bör finnas för verksamhetskritiska serverar med målsättningen att medföra en minimal påverkan på systemprestanda och resurser.

Det kan också vara värt att ta hänsyn till var fysiska och logiska serverar för e-post finns placerade exempelvis i de fall där e-post skickas utanför Sveriges gräns bland annat med tanke på den s.k. FRA-lagen.

Skydd för e-post så att okända virus, maskar, trojaner, spionprogram rensas bort kan anskaffas som extern tjänst, ibland kallat mailtvätt eller spamtvätt. Risken är stor att e-posten också skickas vidare till underleverantörer av datorkapacitet med okänd kvalitet på internetanslutning och med oklar geografisk placering. Detta kan orsaka tröghet i distributionen av e-post, risk för obehörig läsning m.m. Det är därför viktigt att ställa krav på leverantören om att hanteringen sker i serverar placerade inom Sveriges gränser och att tjänsten köps av betrodda företag.

6.6 Krav på tillgänglighet för fast telefoni

För ökad tillgänglighet till den fasta telefonin kan inkommande, utgående respektive dubbelriktade linjer dedicerats på varje trunkförbindelse. Detta ökar möjligheten för inkommande och utgående samtal att erhålla access till och

från den egna abonnentväxeln. Denna anpassning sker i samråd med operatören.

En organisation som har traditionell kretskopplad telefonlösning på plats kan med fördel komplettera denna med en internetbaserad lösning och även kunna ta emot SIP-trafik från hela internet utan att telefonmässigt gå via en teleoperatör. Detta med anledning av att det finns tänkbara scenarion då en specifik teleoperatörs infrastruktur har störningar på sådant sätt att dess telefonitjänst inte är tillförlitlig medan internet-baserade tjänster fortfarande fungerar bra.

En organisation bör i samband med upphandling av en VoIP/IP-telefonitjänst ställa krav på kryptering av SIP-signalering och mediastömmar, speciellt om tjänsten är internetbaserad, på liknande sätt som man gör för e-posttjänster.

6.7 Krav på täckning, kapacitet och elförsörjning i mobiltelefoninät

Täckning och kapacitet utgör tillsammans med basstationernas elförsörjning de tre viktigaste parametrarna för hur robust ett mobilnät är. Operatörerna presenterar information om täckning på sina webbplatser. Det finns även tidningar som utför neutrala utredningar av de olika näten och som ger en bild av vilken täckning de olika operatörerna erbjuder.

När det gäller kapacitet (uttryckt i antal samtidiga samtal på given geografisk yta) är detta information som operatörerna normalt inte publicerar. Detsamma gäller hur länge basstationer fungerar vid strömavbrott. Dessa frågor får man diskutera med sin operatör eller ställa frågor om/krav på vid upphandling.

6.8 Krav på tillgång till svensk spårbar tid

Tid och frekvens eller frekvenssynkronisering spelar en väsentlig roll i dagens samhälle. I ett växande antal nätbaserade tillämpningar, är det väsentligt att känna till rätt och spårbar tid. Det kan handla om dokument och handlingar som rör e-förvaltning inom offentlig sektor, elektroniska banktransaktioner, e-handelsplatser samt allmänna kommunikationer som att bussar, tåg och flyg går i rätt tid. Det kan också handla om tidsloggar för larmsystem, system för kameraövervakning, olyckshändelser och dataintrång. Kraven på noggrannhet för tidskritiska tillämpningar som exempelvis digitala certifikat, e-legitimationer

etc. är inte entydigt bestämda men torde handla om typiskt 10 till 100 millisekunder.

För ökat oberoende och hållbarhet ska det vid anskaffning av elektronisk kommunikation ställas krav på att det via anskaffad anslutning ska gå att med Network Time Protocol (NTP) regelbundet hämta tid från de publika tidsserverna i Sverige för att få tillgång till svensk spårbar tid som benämns UTC(SP) dvs. Universal Time Co-ordinated hos Sveriges Tekniska Forskningsinstitut, SP i Borås. Dessa tidskällor är oberoende av funktioner utomlands till skillnad från GPS-systemet eller någon annan utomlands kontrollerad källa för tid. Om tid tillhandahålls av operatören, ska den likaså vara baserad på svensk spårbar tid.

7 Avtal med leverantör av elektronisk kommunikation

7.1 Avtal för önskad grad av tillgänglighet

Organisationer kan skaffa nödvändig tillgänglighet till extern elektronisk kommunikation genom att ställa krav i sitt operatörsavtal. Speciellt när kraven på tillgänglighet är höga, kan det vara bra att känna till vilka möjligheter operatörerna har att tillgodose kraven.

Att avtala om 100 procents tillgänglighet är knappast rimligt för någon organisation på grund av att det rent praktiskt skulle vara i det närmaste omöjligt för en leverantör att uppnå. Dessutom skulle en nära nog fullständig tillgänglighet bli orimligt dyr att realisera.

En god hjälp för att kunna ställa adekvata krav vid avtal är Kammarkollegiets förfrågningsunderlag Ramavtalsupphandling för datakommunikation, nätverk och telefoni¹⁰.

7.1 Viktigt att ange vad som ska omfattas av avtalet

När avtal ingås med en tjänsteleverantör/operatör är det viktigt att klargöra vad leverantören ska tillhandahålla till köparen. Detta ska tydligt framgå av kravspecifikation, uppdragsbeskrivning m.m.

Till avtalet kan kopplas så kallade Service Level Agreements (SLA) där man avtalar vilka nivåer som ska gälla för tillhandahållandet av respektive tjänst, exempelvis nivåer för tillgängligheten hos ett system och nivåer för hur snabbt ett fel ska avhjälpas. Ju viktigare en funktion är för verksamheten, desto högre bör servicenivån vara. Samtidigt är det av kostnadsskäl viktigt att inte välja onödigt höga servicenivåer eftersom det driver leverantörens kostnader och därmed påverkar priset som köparen får betala.

Till ett SLA kopplas ofta bestämmelser om att leverantören ska betala vite till köparen om leverantören inte når upp till servicenivåerna. Ett alternativ till vite som ofta är att föredra är att till leverantören exempelvis föreslå att leverantören som kompensation når upp till en servicenivå som ligger högre än vad avtalet säger och som kunden har nytta av. Andra kompensationsformer

¹⁰ www.avropa.se/upload/Bilagor/Aktuella/RAO-Komm_tjanst-2008/F%e3%b6rfr%e3%a5gningsunderlag%20Kommunikation%20som%20r%e3%a4nst.pdf

som kan förhandlas fram är att leverantören erbjuder förbättrade avtalsvillkor eller att leverantören utan kostnad erbjuder ytterligare service. För tjänster och funktioner som är verksamhetskritiska kan vitesbestämmelser ändå vara på sin plats. Det bör finnas inslag av både piska och morot i ett SLA.

Nivåerna som anges i SLA bör vara kvantifierade och därmed mätbara, till exempel att systemet ska vara tillgängligt en viss procent av tiden och att fel ska avhjälpas inom en viss tid. Det bör framgå under vilken tid man mäter nivåerna, exempelvis 24 timmar om dygnet eller under normal kontorstid. Dessutom bör man definiera vad som ska mätas. Måste systemets alla delar fungera eller räcker det med att väsentliga funktioner är tillgängliga? Ska man betrakta varje avvikelse från specifikationen som ett fel eller är det endast hindrande avvikelser som avses? Slutligen bör man klargöra hur mätningen ska genomföras och vem som ansvarar för mätningen.

7.2 Vilka avbrottstider är acceptabla?

Risikanalysen har fastställt hur långa avbrott som verksamheten kan acceptera för varje funktion. När sedan dessa krav ska omvandlas till krav på extern elektronisk kommunikation, måste hänsyn tas till eventuell egen återställning av system och utrustning.

Baserat på de tillgänglighetskrav som verksamheten ställer, exempelvis uttryckt i acceptabla avbrottstider för planerat underhåll, inställetid för leverantören för åtgärd av avbrott i tjänsten m.m., kan servicenivåer på intern utrustning och interna tjänster samt på operatörens tjänster definieras.

7.2.1 Tillgänglighet i procent av total kalendertid

Tillgänglighet (även kallat *upptid*) uttrycks ofta i procent enligt tabellen nedan. För att förenkla värderingen anges också den otillgänglighet (eller *nerid*), uttryckt i tid som det innebär på ett år – se figur 4 nedan.

Figur 4: Tillgänglighet i procent av total kalendertid

Tillgänglighet	Otillgänglighet -tid per år	Otillgänglighet – tid per månad
90 %	876 tim	73 tim
99 %	87,6 tim	7 tim 18 min
99,9 %	8,76 tim	43 min
99,99 %	0,9 tim= 54 min	4 min 30 sek
99,999 %	0,09 tim= 5,4 min	27 sek
99,9999 %	0,54 min= 32 sek	2,6 sek

Observera att krav på 99 procents tillgänglighet kan tyckas vara mycket, men det innebär en acceptans för totalt nära fyra dygns avbrott per år, utspritt över ett antal dygn under året eller sammanhängande. I avtal kan dessutom tid för planerade avbrott för service, uppgraderingar etc. vara undantagna från avtalad tillgänglighet.

Vid avbrott som drabbar många, gör operatörerna i första hand avhjälpande åtgärder för att bistå kunder med avtal om högre tillgänglighet. För kunder med lägre avtalad tillgänglighet finns risk för försenade åtgärder på grund av resursbrist hos leverantören. Det bör därför framgå av avtalet hur tjänsteleverantören ska kompensera kunden för eventuell försenad åtgärd för tillgång till fungerande avtalad elektronisk kommunikation.

7.2.2 Tillgänglighet i timmar

Ett annat sätt att uttrycka tillgänglighet är att använda timmar istället för procent som bas för beräkning av tillgänglighet och otillgänglighet vilket exempelvis används i Kammarkollegiets ramavtal¹¹ avsedda för offentlig sektor inom området elektronisk kommunikation. Detta avviker i många fall från leverantörernas standardvillkor. Syftet är att göra det enklare att följa upp den levererade tillgängligheten.

¹¹ http://www.avropa.se/templates/ramavtalsomrade_3478.aspx

Tabellen nedan i figur 5, har hämtats ur Kammarkollegiets bilaga om ”Service och tillgänglighet” för avtal om fasta och mobila operatörstjänster. Den visar de olika nivåer (klasser) som kan köpas inom ramavtalen och vilka avbrotts-tider och antal fel som respektive nivå innebär. I avtalet ska *servicetiden* anges dvs. under vilka tider eventuella fel, avbrott och störningar kan åtgärdas av operatören.

Åtgärdstid är den tid som förflyter från tidpunkten då felet anmälts alternativt upptäckts av leverantören, tills dess att felet är åtgärdat och räknas bara inom avtalad servicetid.

Avbrotts-tid är den sammanlagda tiden för att åtgärda fel. Exempel på servicetid är vardagar klockan 8.00 till 18.00 eller alla dagar dygnet runt.

Drifftid är hela den tid (inklusive servicetid) då avtalade funktioner, produkter och tjänster ska vara tillgängliga för organisationen att använda med avtalad funktionalitet.

Figur 5: Åtgärdstider

Nivå	Maximal åtgärdstid per fel under servicetid (tim)	Maximalt antal fel under servicetid per månad (antal)	Maximal avbrotts-tid per månad under servicetid (tim)	Servicetid	Drifftid
1	2	2	2	00-24 Må-Sö	Alla dagar dygnet runt
2	4	4	4	00-24 Må-Sö	Alla dagar dygnet runt
3	8	4	8	00-24 Må-Sö	Alla dagar dygnet runt
4	4	4	4	8.00-18 Må-Fr	Alla dagar dygnet runt
5	8	4	12	8.00-18 Må-Fr	Alla dagar dygnet runt
6	12	8	24	8.00-18 Må-Fr	Alla dagar dygnet runt

I figuren ovan innebär exempelvis nivå 2: Under avtalad servicetid måste fel åtgärdas inom 4 timmar, högst 4 fel per månad och avbrotts-tiden får inte överskrida 4 timmar per månad.

7.3 Avtal om fast telefoni – kretskopplad eller paketförmedlande

- Skaffa ett eller flera reservtelefonnummer till växeln, som endast används då huvudnumret är satt ur funktion. Dessa nummer bör inte vara kända för allmänheten utan bör situationsanpassas samt meddelas de som är i behov av dessa telefonnummer.
- Skaffa separata telefonabonnemang som antingen kopplas till den egna telefonväxeln för att skapa reservväg då ordinarie förbindelser sätts ur funktion alternativt kopplas helt skilt från den egna telefonväxeln vilket ger telefonifunktionen ytterligare ökad robusthet då denna kommunikationsväg fungerar även då telefonväxeln är satt ur funktion.

Om abonnentväxeln är nätgrupperad (sammankopplad) med en eller flera andra PBX:er, inom verksamheten eller i någon annan konstellation, kan konfiguration av hela telefonisystemet ske så att samtliga ingående telefonväxlar har tillgång till samtliga förbindelser inom nätgruppen.

7.4 Avtal om mobiltelefoni

Mobiltelefoni kan ses som ett reservalternativ till fast telefoni då den till stora delar använder en annan infrastruktur. Mobiltelefoni används inom alla organisationer men på olika sätt. Användningen indelas i följande användningsfall:

- Enskilda mobilabonnemang som ett komplement till fast telefoni.
- Mobiltelefoner som anknytningar i en egen PBX, kan ses som en ersättare för den fasta telefonen.
- Mobila Centrexlösningar, kan ses som en ersättare för hela den interna och externa telefonin.

Beroendet av fungerande mobiltelefoni blir olika för de tre fallen ovan och därmed blir även tillgänglighetskraven olika.

7.4.1 Avbrottsinformation

De operatörer som har egen infrastruktur publicerar information om avbrott och kapacitetsnedsättningar i realtid på sina webbplatser.

7.4.2 Åtgärder som kan vidtas för att höja tillgängligheten till mobiltelefoni

Nedan följer några förslag på åtgärder för att öka tillgängligheten:

- Skaffa reservabonnemang hos alternativ operatör. Ha en strategi för hur dessa ska användas och hur nummer ska spridas.
- Vid övergång till mobil Centrex, behåll ett antal fasta telefoner på kontoret.

Möjlighet finns även att ansluta sin PBX till en eller flera mobiloperatörers nät för att erhålla ökad funktionalitet för verksamhetens mobiltelefoner samt en bättre prisbild för mobiltelefonsamtal.

7.5 Avtal om information från operatören

7.5.1 Information vid avbrott och störningar

Organisationen bör i sitt avtal med operatören reglera kraven på information vid inträffade avbrott och störningar. I avtalet ska följande tydligt framgå:

- När, dvs. vid vilken grad av störning som organisationen ska informeras
- Hur, dvs. i vilken form informationen ska förmedlas, och till vem
- Vad informationen ska omfatta, t.ex. påverkan på avtalade tjänster, prognoser för färdigtidpunkt, faktisk färdigtidpunkt

En del operatörer rapporterar om avbrott och störningar via sina webbplatser. Denna driftinformation kan innefatta såväl planerade arbeten som aktuella störningar i olika typer av elektroniska kommunikationstjänster. För vissa organisationer kan denna information vara tillräcklig.

7.5.2 Avtal om information om driftsstatistik

I avtalet med operatören bör ingå krav på tillhandahållande av driftsstatistik såhått organisationen kan försäkra sig om att leverantören lever upp till kraven i ingångna avtal. Statistiken bör spegla villkoren i avtalet och kan exempelvis omfatta:

- Tillgänglighet i förhållande till avtalet
- Utnyttjandegrad vid olika tidpunkter och intervall (dygn, vecka, månad)
- Svarstider i kundtjänst

7.6 Vad bör beaktas vid avtal om molntjänster?

Med molntjänster eller s.k. Cloud Computing menas i detta sammanhang att man kan köra serverbaserade applikationer över internet även kallat SaaS eller Software as a Service. Det traditionella sättet att hantera applikationer är att ett företag eller en organisation installerar applikationer på egna servrar och ansvarar för drift och underhåll av både server och applikation. Alternativt överlåter man detta ansvar genom s.k. outsourcing till en leverantör av molntjänster som installerar applikationen på sina servrar samt ansvarar för drift och underhåll av både servrar och applikationer i egna datacenter. Skäl som för vissa organisationer kan tala för molntjänster är skalbarhet, dvs. man kan enkelt öka eller minska antalet användare, det går snabbt och enkelt att komma igång då programvara inte behöver installeras på kundens servrar och annan infrastruktur. För andra organisationer kan molntjänster framstå som mindre lämpligt, bland annat avseende krav på tillgänglighet, integritet och konfidentialitet.

Vid införande av molntjänster är det flera nya aspekter som man bör beakta. exempelvis:

- Hur säkerställer man prestanda och tillgänglighet på förbindelsen till molntjänstleverantörens datacenter?
- Hur redundant och robust är molntjänstleverantörens servrar anslutna till internet?
- Hur skriver man ett väl fungerande avtal och SLA?
- Hur förhindrar man inlåsning till leverantör av molntjänster?
- Hur skyddas konfidentiell och hemlig information?
- Hur skyddas integriteten?

Om molntjänster ska användas, ökar således kraven på fungerande externa anslutningar då dessa är helt avgörande för att en organisation överhuvudtaget

ska kunna använda system och applikationer som annars normalt finns internt på det lokala nätet.

När det gäller s.k. grid computing för att exempelvis utnyttja extern beräkningskraft genom hopkopplade datorer på nätet, måste liknande hänsyn tas som diskuterats ovan för molntjänster.

7.7 Övriga avtalsvillkor

I organisationers avtal med leverantörer av extern anslutning och andra tjänster, erbjuds ofta långa bindningstider och/eller uppsägningstider, ibland i kombination med sampaketering och särskilda prisvillkor. Detta gör det svårare att byta mellan de tjänsteleverantörer som finns att tillgå och att jämföra fördelarna mellan olika alternativ. Marknaden för elektronisk kommunikation präglas av en snabb teknikutveckling och förändrade prisbilder. I avtal bör därför bindnings- och uppsägningstiden inte utgöra ett hinder för möjligheten att byta tjänsteleverantör vid en tidpunkt som är lämpligast för verksamheten.

7.8 Stöd för incidenthantering

Ett gott råd till en organisation är att upprätta en kontakt med ett s.k. Computer Emergency Response Team (CERT). Vid allvarigare IT-incidenter kan organisationen behöva extern assistans med att avhjälpa de problem som uppstått. En del av denna assistans kan komma direkt från en operatör, men somliga händelser ligger helt eller delvis utanför operatörens direkta ansvar. Detta gäller speciellt om det som stör kommunikationen kommer ur innehållet i trafiken - trafiken flyter bra, så operatören gör rätt, men innehållet i trafiken stör ut de system den kommer fram till.

Exempel på IT-incidenter som kan störa den elektroniska kommunikationen är överbelastningsattacker, förvanskningar av webbplatser s.k. defacement, riktade attacker med skadlig kod eller större utbrott av skadlig kod. Delar av dessa incidenter kan eventuellt hanteras av operatör eller säkerhetspartner om man avtalat om detta, men det är också möjligt att söka hjälp av en CERT. Detta gäller i synnerhet om en incident verkar komma från internationell källa eller har någon annan än den egna operatörens kunder som ursprung. CERT:ar har ofta stora internationella och nationella nätverk bland myndigheter och privat sektor, och kan agera kontaktförmedlare mellan de drabbade och de som kan avhjälpa problemet. En del CERT:ar har egen problemlösande förmåga med anställda IT-säkerhetsexperter som kan

analysera datorer och nätverkstrafik för att hitta orsaken till och mildra effekterna av en IT-incident. CERT:ar kan också agera anonymiserande mellanhand för känslig information, om den som drabbats vill söka hjälp utan att behöva avslöja vem som drabbats. Ett exempel kan vara att man hittar problem med ett system man använder, men inte vill gå direkt till leverantören av affärsmässiga skäl.

I Sverige finns det CERT-funktioner tillgängliga både via privat sektor och via myndigheter. Den svenska stats-CERT:en och tillika alla myndigheters CERT, heter CERT-SE och har samtliga ovanstående förmågor. CERT-SE bedriver verksamhet 24/7/365 dvs. dygnet runt under årets alla dagar.

Bilaga - 1 Infrastrukturen för elektronisk kommunikation

Viktigt med robusthet på infrastrukturnivå

Infrastrukturens robusthet avgör till stor del nivån på tillgängligheten till nätet för anslutna användare. I de nationella stamnäten för elektronisk kommunikation, som är uppbyggda av optofiber eller radiolänk, pågår ständiga förbättringar för att höja robustheten allteftersom svaga punkter upptäcks.

Operatörerna utbyter trafik med varandra i nätet i fysiskt väl skyddade och vanligen dubbelanslutna knutpunkter ofta kallade IXP:er (Internet Exchange Points). För att förstärka uthålligheten är IXP:erna dessutom försedda med reservsystem för elförsörjning. I många fall, men inte alltid, finns redundans i operatörernas nät. Detta gör att man kan leda om trafik och på sätt minimera konsekvenser vid skador.

Nationellt och globalt fungerar elektronisk kommunikation genom att ett stort antal nät, som ägs och förvaltas av olika privata och statliga aktörer, fysiskt och logiskt kopplats samman. När det gäller internet har alla anslutna datorer möjlighet att kommunicera med varandra genom att samtliga använder IETF - standarden Internet Protocol (IP) för förmedling av trafiken. För att operatörerna ska få minskade driftskostnader är det sen flera år en pågående trend, att olika typer av nät konvergerar mot IP-tekniken.

Nätens infrastruktur, t.ex. fiber, koppar, radio och utrustning för transmission och routing (vägval) används för att förmedla publika IP-tjänster, exempelvis internettrafik. De används även för annan trafik och olika tillämpningar, exempelvis fast och mobil telefoni samt virtuella privata nät. Nät och nätutrustning används således för olika slags tjänster, varav vissa har garanterad tillgänglighet och kvalitet enligt avtal. Resurser för överföring av exempelvis publik IP-trafik (internettrafik) från ändpunkt till ändpunkt är varierande och oförutsägbara. Detta leder till att kvaliteten på denna trafik inte kan garanteras.

Vad ingår i infrastrukturen för elektronisk kommunikation?

Fysiska delar av infrastrukturen

Den fysiska infrastrukturens olika delar, är exponerad för mekanisk påverkan. De viktigaste komponenterna i den fysiska infrastrukturen är:

- kanalisation (rör, stolpar etc.),
- förmedlingsmedia i form koppar- och fiberkabel samt utrustning för radiokommunikation,
- änd- och förmedlingsutrustning för elektriska impulser, laserljus eller radiovågor såsom dataväxlar (switchar), routrar för vägval inom och mellan operatörers nät, nätnav (hubbar), förstärkare (repeaters), olika kontaktdon,
- knutpunktsväxlar för trafikutbyte mellan olika operatörer,
- maskinvara för namnservrar för domännamnsystemet (DNS) och för resolverservrar för uppslagningar i DNS,
- maskinvara för tidsservrar för spårbar exakt tid,
- maskinvara för servrar för utdelning av IP-adresser,
- maskinvara för servrar och övrig utrustning som används för olika tjänster (webb, e-post, radio, TV, video, telefoni m.fl.),
- hårdvara för utrustning som används för övervakning, brandväggar, analysinstrument, statistik, felsökning och loggar.

Logiska delar av infrastrukturen

Den logiska infrastrukturen såsom protokoll, operativsystem och tillämpningar för växlar och routrar är exponerad för intrång, överbelastning och manipulation. Den är dynamisk till sin karaktär dvs. kan i många fall ändras även på avstånd via nätet. Till den logiska infrastrukturen hör även personella resurser exempelvis deras kapacitet och kompetens. De viktigaste delarna i den logiska infrastrukturen är:

- operativsystem för nätverksutrustning, övervakningssystem, DNS-servrar, applikationsservrar m.m.,
- regler eller protokoll med hjälp av vilka elektronisk kommunikation sker t.ex. routing- och växlingsfunktioner för styrning av trafik mellan operatörer och inom en operatörs nät,
- programvara för översättning av domännamn till IP-adresser och omvänt dvs. DNS,

- programvara för lagring och distribution av spårbar tid, Network Time Protocol (NTP),
- programvara i änd- och förmedlingsutrustning för elektriska impulser, laserljus eller radiovågor,
- programvara för utdelning av IP-adresser m.m. såsom DHCP (Dynamic Host Configuration Protocol),
- programvara för drift, övervakning, planering, brandväggar, intrångsdetekteringssystem, loggar, analysinstrument, statistik och felsökning,
- personal för drift, övervakning, planering, brandväggar, intrångsdetekteringssystem, loggar, analysinstrument, statistik och felsökning,
- kundtjänstfunktioner inklusive personal.

Infrastrukturens säkerhet – hot och skydd

Under 1990-talet har stora investeringar genomförts för att förlägga viktiga växlar och centrala delar av transmissionsnät och styrsystem i skyddade utrymmen i form av berggrum. Idag finns ett stort antal operatörer, som har bedömts vara samhällsviktiga, förlagda i dessa berggrum. De skyddade utrymmena utgör därmed viktiga knutpunkter för elektronisk kommunikation med system för reservkraftförsörjning.

Det är viktigt att notera att ökad redundans kan vara ett komplement men också ett alternativ till ett förbättrat skydd. En viktig systemkomponent blir mindre sårbar om den skyddas och mindre kritisk om den dubblas.

För detaljerade rekommendationer avseende fysisk säkerhet, se rapporterna *Robusta noder*¹² och *Robusta nät*. Rapporterna har tagits fram i samarbete med Svenska Stadsnätetsföreningen.

För att öka domännamnsystemets motståndskraft mot hotande överbelastningsattacker, är det viktigt att tillgängligheten till namnservrarna för en zon förstärks. Detta säkerställs genom att flera kopior av zon-informationen finns på fysiskt och logiskt åtskilda nät vilka i sig har tillfredsställande överkapacitet.

Då protokollet för gränsrouting, BGP, saknar faciliteter för att garantera äkthet och källa, finns det ett hot om att falsk routinginformation kan spridas av operatörerna. Detta kan leda till att trafiken riskerar att förmedlas till felaktiga

¹² www.ssnf.org/upload/Projektdokument/robusta_noder.pdf

destinationer. Konsekvenserna kan i vissa fall bli svåra och medföra att delar av internet eller andra IP-baserade nät blir mer eller mindre otillgängliga. För närvarande saknas skydd mot falsk gränsroutinginformation men arbete pågår inom IETF för att ta fram en standardiserad lösning.

Tillgänglighet genom redundans

Det är viktigt att ha redundans på alla nivåer.

Redundans på kanalisationsnivån innebär att en kablar förläggs i fysiskt och rumsligt åtskild kanalisation.

Redundans på fibernivå och transmissionsnivån erhålls genom att det finns alternativa fibervägar i fiberstamnätet mellan två punkter. Skulle en fiber skadas kan trafiken gå i alternativ fiber. Motsvarande gäller för trådlös transmission, där redundans byggs upp genom alternativa basstationer.

Exempel på *redundans på IP-nivån* är att trafiken vid behov genom routingbeslut kan välja alternativ väg på IP-paketnivå. Redundans för nationell och global IP-kapacitet kan erhållas genom samtrafik med flera operatörer på skilda ställen i IP-nätet.

Redundans som rör DNS behandlas i avsnitt 4.6.

Redundans för applikationsnivån, exempelvis e-post och webb, beskrivs i kap 4.

Bilaga 2 - Tryggad tillgång till adresser genom IPv6

Dagens internetkommunikation bygger på protokollet IPv4, Internet Protocol version 4, och detta kommer att fortsätta dominera under flera år framöver.

I början på 90-talet insåg man att adresserna snart skulle ta slut vilket föranledde utveckling av nya regler för hur adresser skulle delas ut (CIDR¹³) samt en metod för att en stor mängd datorer kan dela på ett mindre antal IP-adresser som kan kommunicera med internet, kallad Network Address Translation (NAT). NAT var en snabb och enkel lösning på problemet med adresstillgång, men som samtidigt negativt påverkar tillgängligheten till vissa tjänster. Trots att NAT används i stor skala, har IPv4-adresserna tagit slut (februari 2011) hos Internet Assigned Numbers Authority (IANA). IANA är den funktion inom Internet Corporation for Assigned Names and Numbers (ICANN) som bland annat administrerar, förvaltar och distribuerar IP-adresser. Adresstilldelning går till så att IANA delar ut adresser till fem s.k. Regional Internet Registries (RIR). Idag vet man att adresserna hos dess RIR i sin tur kommer att ta slut någon gång under 2011 eller 2012. Det nya IPv6-protokollet, vars främsta fördel är det stora adressutrymmet, behövs för fortsatt gynnsam utveckling av och tillgång till tjänster på internet. Införande av IPv6 är ett steg som alla operatörer, tjänstetillhandahållare och konsumenter måste ta för att i framtiden kunna förmedla, tillhandahålla respektive konsumera alla slags tjänster. För operatörerna innebär stöd för IPv6 ökade kostnader, varför investeringar i IPv6-stöd görs först när tillräcklig efterfrågan finns.

Det är viktigt för organisationer som vill kunna utveckla och tillhandahålla fler tjänster på internet att se till att man får tillgång till det antal IP-adresser som verksamheten har behov av. Nu när IPv4-adresserna i praktiken är slut, behöver organisationer och operatörer kunna hantera kommunikation över såväl IPv4 som IPv6. Det är viktigt för varje verksamhet att förbereda sig och skaffa ökad kunskap om hur ens tjänster kan komma att behöva anpassas för att vara nåbara över IPv6.

IPv6 är tyvärr inte bakåtkompatibelt med IPv4. Det bästa sättet att hantera detta är att vara ansluten till internet både via IPv4 och IPv6 genom s.k. dual stack och därmed stödja båda protokollen för externt åtkomst till servrar för exempelvis webb och e-post. Ett alternativt sätt för att en IPv6-ansluten abonnent ska kunna kommunicera med en annan IPv6-ändpunkt, trots att mellanliggande nät inte känner till IPv6, är att använda sig av s.k. tunnling dvs.

¹³ Classless Inter-Domain Routing – Ger större möjlighet att partitionera subnät i mindre delar än vad som var tillåtet tidigare. IETF RFC1518, RFC1519.

IPv6-paket döljs genom att helt enkelt stoppas in i IPv4-paket som packas upp när det kommer fram till IPv6-destinationen. Ytterligare en variant är att använda olika slags funktioner för adressöversättning.

Det är viktigt att förstå att det inte är fråga om en omedelbar övergång till IPv6 där det nya protokollet ersätter det gamla. Snarare är det fråga om att ytterligare ett protokoll införs vid sidan om det befintliga, så att protokollen kommer att samexistera och måste hanteras parallellt under lång tid framöver.

Bilaga 3 - Branschstandard för DNS-tjänst med kvalitet

Nedanstående branschstandard har definierats av .SE (Stiftelsen för internetinfrastruktur) som ett led i en undersökning som ingår i ett av .SE:s satsningsområden, Hälsoläget i .se.

För den mer tekniskt bevandrade läsaren redovisas nedan i detalj vad vår branschstandard för DNS-tjänst med kvalitet innefattar i termer av rekommendationer. Den som vill testa sin egen domän kan enkelt göra det på <http://dnscheck.iis.se/>

Minst två namnservrar

Rekommendation: DNS-data för en zon bör ligga på minst två separata namnservrar. Dessa namnservrar bör av tillgänglighetsskäl vara logiskt och fysiskt separerade så att de är placerade på olika operatörsnät, i olika autonoma system (AS).

Förklaring: För varje underliggande domän skall det finnas minst två fungerande namnservrar. De skall vara listade som NS-poster för domänen i fråga. De bör vara fysiskt separerade och placerade på olika nätsegment för att högsta funktionalitet ska erhållas. Det säkerställer att domänerna fortsätter att fungera även om någon av de aktuella namnservrarna skulle sluta fungera.

Konsekvens: När den enda servern eller den enda operatören får ett avbrott blir DNS-funktionen onåbar för den domän som ligger på servern eller i operatörens nät. Därmed kan man inte heller nå tjänster hos domänen, även om dessa har placerats hos andra aktörer än den egna namnsveroperatören.

Alla namnservrar som utpekas i delegeringen ska existera i underliggande zon

Rekommendation: De NS-poster som listas i den överliggande zonen (.se eller motsvarande) för att peka ut (delegera) en viss domän skall samtliga finnas införda i den underliggande zonen.

Förklaring: I den överliggande zonen används NS-poster för att överlåta ansvaret för en viss domän till andra servrar. Denna lista av datorer skall enligt DNS-dokumentationen finnas införda även i den zonfil som "tar emot"

ansvaret, och som innehåller övriga data om zonen. Listorna måste hållas synkroniserade, så att alla NS-poster som förekommer i zonfilen för toppdomänen också återfinns i den underliggande domänen. Listan i den överliggande zonfilen uppdateras inte automatiskt, utan endast efter "manuell" anmälan till ansvarig registreringsenhet. Vid förändring som leder till behov av ändring i överliggande zon skall underliggande zons administrativa kontaktperson utan dröjsmål se till att registreringsenheten meddelas om detta.

Konsekvens: Om den överliggande zonen innehåller information om den underliggande zonen som inte existerar i den underliggande zonen innebär det att den som ställer frågor om domänen inte kan få svar, med påföljd att tillgängligheten påverkas.

Auktoritet

Rekommendation: Samtliga namnservrar som listats med NS-poster i en delegerad zon skall svara auktoritativt för domänen.

Förklaring: Vid kontroll mot servrarna för underdomänen skall man kunna få konsistenta och repeterbara auktoritativa svar för SOA- och NS-poster för underdomänen. Detta gäller samtliga servrar som finns listade i den underliggande zons DNS för domänen i fråga.

Konsekvens: DNS fungerar oftast även om detta fel existerar. Men att felet existerar i en zon tyder på bristande rutiner hos den som ansvarar för innehållet i DNS för den domänen.

Serienummer för zonfil

Rekommendation: Samtliga namnservrar som listats med NS-poster i den delegerade zonen skall svara med samma serienummer i SOA-posten för domänen.

Förklaring: Serienumret i SOA-posten är en sorts versionsnummer för zonen, och om servrarna har samma serienummer på sina zoner visar detta att de är synkroniserade. Det kontrolleras genom att fråga respektive server om SOA-posten och jämföra serienumren i svaren. SOA står för Start of Authority.

Konsekvens: Om namnservrarna inte är synkroniserade och inte har samma version av zonfilen riskerar den som ställer frågor om en domän att inte få något svar. Tillgängligheten påverkas.

Kontaktadress

Rekommendation: Zonkontaktadressen i SOA-posten skall vara nåbar.

Förklaring: I SOA-posten för en domän ingår som andra delpost en e-postadress som ska fungera som kontaktpunkt om någon behöver nå administratören för domänen i fråga. Vid enkel kontroll skall e-postservern för e-postadressen inte ge uppenbara felmeddelanden (t.ex. ”user unknown”). Vid fördjupad kontroll ska provbrev kunna sändas till adressen och dessa ska besvaras inom tre dygn.

Konsekvens: Syftet med att ha en aktuell e-postadress för kontakter är att snabbt kunna påtala problem med nåbarheten av en domän. Om sådan inte finns kan möjligheten att lösa problem som uppstår i DNS p.g.a. någon enskild domän komma att minska.

Nåbarhet

Rekommendation: Alla NS-poster i den underliggande zonen ska vara nåbara för DNS-trafik från internet.

Förklaring: NS-posterna för en domän är listan över de datorer som fungerar som namnservrar för den domänen. Samtliga uppräknade servrar ska vara nåbara från internet på alla de adresser som finns listade i motsvarande adressposter i DNS för datorerna i fråga.

Konsekvens: Om en namnservrar inte är nåbar trots att den står i listan över namnservrar som svarar på frågor om en domän, innebär det att frågeställaren inte får svar. Tillgängligheten påverkas.

Bilaga 4 - Internet Governance

Vad avses med Internet Governance?¹⁴

Internet Governance brukar vanligen kallas internets styrning och förvaltning på svenska. Det finns olika sätt att se på vad som ska/bör omfattas av begreppet Internet Governance. I denna bilaga är utgångspunkten det som diskuterats och tagits fram inom ramen för FN:s toppmöte om informationssamhället World Summit on the Information Society (WSIS) som genomförts i två faser, 2003 i Genève och 2005 i Tunis. I Tunis förhandlades den s.k. Tunisagendan¹⁵ fram, ett dokument som samlar det internationella samfundets arbete med bl.a. Internet Governance. Baserat på ett mandat från första fasens WSIS-möte (2003) tillsatte FN:s generalsekreterare en arbetsgrupp, Working Group on Internet Governance (WGIG). Den definition som WGIG tog fram, i sin rapport från juni 2005¹⁶, om vad Internet Governance är lyder som följer.

Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.

Ett resultat av WSIS var bildandet av Internet Governance Forum (IGF), som dels håller ett årligt ambuleringstredagarsforum i december, dels ett antal förmöten i Genève. IGF är ett viktigt multistakeholder¹⁷-forum för erfarenhetsutbyte och debatt öppet för alla. Genom att man kan samla och diskutera de kontroversiella frågorna på ett ställe blir det transparent och kostnadseffektivt för deltagarna.

Tunisagendans delar om Internet Governance är i mångt och mycket en kompromiss mellan de skilda uppfattningar som fanns 2005 om hur internet ska hanteras i det globala samfundet. Särskilt kontroversiell var diskussionen om kontrollen av internets s.k. kritiska resurser, dvs. IP-adresser och vissa delar av domännamssystemet (DNS). Varefter samhällen blir alltmer beroende av internet blir de också i ökande grad strategiskt viktiga resurser i infrastrukturen för elektronisk kommunikation. Det är därför viktigt hur förvaltningen av internet sker.

¹⁴ :SE (Stiftelsen för Internetinfrastruktur) har publicerat en Internetguide med titeln Styrningen av Internet för den som vill läsa mer: http://www.iis.se/docs/Styrningen-av-Internet_webb.pdf

¹⁵ *Tunis Agenda for the Information Society*, Doc: WSIS-05/TUNIS/DOC/6(Rev.1)-E. Hämtat från <http://www.itu.int/wsis/docs2/tunis/off/6rev1.html>

¹⁶ Report of the Working Group on Internet Governance, Chateau de Bossey, June 2005

¹⁷ Med multistakeholder avses här att olika organisationer tillåts att delta på liknande villkor i diskussionerna. Organisationerna kan vara regeringar/myndigheter, civilsamhället och privat sektor etc.

Utifrån den definitionen gör PTS tolkningen att när vi pratar om Internet Governance så handlar det om att olika aktörer (privat sektor, regeringar, myndigheter, föreningar, akademier etc.), utifrån sina respektive roller, på liknande villkor är delaktiga i att utveckla gemensamma principer, normer, regler, beslutsförfaranden m.m. för att forma utvecklingen och användningen av internet dvs. det handlar inte om ett uppifrån och ner perspektiv, där regeringar och myndigheter dikterar villkoren utan mer om ett gemensamt arbete. Tunisagendan¹⁸ för informationssamhället (från november 2005) framgår följande i paragraf 58.

Internet governance includes more than Internet naming and addressing. It also includes other significant public policy issues such as, inter alia, critical Internet resources, the security and safety of the Internet, and developmental aspects and issues pertaining to the use of the Internet.

Med utgångspunkt i detta kan även nedanstående områden anses omfattas av det vi kallar Internet Governance:

- toppdomäner såsom gTLD¹⁹:er, ccTLD²⁰:er IDN ccTLD²¹:er och IDN gTLD:er.
- övriga delar av domännamssystemet
- adressering, såsom IPv4²², IPv6²³
- identifiering av AS²⁴ genom ASN²⁵
- robust och säker drift av internets fysiska och logiska infrastruktur.
- frågor kring tillgång, öppenhet, mångfald (t.ex. funktionshindrades tillgång till tjänster över internet) m.m.

¹⁸ *Tunis Agenda for the Information Society*, Doc: WSIS-05/TUNIS/DOC/6(Rev.1)-E. Hämtat från <http://www.itu.int/wsis/docs2/tunis/off/6rev1.html>

¹⁹ generic Top Level Domain

²⁰ country code Top Level Domain

²¹ Internationalized Domain Name country code Top Level Domain

²² Internet Protocol version 4.

²³ Internet Protocol version 6.

²⁴ Autonomous System.

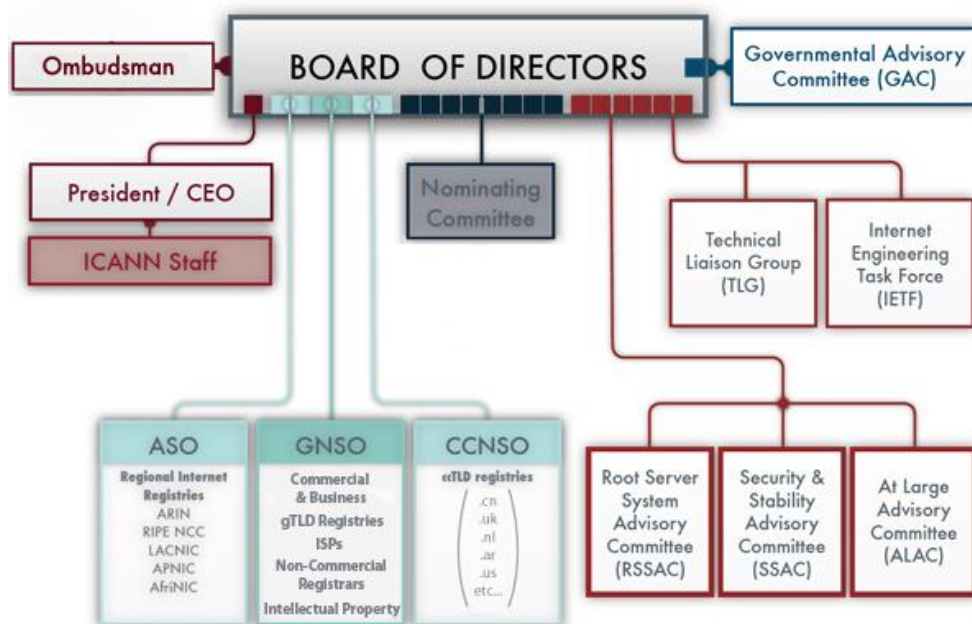
²⁵ Autonomous System Number

ICANN/GAC har kontrollen över vissa kritiska resurser

ICANN är en privaträttsligt icke vinstdrivande USA-baserad stiftelseorganisation som ansvarar för teknisk samordning och innehåll av bland annat domännamnssystemets rotzon dvs. den datafil som innehåller namnen på alla toppdomäner. Ändringar i rotzonen som föranletts av ICANN:s tilldelning/delegering av nya toppdomäner måste godkännas av US Department of Commerce (DoC) innan de kan verkställas, vilket rent operativt sker av det amerikanska företaget Verisign. Via ICANN:s IANA²⁶-funktion sker tilldelning av IP-adressblock till fem olika regionala internetregistraturer eller Regional Internet Registries (RIR), varav RIPE NCC är den som betjänar bland annat Europa.

Knutet till ICANN finns ett antal olika stödkommittéer och rådgivande kommittéer, varav GAC (Governmental Advisory Committee) är en – se figur 6 nedan. GAC är en mellanstatlig rådgivande kommitté till ICANN, öppen för regeringar och vissa andra organisationer. Figur 1 nedan illustrerar hur ICANN är strukturerat.

Figur 6 **Strukturen för ICANN**



Källa: ICANN

²⁶ Internet Assigned Numbers Authority.

Bilaga 5 - Ordlista och förkortningar

ADSP	Author Domain Signing Practices används för att validera signaturer i kombination med DKIM (se nedan) och för att upptäcka otillåten borttagning av signaturen i DKIM.
AS	Autonomt system
BGP	Border Gateway Protocol
CERT-SE	En oberoende organisation som stödjer samhället vid hot mot IT-säkerheten. CERT-SE bedömer och informerar löpande om hot mot IT-säkerheten som riskerar att drabba myndigheter, landsting, kommuner och företag. CERT-SE tillhandahåller en funktion för informationsutbyte om IT-incidenter mellan samhällets organisationer och sprider information i samhället om nya problem som kan störa IT-system. CERT-SE lämnar också information och råd om förebyggande åtgärder samt sammanställer och ger ut statistik som underlag för kontinuerliga förbättringar i det förebyggande arbetet. Hette tidigare Sveriges IT-incidentcentrum (SITIC).
DKIM	Domain Keys Identified Mail – gör det möjligt för e-postservrar att skicka och ta emot signerad e-post
DNS	Domain Name System, domännamnsystemet
DNSCheck	DNSCheck är ett verktyg som tagits fram av .SE (Stiftelsen för internetinfrastruktur) för att en domäninnehavare ska kunna kontrollera om en .se domän är korrekt konfigurerad.
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 domännamns hierarkin

Domännamn	Ett unikt namn, sammansatt av namndelar, där en i domännamnssystemet lägre placerad domän står före en högre placerad domän, t.ex. pts.se..
DoS-attack	Denial of Service-attack: Tillgänglighetsförhindrande attack, vanligen utförd genom avsiktlig överbelastning
ICANN	Internet Corporation for Assigned names and Numbers: Har bland annat ansvar för policies kring fördelningen av IP-nummer och domännamn.
ISDN-BRA	Integrated Services Digital Network - Basic Rate Access
ISDN-PRA	Integrated Services Digital Network Access – Primary Rate Access
IETF	Internet Engineering Task Force: Internationell standardiseringsorganisation för internets protokoll.
ISP	Internet Service Provider, internetoperatör som förvärvsmässigt transporterar IP-paket från avsändare som är någon annan och utanför det egna nätet till en tredje part
IP	Internet Protocol, kommunikationsprotokoll som handhar adressering, vägval och överföring av IP-paket på internet på det som kallas nätverksnivån.
IP-adress	Numerisk adress till en dator eller annan utrustning i ett IP-nät. Adressen skrivs i version 4 (IPv4) vanligen som fyra heltal åtskilda 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).
IPv6	Internet Protocol, version 6 (128-bitars IP-adress).
MSB	Myndigheten för samhällsskydd och beredskap vars uppgift är att utveckla och stödja samhällets förmåga att hantera olyckor och kriser.

NAT	Network Address Translation – Adressöversättning av publika IP-adresser (adresser routbara över internet) till privata adresser (adresser icke routbara över internet) och vice versa. NAT innebär dock problem för viss typ av kommunikation, exempelvis IP-telefoni eller VPN-förbindelser mellan företag och organisationer när adresskonflikter uppstår.
NS	Namnserver i domännamssystemet (DNS) som innehåller en databas som anger relationen mellan domännamn och IP-adress.
NS-post	Information om vilka namnservrar som svarar på frågor om en domän.
Pharming	Utförs genom manipulation av namnservrar så att översättningen mellan IP-adressen och domännamnet förfalskas så att en förövare efter eget tycke kan omdirigera en besökare från en webbplats till en annan.
Phishing	Nätfiske: en attack utförd via e-post som syftar till att samla in känslig information från internetanvändare.
Redundans	Reservkapacitet t.ex. en dubblerad extern anslutning.
Resolver	Namnserver som ställer frågor till DNS databasservrar
Robusthet	Med robusthet menas i detta sammanhang förmågan att motstå störningar och avbrott samt förmågan att minimera konsekvenserna om de ändå inträffar
RIR	Regional Internet Registry, förvaltar och delar ut IP-adressblock och andra nummer och parametrar som används på internet för en specifik region. Det finns fem RIR:ar i världen.
Routing	På nätverksnivån hanteras IP-paketens väg genom nätet av speciell utrustning, s.k. router. Routing <i>inom</i> en operatörs nät görs på grundval av ett antal tekniska parametrar, som t.ex. avstånd, fördröjning och kapacitet.

Routing *mellan* operatörernas nät sker i publika eller privata knutpunkter enligt en global standard från IETF, Border Gateway Protocol (BGP) och styrs av beslut baserade på operatörernas policy

Sitic	Se CERT-SE.
SLA	(Service Level Agreement) servicegaranti i form av ett avtal där t.ex. ett företag som tillhandahåller en internetjänst åtar sig att upprätthålla en viss kvalitet på sin tjänst med ersättningsskyldighet om tjänstetillhandahållaren inte uppfyller avtalade krav som avtalats.
Slavserver	Namnserverar i DNS som hämtar uppdaterade kopior på deras respektive zons databas från den s.k. masterservern för zonen.
Spam	Spam är det samma som skräppost, oönskade e-post-meddelanden.
Toppdomän	Nivå i DNS-hierarkin som ligger närmast under högsta nivån dvs. rot t.ex. .se, .com
UTC	Universal Time Co-ordinated – Koordinerad universell tid
Webbserver	Dator som kan kommunicera via Hyper Text Transport Protocol (http) och försedd med förmåga att presentera och distribuera lättillgänglig information till användare anslutna till internet via Hyper Text Markup Language (HTML) - sammantaget kallat www (World Wide Webb).
WiFi/WLAN	Wireless Fidelity står liksom WLAN – wireless local area network - för IEEE 802.11 standarden
Wimax	Worldwide Interoperability for Microwave Access – ett protokoll för fast och mobil trådlös kommunikation.
Zon	En zon är en del av en domän som en viss namnserver-administratör/operatör är ansvarig för. Exempelvis är PTS ansvarig för zonen pts.se som är en del av domänen .se.

Litteratur

<http://www.pts.se/sv/Dokument/Rapporter/Internet/2009/Oppna-nat-och-tjanster---PTS-ER-2009/>

<http://www.pts.se/sv/Dokument/Rapporter/Internet/2010/God-funktion-och-teknisk-sakerhet-i-stadsnat---PTS-ER-20102/>

<http://www.pts.se/sv/Dokument/Rapporter/Telefoni/2010/Allmanhetens-klagomal-till-PTS-pa-området-elektronisk-kommunikation-2009/>

<http://www.iis.se/docs/Rapport-Halsolaget-2010-101026.pdf>

http://www.iis.se/docs/E-post_att_lita_pa1.pdf

Källhänvisningar

Myndighetsanslutningar, okt 2008, Netnod

Näbarhet på nätet, Hälsoläget i .se, 2007, .SE och KBM

PTS allmänna råd om god funktion och teknisk säkerhet, PTSFS 2007:2

Robust elektronisk kommunikation - Strategi för åren 2009-2011 - PTS-ER-2009:25

Service och tillgänglighet, bilaga 4 till Fasta och mobila operatörstjänster samt transmission, 2009, Kammarkollegiet

Länkar till ramavtal inom offentlig förvaltning

<http://www.kammarkollegiet.se/it-upphandling/ramavtal/vaegledning-och-soekhjaelp>

<http://www.avropa.se/>