

# God funktion och teknisk säkerhet i stadsnät

Tillsyn av elektroniska  
kommunikationer



## **God funktion och teknisk säkerhet i stadsnät**

Tillsyn av elektroniska kommunikationer

### **Rapportnummer**

PTS-ER-2010:2

### **Diarienummer**

09-8723

### **ISSN**

1650-9862

### **Författare**

Rapporten är sammanställd av en projektgrupp ledd av Patrik Bystedt. I arbetet har Erika Hersaeus och Staffan Lindmark deltagit.

### **Post- och telestyrelsen**

Box 5398

102 49 Stockholm

08-678 55 00

[pts@pts.se](mailto:pts@pts.se)

[www.pts.se](http://www.pts.se)

## Förord

Samhället blir allt mer beroende av väl fungerande och säkra elektroniska kommunikationer, t.ex. av fast och mobil telefoni och Internet. PTS arbetar för att se till att elektroniska kommunikationer har en god funktion och teknisk säkerhet, bland annat genom tillsyn av bestämmelserna i lagen om elektronisk kommunikation.

Stadsnäten fyller en allt viktigare samhällsfunktion för tillhandahållandet av elektroniska kommunikationstjänster. PTS har därför under 2009 genomfört en planlagd tillsyn av hur bestämmelserna om god funktion och teknisk säkerhet efterlevs i stadsnäten.

I denna rapport redovisar vi resultatet av tillsynen, hur den har genomförts och vilka slutsatser vi har dragit.

Katarina Kämpe  
Stf. generaldirektör

# Innehåll

<b>Förord</b>	<b>3</b>
<b>Sammanfattning</b>	<b>6</b>
<b>Abstract</b>	<b>8</b>
<b>1 Planlagd tillsyn av god funktion och teknisk säkerhet</b>	<b>10</b>
1.1 PTS har genomfört en planlagd tillsyn	10
1.2 Syftet är att öka det förebyggande arbetet, höja beredskapen och förmågan att hantera avbrott och störningar	10
1.3 Tillsynen omfattade tio stadsnät	10
1.4 Tillsynen bestod av en enkät och intervjuer	11
1.5 Information skickad till samtliga stadsnät	11
1.6 Rapportens disposition	12
<b>2 Bestämmelser om god funktion och teknisk säkerhet</b>	<b>13</b>
2.1 Bestämmelser i LEK syftar till att skapa en grundläggande säkerhetsnivå	13
2.2 PTS allmänna råd utgör rekommendationer	13
2.2.1 Riskanalyser är en förutsättning för säkerhetsarbetet	14
2.2.2 Hantering av identifierade risker	14
2.2.3 Planering för hantering av avbrott och störningar	14
2.2.4 Uppföljning av inträffade avbrott och störningar	15
2.2.5 Genomförandet av säkerhetsarbetet styrs av tjänstetillhandahållarens förutsättningar	15
<b>3 Övergripande slutsatser av tillsynen</b>	<b>16</b>
3.1 Frågor relaterade till teknisk infrastruktur är relativt väl omhändertagna, men mer fokus bör läggas på mjuka faktorer och förebyggande arbete	16
3.2 Personberoendet behöver minskas i flera fall	17
3.3 Dokumentationen behöver utvecklas för att bättre säkerställa kvalitet, enhetlighet och kontinuitet	18
3.4 Beredskapen behöver utvecklas och formaliseras för att bättre säkerställa snabb felavhjälpning	20
3.5 Ansvar för funktion och säkerhet behöver vara tydligt i komplexa stadsnätmodeller	21
<b>4 Detaljerade slutsatser av tillsynen</b>	<b>24</b>
4.1 Det övergripande säkerhetsarbetet	25
4.1.1 Ett säkerhetsarbete bedrivs, men det bör vara mer framåtsyftande och långsiktigt	25
4.1.2 Säkerhetsarbetet bör beslutas om av ledningen	25
4.1.3 Det finns goda exempel på lokal och regional samverkan	26
4.2 Riskanalys och hantering av identifierade risker - en förutsättning för säkerhetsarbetet	27
4.2.1 Alla tillhandahållare av nät och tjänster bör regelbundet genomföra riskanalyser och ha dokumenterade rutiner	27
4.2.2 Riskanalysen bör omfatta alla delar av verksamheten, såväl teknisk infrastruktur som mjuka faktorer	28
4.2.3 Riskhanteringen är ofta informell, vilket kan leda till otydlighet och bristande uppföljning	29
4.2.4 Uppföljning bör göras för att säkerställa att beslutade säkerhetsåtgärder genomförs och får avsedd effekt	30
4.3 Hantering av avbrott och störningar	31
4.3.1 Alla tillhandahållare av nät och tjänster bör ha dokumenterade rutiner för hantering av avbrott och störningar	31
4.3.2 Rutiner och handlingsplaner bör hållas uppdaterade och testas regelbundet	31
4.3.3 En fastställd prioriteringsordning bör framgå av rutiner och handlingsplaner	32
4.3.4 Övervakning dygnet runt behövs för att snabbt upptäcka avbrott och störningar	32
4.3.5 Beredskap dygnet runt behövs för att snabbt kunna påbörja felavhjälpning	33
4.3.6 Utbildning och övningar är viktiga för att öva färdigheter, sprida kompetens och förbättra samverkan	35

4.3.7	<i>Enhetlig driftinformation behövs för kunder, samarbetspartners, allmänhet och samhällets alarmeringstjänst</i>	35
4.3.8	<i>Dokumenterade rutiner för uppföljning av avbrott och störningar saknas i stor utsträckning</i>	36
4.4	<i>Åtgärder för att förebygga vanliga orsaker till avbrott och störningar</i>	37
4.4.1	<i>Reservkraft finns för viktiga funktioner, tester bör genomföras regelbundet</i>	37
4.4.2	<i>Redundans behöver säkerställas i viktiga funktioner</i>	38
4.4.3	<i>Viktigt att säkerställa att förbindelser i centrala nät är redundanta</i>	38
4.4.4	<i>Arbetet med riskanalyser och tester före installationer och uppgraderingar bör förbättras</i>	39
4.4.5	<i>Användare och samarbetspartners bör informeras om installationer och uppgraderingar som kan påverka driftsäkerheten</i>	40
4.4.6	<i>Erfarenheter och rutiner saknas för att hantera IT-incidenter som skadlig kod och överbelastningsattacker</i>	41
4.4.7	<i>Avtal och samarbete är vanligt för att säkerställa god funktion och teknisk säkerhet i fastighets- och områdesnät</i>	41
<b>5</b>	<b>PTS fortsatta arbete relaterad till god funktion och teknisk säkerhet</b>	<b>43</b>
5.1	Fortsatt tillsyn, information och kunskapshöjande arbete	43
5.2	PTS verkar för robusta kommunikationer	43
5.3	Sitic informerar och ger råd om IT-incidenter	44

## Bilagor

<b>Bilaga 1</b>	<b>47</b>
Stadsnät som omfattades av tillsynen	47
<b>Bilaga 2</b>	<b>49</b>
Utskickad tillsynsenkät	49
<b>Bilaga 3</b>	<b>57</b>
PTS allmänna råd om god funktion och teknisk säkerhet m.m. (PTSFS 2007:2)	57

## Sammanfattning

PTS har under 2009 genomfört en planlagd tillsyn av hur bestämmelser om god funktion och teknisk säkerhet efterlevs bland stadsnät. Tillsynen omfattade 10 stadsnät och de resultat och slutsatser som presenteras i denna rapport bygger på en enkätundersökning och kompletterande intervjuer. Bestämmelserna om god funktion och teknisk säkerhet gäller för alla som tillhandahåller elektroniska kommunikationsnät- eller tjänster och syftar till att skapa en grundläggande säkerhetsnivå för elektroniska kommunikationer. Med säkerhet avses i detta sammanhang främst uthållighet, tillgänglighet och driftsäkerhet.

PTS har utfärdat allmänna råd som förtydligar bestämmelserna och utgör rekommendationer för hur säkerhetsarbetet kan bedrivas. Säkerhetsarbete innebär i detta fall att förebygga avbrott och störningar genom att genomföra riskanalyser och riskhantering, planera för hantering av avbrott och störningar samt följa upp dessa när de inträffar.

Tillsynsarbetet syftar till att öka det förebyggande arbetet, höja beredskapen och förmågan att hantera avbrott och störningar. Detta uppnås genom att öka medvetenheten om bestämmelserna, kontrollera hur de efterlevs och sprida kunskap om hur säkerhetsarbetet kan bedrivas. Den förväntade effekten av tillsynsarbetet är att det säkerhetsarbetet som tillhandahållare av nät och tjänster bedriver fortsätter att utvecklas, och är kontinuerligt, systematiskt samt framåtsyftande och långsiktigt.

Resultatet visar att alla stadsnät i tillsynen bedriver ett säkerhetsarbete. Säkerhetsfrågor relaterade till den fysiska infrastrukturen är relativt väl omhändertagna. Det framgår t.ex. av arbetet med att säkerställa redundans i elförsörjning och i viktiga förbindelser och funktioner. Övervakning av avbrott och störningar finns i regel dygnet runt, året runt, vilket är viktigt eftersom det finns ett beroende av att elektroniska kommunikationstjänster är tillgängliga dygnet runt. Det förebyggande säkerhetsarbetet med t.ex. riskanalyser, riskhantering och planering för avbrott och störning är däremot inte lika väl utvecklat.

Det är vanligt att se säkerhetsarbete som aktiviteter kopplade till teknisk infrastruktur. PTS anser att det behövs en bredare syn på säkerhetsarbetet, och att det bör omfatta alla delar av verksamheten. Det inbegriper såväl teknisk infrastruktur som mer mjuka faktorer, som t.ex. personal, kompetens, rutiner och processer. De mjuka faktorerna glöms lätt bort i sammanhanget trots att de i allra högsta grad bidrar till tjänsternas och nätens goda funktion och tekniska säkerhet. I rapporten lyfts ett antal olika mjuka faktorer fram som PTS anser bör få ökat fokus i säkerhetsarbetet.

- Personberoendet behöver minskas i flera fall

- Dokumentationen behöver utvecklas för att bättre säkerställa kvalitet, enhetlighet och kontinuitet
- Beredskapen behöver utvecklas och formaliseras för att bättre säkerställa snabb felavhjälpning
- Ansvar för funktion och säkerhet behöver vara tydligt i komplexa stadsnätmodeller

Tillsynen visar på ett antal generella förbättringsområden som tillhandahållare av nät och tjänster behöver adressera. Det är viktigt att marknadsaktörer fortsätter att öka det förebyggande arbetet, höja beredskapen och förmågan att hantera avbrott och störningar.

PTS kommer därför att fortsätta tillsynsarbetet och genomföra uppföljande tillsyn för att se att utvecklingen av säkerhetsarbetet går i önskvärd riktning. Arbetet kommer att bestå av planlagda och händelsestyrda tillsynsinsatser. PTS kommer även att fortsätta att arbeta med informations- och kunskapshöjande insatser.

## Abstract

In 2009, the Swedish Post and Telecom Agency (PTS) carried out scheduled supervision of urban networks' compliance with provisions concerning good function and technical security. This supervision encompassed ten urban networks; the results and conclusions presented in this report are based on a questionnaire and subsequent follow-up interviews. The provisions concerning good function and technical security apply to all parties providing electronic communications networks or related services and have the aim of establishing a basic level of security for electronic communications. In this context, 'security' mainly refers to sustainability, accessibility, availability and operational reliability.

PTS has issued general advice explaining these provisions and serving as recommendations for how security may be dealt with. In this case, security work means preventing interruptions, interference and disruptions by carrying out risk analyses and risk management, planning for the management of interruptions, interference and disruptions, and following these events up when they occur.

The aim of supervisory work is to raise the level of preventative work, preparedness as well as one's capacity to manage interruptions, interference and disruptions. This is achieved by increasing awareness about the provisions, monitoring compliance with them and also disseminating knowledge about how security work can be managed. The anticipated effect of supervisory work is the continuing development of security work carried out by providers of networks and services, and that this work is ongoing, systematic, forward-looking and long-term.

The results show that all urban networks encompassed by this supervision carry out activities related to security. Security issues relating to physical infrastructure are relatively well managed. For example, this has been demonstrated by efforts to safeguard redundancy in terms of the power supply and in important links and functions. As a rule, interruptions, interference and disruptions are monitored around the clock all year round, which is crucial as there is a dependence on electronic communications services being available 24/7. On the other hand, preventative security work involving (for instance) risk analyses, risk management and planning for interruptions, interference and disruptions is not as well-developed.

It is common to view security work as activities linked to technical infrastructure. PTS considers that a broader perspective is needed for security work, and that it should encompass all parts of an operation. This includes technical infrastructure as well as soft factors, such as staff, professional skills, routines and processes. Soft factors are easily forgotten in this context, despite

their key contribution to the good function and technical security of services and networks. This report highlights a number of various soft factors that, in the view of PTS, deserve a greater focus in connection with security work:

- In several cases, dependence on individuals should be reduced
- Documentation needs improvement to better ensure quality, uniformity and continuity
- Preparedness needs to be improved and formalised in order to better ensure rapid fault rectification
- Responsibility for functions and security should be defined in complex models for urban networks

The supervisory work indicates a number of general areas needing improvement that should be addressed by providers of networks and services. It is important that market stakeholders continue to increase their preventative work and raise their level of preparedness and capacity to deal with interruptions, interference and disruptions.

Consequently, PTS will continue its supervisory work and carry out supervisory follow-ups in order to ensure that security work progresses in the right direction. This work will consist of supervisory measures that are both scheduled and dictated by events. PTS will also continue its work relating to initiatives with the aim of distributing information and raising awareness.

# 1 Planlagd tillsyn av god funktion och teknisk säkerhet

## 1.1 PTS har genomfört en planlagd tillsyn

PTS har under hösten 2009 genomfört en planlagd tillsyn av bestämmelser om god funktion och teknisk säkerhet i lagen (2003:389) om elektronisk kommunikation (LEK). En planlagd tillsyn är vanligtvis av generell tematisk karaktär riktad mot flera tillhandahållare av nät eller tjänster.

Den här rapporten redovisar hur tillsynen genomförts, vilka resultat som tillsynen har gett och de slutsatser som PTS har dragit. I rapporten ges även goda exempel från tillsynen och råd för hur säkerhetsarbetet kan bedrivas.

## 1.2 Syftet är att öka det förebyggande arbetet, höja beredskapen och förmågan att hantera avbrott och störningar

Syftet med den planlagda tillsynen har i första hand varit att få en generell uppfattning om hur bestämmelser efterlevs snarare än att kontrollera efterlevnaden hos enskilda aktörer.

Mer specifikt var syftet med tillsynen

- att öka medvetenheten om bestämmelser och PTS allmänna råd om god funktion och teknisk säkerhet
- att kontrollera hur bestämmelserna efterlevs
- att sprida kunskap om hur säkerhetsarbetet kan bedrivas för att uppfylla bestämmelserna (t.ex. genom att lyfta fram goda exempel)
- för att därmed öka det förebyggande arbetet och höja beredskapen och förmågan att hantera avbrott och störningar.

Den förväntade effekten av tillsynsarbetet är att det säkerhetsarbetet som tillhandahållare av nät och tjänster bedriver fortsätter att utvecklas, och är kontinuerligt, systematiskt samt framåtsyftande och långsiktigt.

## 1.3 Tillsynen omfattade tio stadsnät

Den genomförda tillsynen var den andra planlagda tillsynen som PTS genomfört avseende bestämmelserna om god funktion och teknisk säkerhet.

Under hösten 2007 och våren 2008 genomfördes en liknande planlagd tillsyn<sup>1</sup> som omfattade 53 stycken större tjänstetillhandahållare.

Den nu genomförda tillsynen avgränsades och inriktades mot stadsnätsoperatörer. Stadsnäten fyller en allt viktigare samhällsfunktion och PTS såg ett behov av att genomföra en tillsyn för att se hur bestämmelserna efterlevs.

Totalt finns i Sverige cirka 150 stadsnät. Tillsynen avgränsades mot ett urval av dessa, totalt 10 stycken, se bilaga 1. Stadsnäten i Sverige ser olika ut. I urvalet har PTS beaktat geografiska och demografiska aspekter som var i landet stadsnätet finns och om det kännetecknas av tätort eller glesbygd. I urvalet har också beaktats faktorer som stadsnätets storlek, de tjänster som tillhandahålls och de samverkans- och affärsmodeller som finns. Ambitionen har varit att få en spridning av dessa faktorer i urvalet. Den planlagda tillsyn som genomfördes 2007-2008 innefattade fem större stadsnät. Ingen av dessa fem stadsnät omfattades av den nu genomförda tillsynen.

#### **1.4 Tillsynen bestod av en enkät och intervjuer**

De resultat och slutsatser som presenteras i denna rapport bygger på en enkätundersökning och efterföljande intervjuer vid särskilda tillsynsbesök och telefonmöten.

I september 2009 skickades en enkät ut till de 10 stadsnät som omfattades av tillsynen. Enkäten bestod av 36 frågor uppdelade i tio olika delområden, se bilaga 2.

Baserat på enkätsvaren valdes fem stadsnät ut för kompletterande intervjuer. Syftet med intervjuerna var att utifrån lämnade svar få en djupare inblick i ett antal utvalda frågeställningar. Tillsynsbesök och telefonmöten gjordes i form av presentation och diskussion av de frågeställningar som valts ut. Någon utförligare fysisk inspektion gjordes inte. Intervjuerna genomfördes under november 2009.

#### **1.5 Information skickad till samtliga stadsnät**

I samband med tillsynen genomfördes även en informationsinsats där en skrivelse tillsammans med PTS allmänna råd skickades ut till samtliga stadsnät som är anmälda hos PTS. Innehållet i skrivelsen motsvarade i stort kapitel 2 i rapporten. PTS allmänna råd utgör bilaga 3 till rapporten.

---

<sup>1</sup> God funktion och teknisk säkerhet i elektroniska kommunikationer, PTS-ER-2008:13

Syftet med informationsinsatsen var att informera om den planlagda tillsynen, att öka medvetenheten om bestämmelser och PTS allmänna råd samt att sprida kunskap om hur säkerhetsarbetet kan bedrivas för att uppfylla bestämmelserna (t.ex. genom att lyfta fram goda exempel).

### **1.6 Rapportens disposition**

Rapporten består av fem kapitel och tre bilagor. I kapitel 1 redogörs för syftet med tillsynen, hur den genomfördes och de avgränsningar som gjordes. I kapitel 2 ges en bakgrund till bestämmelserna om god funktion och teknisk säkerhet samt en beskrivning av PTS allmänna råd och vad dessa innehåller.

I kapitel 3 redovisas övergripande slutsatser av tillsynen. I kapitel 4 presenteras resultatet av tillsynen mer i detalj. Dispositionen i kapitlet följer enkätens uppbyggnad. Resultaten redovisas i aggregerad form med en analys av resultaten och en redovisning av slutsatser.

Kapitel 5 redogör för PTS fortsatta arbete relaterad till god funktion och teknisk säkerhet.

Bilaga 1 redovisar de stadsnät som omfattades av tillsynen. Bilaga 2 utgörs av den enkät som skickades till de utvalda stadsnäten. Slutligen består bilaga 3 av PTS allmänna råd om god funktion och teknisk säkerhet m.m.

## 2 Bestämmelser om god funktion och teknisk säkerhet

### 2.1 Bestämmelser i LEK syftar till att skapa en grundläggande säkerhetsnivå

I lagen (2003:389) om elektronisk kommunikation (LEK) finns bestämmelser om god funktion och teknisk säkerhet. Den 1 juli 2005 gjordes en förändring i LEK som innebär att bestämmelserna numera gäller för alla som tillhandahåller elektroniska kommunikationsnät eller -tjänster. Tidigare gällde den endast tillhandahållare av fast telefoni. Av bestämmelserna följer en allmän skyldighet att se till att verksamheten uppfyller rimliga krav på god funktion och teknisk säkerhet samt på uthållighet och tillgänglighet vid extraordinära händelser i fredstid.

Syftet med bestämmelserna är att bidra till effektiva och säkra elektroniska kommunikationsnät och -tjänster samt att skapa en grundläggande säkerhetsnivå för dessa kommunikationer. Med säkerhet avses i detta sammanhang främst uthållighet, tillgänglighet och driftsäkerhet.

I 5 kap, 6a § LEK framgår följande:

*Den som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster skall se till att verksamheten uppfyller rimliga krav på god funktion och teknisk säkerhet samt på uthållighet och tillgänglighet vid extraordinära händelser i fredstid. Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om på vilket sätt skyldigheten skall fullgöras och om undantag från skyldigheterna.*

Bestämmelserna om god funktion och teknisk säkerhet ger således ett uttryck för en grundläggande nivå av driftsäkerhet. PTS har i tillsynsarbetet inte använt bestämmelserna för att ställa utökade krav på en viss tjänstetillhandahållare eller en viss typ av tjänster. Ofta finns avtalsförhållanden mellan tjänstetillhandahållaren och de som använder tjänsterna. För de flesta tjänster är nivån på krav i sådana avtal ofta högre än den grundläggande nivån som anges i bestämmelserna om god funktion och teknisk säkerhet.

### 2.2 PTS allmänna råd utgör rekommendationer

Sedan maj 2007 finns PTS allmänna råd som förtydligar bestämmelserna om god funktion och teknisk säkerhet i LEK. Allmänna råd är rekommendationer om hur en författning bör tillämpas. De utesluter inte andra sätt att uppnå

målen i författningen. Allmänna råd bör följas om inte den som berörs av bestämmelsen kan visa att kraven i bestämmelsen uppfylls på annat sätt.

De allmänna råden om god funktion och teknisk säkerhet utgör PTS rekommendationer om hur säkerhetsarbete kan bedrivas för att uppfylla kraven i LEK. Detta bör ske genom riskanalyser och riskhantering samt planering för och uppföljning av avbrott och störningar. De allmänna råden omfattar samtliga tillhandahållare av elektroniska kommunikationsnät och -tjänster, oavsett vilken teknik som används. PTS allmänna råd utgör bilaga 3 till rapporten. I nedanstående stycken görs en sammanfattande beskrivning av dem.

### **2.2.1 Riskanalyser är en förutsättning för säkerhetsarbetet**

Riskanalyser är en grundförutsättning för ett kontinuerligt och systematiskt säkerhetsarbete eftersom det innebär att identifiera och analysera de risker en verksamhet är utsatt för.

I arbetet med riskanalyser ingår att ta fram dokumenterade rutiner för utförandet av analysarbetet samt att genomföra själva riskanalysen. Denna genomförs genom att identifiera hot och bedöma sannolikhet för, och konsekvens av, om hoten inträffar. Riskerna identifieras genom en sammanvägd bedömning av sannolikheten och konsekvensen. Det finns ett flertal metoder för att genomföra riskanalyser.

### **2.2.2 Hantering av identifierade risker**

När riskanalysen har genomförts vidtar arbetet med att hantera riskerna. I riskhanteringen ingår att fatta beslut om hur identifierade risker tas om hand.

Tjänstetillhandahållare kan välja att hantera risker på det sätt, i den utsträckning och omfattning som är lämplig med hänsyn till verksamhetens inriktning och förutsättningar. Ett sätt att hantera en risk är att vidta skyddsåtgärder för att förebygga att en störning eller ett avbrott uppstår. Ett annat sätt är att så långt som möjligt begränsa konsekvenserna när en störning eller ett avbrott väl inträffar. Ofta bidrar en skyddsåtgärd till att både minska risken för att störningar och avbrott inträffar och att begränsa konsekvenserna om så trots allt sker.

### **2.2.3 Planering för hantering av avbrott och störningar**

Genom det förebyggande arbetet med riskanalyser och riskhantering kan många säkerhetsproblem förebyggas och konsekvenserna av dem begränsas. Risken för att avbrott och störningar trots allt uppstår kan dock aldrig

elimineras helt. En verksamhet behöver därför ha en beredskap och planer för hur avbrott och störningar ska hanteras.

Detta innebär att det bör finnas dokumenterade rutiner och planer för hur organisationen, personal och ansvariga ska agera i händelse av avbrott eller störningar. Rutinerna och planerna bör ange vilka åtgärder som ska vidtas vid olika typer av avbrott och störningar.

För viktiga funktioner är planer för hantering av avbrott och störningar gällande elförsörjning, förbindelsevägar och funktionsförmåga särskilt betydelsefulla. Med viktiga funktioner avses bl.a.

- lokalstationer
- basstationer
- huvudnoder
- register för att lokalisera användare
- kunddatabaser
- namnservrar
- knutpunkter för trafikutbyte
- driftledningscentraler.

#### **2.2.4 Uppföljning av inträffade avbrott och störningar**

Det är viktigt att följa upp inträffade avbrott och störningar för att kunna dra nytta av erfarenheterna i det fortsatta säkerhetsarbetet.

I arbetet med uppföljning ingår att ta fram dokumenterade rutiner för arbetet samt att följa upp inträffade avbrott och störningar. Dessutom bör orsaker till avbrott och störningar analyseras och beaktas vid planering och utbyggnad av infrastruktur.

#### **2.2.5 Genomförandet av säkerhetsarbetet styrs av tjänstetillhandahållarens förutsättningar**

PTS allmänna råd anger att säkerhetsarbetet kan anpassas till vad som är skäligt med hänsyn till typen av risk eller avbrott och störning samt den enskilda verksamhetens inriktning och förutsättningar. Detta möjliggör för tjänstetillhandahållare att anpassa säkerhetsarbetet efter verksamhetens förutsättningar och behov.

Sammantaget bör ett systematiskt och kontinuerligt säkerhetsarbete baseras på ett återkommande arbete med riskanalys, riskhantering, planering för avbrott och störningar samt uppföljning av dessa. Detta ger en god förutsättning för att tillhandahålla elektroniska kommunikationsnät och -tjänster med god funktion och teknisk säkerhet.

## 3 Övergripande slutsatser av tillsynen

### Övergripande slutsatser av tillsynen

---

- Frågor relaterade till teknisk infrastruktur är relativt väl omhändertagna, men mer fokus bör läggas på mjuka faktorer och förebyggande arbete
- Personberoendet behöver minskas i flera fall
- Dokumentationen behöver utvecklas för att bättre säkerställa kvalitet, enhetlighet och kontinuitet
- Beredskapen behöver utvecklas och formaliseras för att bättre säkerställa snabb felavhjälpning
- Ansvar för funktion och säkerhet behöver vara tydligt i komplexa stadsnätmodeller

I detta kapitel redovisas de övergripande slutsatser som PTS drar av resultaten i den genomförda tillsynen. Mer detaljerade slutsatser som relaterar till de olika delarna i säkerhetsarbetet finns redovisade i kapitel 4.

### 3.1 Frågor relaterade till teknisk infrastruktur är relativt väl omhändertagna, men mer fokus bör läggas på mjuka faktorer och förebyggande arbete

PTS allmänna råd anger att tillhandahållare av nät och tjänster bör bedriva ett kontinuerligt och systematiskt säkerhetsarbete. Säkerhetsarbetet bör i huvudsak vara framåtsyftande och långsiktigt samt bör omfatta såväl normala driftsförhållanden som extraordinära händelser.

Alla stadsnät i tillsynen bedriver ett säkerhetsarbete. Det är oftast praktiskt inriktat. När det gäller framåtsyftande och långsiktigt säkerhetsarbete så visar tillsynen att det finns det utrymme för förbättringar. I flera fall är säkerhetsarbetet mer reaktivt och baserat på inträffade avbrott och störningar. Det förebyggande säkerhetsarbetet med t.ex. riskanalyser, riskhantering och planering för avbrott och störningar är inte lika utvecklat. Detta beskrivs utförligare i kapitel 4.

Tillsynen visar också att säkerhetsfrågor som relaterar direkt till den tekniska infrastrukturen är relativt väl omhändertagna. Det framgår t.ex. av arbetet för

att säkerställa redundans i elförsörjning, förbindelser och viktiga funktioner (se avsnitt 4.4.1-4.4.3). Detta är positivt och kan vara en följd av olika satsningar som genomförts för att öka säkerheten i den tekniska infrastrukturen, t.ex. framtagandet av Stadsnätsföreningens (SSNf) rekommendationer för uppbyggnad och dokumentation av säkra noder respektive säker kundanslutning (SKA).<sup>2</sup> Att den tekniska infrastrukturen är säker är en grundförutsättning för att säkerställa god funktion och teknisk säkerhet. Det är dock inte tillräckligt.

Som PTS konstaterade i den planlagda tillsynen 2007-2008<sup>3</sup> är det vanligt att se säkerhetsarbetet som aktiviteter kopplade till teknisk infrastruktur. PTS anser att tillhandahållare av nät och tjänster behöver ha en bredare syn på säkerhetsarbetet, och att det bör omfatta alla delar av verksamheten. Det inbegriper såväl teknisk infrastruktur som mer mjuka faktorer. Som exempel på mjuka faktorer kan nämnas personal, kompetens, rutiner och processer. De mjuka faktorerna glöms lätt bort i sammanhanget trots att dessa i allra högsta grad bidrar till tjänsternas och nätens goda funktion och tekniska säkerhet.

Som ett resultat av tillsynen har vi i fortsättningen av detta kapitel valt att lyfta fram fyra olika mjuka faktorer som vi anser bör få ökat fokus i säkerhetsarbetet. Dessa faktorer presenteras i avsnitten 3.2-3.5.

### **3.2 Personberoendet behöver minskas i flera fall**

*”Vi är en liten organisation med endast ett fåtal personer inblandade. Identifierade risker tas upp direkt med driftansvarig eller med ansvarig tekniker som är i tjänst.”*

De organisationer som driver stadsnät är i regel relativt små. I många fall består de av färre än 10 personer, i vissa fall bara ett fåtal. Detta gör att beroendet av enskilda individer kan vara stort, t.ex. driftansvariga personer eller tekniker som omnämns i citatet ovan.

Beroendet av enskilda individer innebär en sårbarhet. Skulle dessa personer bli sjuka eller byta arbete så kan konsekvensen bli att det blir svårt att upprätthålla den dagliga driften även under normala förhållanden.

Även om tillsynen bara omfattade 10 stadsnät finns det skäl att anta att det kan se likadant ut bland flera mindre stadsnät och andra mindre nätägare. Dessa behöver därför se över sitt beroende av enskilda individer och vid behov hitta lösningar för att minska detta beroende. Det finns flera olika åtgärder som kan vidtas.

---

<sup>2</sup> <http://www.ssnf.org/templates/Base.aspx?id=418>

<sup>3</sup> God funktion och teknisk säkerhet i elektroniska kommunikationer, PTS-ER-2008:13, kap. 9.4.

- Dokumentation av infrastruktur, processer och rutiner är en åtgärd som gör att beroendet av en eller ett fåtal personer minskar genom att ersättare enklare kan ta över eller avlasta i arbetet. Underlag och mallar för dokumentation av infrastruktur har t.ex. tagits fram i det s.k. SKA-projektet. Mer om dokumentation i nästa avsnitt.
- Identifiera och utse personer som är ”backup”. Det kan vara personer inom den egna organisationen eller externt, t.ex. konsulter. Ett av stadsnäten i tillsynen har ett avtal med en konsult som kan ”vidta åtgärder med kort varsel”. Denne konsult har regelbunden kontakt och är insatt i verksamheten så att konsekvenserna av resursbortfall inte behöver bli så stort.
- Utbilda och sprid kompetensen på fler individer, t.ex. personer som är backup. Jobbrotation och att genomföra övningar är ett sätt att sprida kompetensen.
- Samverkan på individnivå med andra nätägare. T.ex. kan tekniker från samverkande stadsnät ha ett utbyte för att lära sig varandras nät, processer och rutiner så att de kan hjälpa varandra om behov uppstår.
- Avtal med entreprenörer och leverantörer kan också innebära att sårbarheten i beroendet till enskilda individer minskar.

### **3.3 Dokumentation behöver utvecklas för att bättre säkerställa kvalitet, enhetlighet och kontinuitet**

I PTS allmänna råd anges att upprättade rutiner för riskanalys, riskhantering och uppföljning av inträffade avbrott och störningar bör dokumenteras och hållas uppdaterade. Vidare bör säkerhetsarbetet i huvudsak vara framåtsyftande och långsiktigt.

Nedanstående resultat av tillsynen visar dock att dokumenterade rutiner och handlingsplaner saknas i stor utsträckning.

- 7 av 10 saknar dokumenterade rutiner för riskanalys.
- 7 av 10 saknar dokumenterade rutiner för riskhantering, t.ex. rutiner som säger när säkerhetsåtgärder ska vidtas och vem som beslutar om dessa.
- 4 av 10 saknar dokumenterade rutiner och handlingsplaner för att hantera avbrott och störningar.
- 7 av 10 saknar dokumenterade rutiner för att följa upp avbrott och störningar.

Det begränsade urvalet av stadsnät i tillsynen gör att det inte går att dra några exakta slutsatser kring andelen som saknar dokumentation, men resultatet indikerar att det finns ett generellt utrymme för förbättringar.

I likhet med en del tjänstetillhandahållare i tillsynen 2007-2008 så säger sig några av stadsnäten i tillsynen vara i en tillväxtfas och ha passerat en brytpunkt för när det blir allt viktigare att dokumentera rutiner och processer. De som saknar dokumenterade rutiner anger i regel att de bedriver ett mer informellt säkerhetsarbete.

En avsaknad av dokumentation kan leda till ett reaktivt arbete som baseras på inträffade avbrott och störningar snarare än att arbeta proaktivt för att hantera nya risker och annat förebyggande arbete. När säkerhetsarbetet är informellt finns också risken att verksamheten blir personberoende och därmed sårbar om nyckelpersoner slutar eller om organisationsförändringar sker.

PTS menar att en till verksamheten anpassad och uppdaterad dokumentation bidrar till att säkerställa struktur och kontinuitet. Det underlättar att upprätthålla kvaliteten i såväl normala situationer som i mer krisartade situationer. Med dokumentation blir också säkerhetsarbetet mer enhetligt och mindre beroende av individen. Det ger också en tydlighet, t.ex. i prioriteringar av vad som ska åtgärdas först när störningar eller avbrott uppstår. Dokumentation minskar godtyckligheten. Ett av stadsnäten i tillsynen poängterar att det i en stressad situation, t.ex. vid en större störning eller avbrott, finns behov av dokumentation. De menar att denna dokumentation bör vara enkel att ta till sig, som exempelvis checklistor, eftersom det i en stressad situation är svårt att ta till sig större mängder text.

PTS anser att alla tillhandahållare av nät och tjänster bör ha dokumenterade och uppdaterade rutiner för säkerhetsarbetet. Denna dokumentation bör finnas för alla delmoment i säkerhetsarbetet (jämför med punktlistan i inledningen av detta avsnitt). För att få kontinuitet i tillämpningen och regelbunden översyn av dokumentationen är det också viktigt att ”bygga in” dokumentationen i den löpande verksamheten. T.ex. genom att löpande följa upp att dokumentation görs och används samt att med regelbundenhet se över att dokumentmallar är ändamålsenliga och uppdaterade. Genom dokumenterade rutiner säkerställs att säkerhetsarbetet blir kontinuerligt och systematiskt. Det blir därigenom också mer enhetligt och mindre personberoende.

Några av stadsnäten i tillsynen anger att de håller på eller planerar att upprätta dokumenterade rutiner för säkerhetsarbetet. Ett av stadsnäten konstaterar att de ser behovet, men är osäkra på var de ska börja och var de ska lägga nivån på dokumentationen. Det finns således också ett visst behov av vägledning i arbetet med att dokumentera.

I arbetet med att upprätta, utveckla och uppdatera dokumentation för säkerhetsarbetet kan olika åtgärder genomföras.

- Ta fram lämpliga rutiner och dokumentation i samverkan med andra nätägare. Detta skulle t.ex. kunna göras inom ramen för SSNf:s verksamhet eller på regional nivå. Ett av stadsnäten i tillsynen tyckte att det vore bra om det fanns mallar som de kunde få och nämnde att t.ex. SSNf skulle kunna verka för att ta fram sådana.
- Utbildning och stöd i tillämpning av dokumentation och metodik kan också med fördel göras i samverkan med andra nätägare. Några av stadsnäten i tillsynen hade goda erfarenheter av liknande regionala initiativ för att genomföra s.k. hälsotester och certifieringar av nät (se avsnitt 4.1.3).
- Att genomföra övningar, t.ex. i form av skrivbordsövningar är ett sätt att göra en översyn av dokumentationen.
- Lära av angränsande verksamheter, t.ex. vad gäller metodik och dokumentation. Stadsnät som drivs i kommunal regi är ofta nära organiserade med andra kommunala verksamheter, t.ex. energi-verksamheten. Rutiner och metoder för t.ex. riskanalyser är ofta generella och kan ofta tillämpas i andra verksamhetsområden. Ett sätt för ”att komma igång”, kan vara att se om rutiner och dokumentation från andra kommunala bolag kan användas och anpassas till stadsnätsverksamheten. Några av stadsnäten i tillsynen har gjort detta.

### **3.4 Beredskapen behöver utvecklas och formaliseras för att bättre säkerställa snabb felavhjälpning**

Resultatet av tillsynen (se avsnitt 4.3.5) visar att flera stadsnät har en inte helt utvecklad beredskap, som till stor del bygger på frivillighet bland tekniker i den ordinarie organisationen. Det kan handla om en eller två personer som har denna uppgift. Dessa stadsnät saknar i regel en formell organisering och rutiner för beredskapen. Ett stadsnät i tillsynen svarade också att larm som kommer nattetid noteras utan omedelbar åtgärd.

PTS ser risker i att beredskapen inte är ordentligt organiserad utan i vissa fall bygger på frivillighet. Den behöver utvecklas och formaliseras för att säkerställa snabb felavhjälpning. Elektroniska kommunikationstjänster används dygnet runt. Beroendet och förväntan på tillgängligheten till tjänsterna är stort. Avbrott och störningar kan också ske dygnet runt. Telefonitjänster används t.ex. för att ringa nödsamtal eller för trygghetslarm. Det är därför tidskritiskt att upptäcka eventuella avbrott och störningar och snabbt kunna påbörja felavhjälpning.

PTS anser därför att alla tillhandahållare av nät och tjänster behöver ha en övervakning och beredskap dygnet runt för att snabbt kunna upptäcka avbrott och störningar och påbörja felavhjälpning.

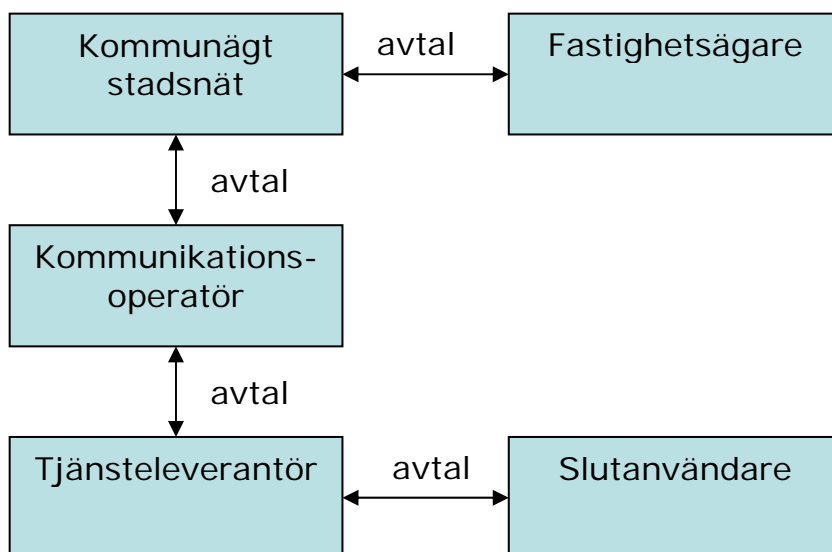
Hur utformningen av beredskapen bör se ut beror av den enskilda verksamhetens förutsättningar. Mindre nätägare har i regel inte samma resurser som större. Det finns dock åtgärder som kan vidtas för att stärka beredskapen.

- Samutnyttja med befintlig jourverksamhet i andra verksamhetsområden som VA-jour, el-jour eller liknande. Flera av stadsnäten i tillsynen har sådana lösningar.
- Utbilda jourpersonal så att den kan utföra vissa felavhjälpande åtgärder. Som exempel kan nämnas att ett stadsnät i tillsynen har utbildat personer i el-jouren så att dessa kan laga fiber om kabelbrott skulle uppstå.
- Avtala med annan part, t.ex. med lokala eller regionala entreprenörer, som snabbt kan påbörja felavhjälpning är en annan åtgärd.
- Samverka med andra nätägare för gemensam beredskap. Jämför med åtgärder för att minska personberoende i avsnitt 3.4. Genom utbyte och samverkan ökas kunskap om nät, processer och rutiner ökas förutsättningar för en gemensam beredskap.

### **3.5 Ansvar för funktion och säkerhet behöver vara tydligt i komplexa stadsnätmodeller**

Stadsnätmodeller är ofta komplexa konstruktioner med flera parter inblandade. Det finns flera olika affärsmodeller, så också bland de stadsnät som omfattats av tillsynen. Oavsett vilken modell som används anser PTS att det är viktigt att säkerställa en tydlig ansvarsfördelning avseende god funktion och teknisk säkerhet.

Nedan är ett exempel på en modell med ett kommunägt stadsnät som upphandlat en kommunikationsoperatör och som i sin tur avtalar med olika tjänsteleverantörer. Tjänsteleverantören har i denna modell avtal med slutanvändare, ibland används begreppet att tjänsteleverantören äger slutkundsrelationen.



Krav på funktion och säkerhet samt ansvarsfördelning bör framgå av avtal

Mellan de olika parterna sluts vanligtvis avtal. Bilden kan kompliceras ytterligare då det kan finnas olika varianter av modellen. Olika parter också kan välja att spela olika roller. T.ex. kan det kommunägda stadsnätet själv ta rollen som kommunikationsoperatör, och ibland även leverera tjänster till slutanvändare.

PTS vill betona att bestämmelserna om god funktion och teknisk säkerhet gäller för alla som tillhandahåller allmänt tillgängliga elektroniska kommunikationsnät eller –tjänster. Detta gäller oavsett vilken teknik eller affärsmodell som används (se vidare i kapitel 2). I modellen ovan innebär det att såväl det kommunala stadsnätet, kommunikationsoperatören som tjänsteleverantörer omfattas av bestämmelserna.

För att tillhandahålla nät och tjänster med god funktion och teknisk säkerhet bör detta konkretiseras i form av krav, t.ex. i form av tillgänglighet, prestanda, övervakning, respons- och åtgärdstider. Dessa krav bör specificeras i avtal mellan respektive part. T.ex. kan nätägaren (det kommunägda stadsnätet) ställa krav vid upphandling av och i avtal med kommunikationsoperatören. På samma sätt kan kommunikationsoperatören ställa krav i avtal av tjänsteleverantörer, eller stadsnätet i avtal med fastighetsägare (se vidare avsnitt 4.4.7). Slutanvändare bör också ställa krav på funktion och säkerhet i avtal med tjänsteleverantören. För att få en helhet är det viktigt att bestämmelser och de krav som respektive part ställer på nät och tjänster säkerställs i hela modellen.

I avtal bör även en tydlig ansvarsfördelning framgå. I komplexa modeller som denna kan det finnas oklara ansvarsförhållanden. Detta kan leda till en otydlighet kring vem som ansvarar för vad. Till exempel vem slutanvändaren ska kontakta vid avbrott och störningar eller vem som ansvarar för att åtgärda olika problem i nät och tjänster. När flera aktörer är inblandade finns det också en risk att problem eller ärenden ”fastnar” vid överlämningar eller en oklarhet för vem som har ansvaret i en viss fråga. Konsekvensen kan då bli att det tar längre tid att åtgärda ett problem.

För att säkerställa god funktion och teknisk säkerhet i stadsnätmodellen bör följande aktiviteter genomföras.

- Krav på funktion och säkerhet identifieras, konkretiseras och formuleras.
- Tydliga ansvarsförhållanden och rutiner överenskommas. Vem ansvarar för vad? Vem ska kontaktas i vilket fall? Hur ska detta ske?
- Eskaleringsrutiner och problemlösningsmodeller tas fram.

Detta bör specificeras i avtal.

## 4 Detaljerade slutsatser av tillsynen

Urval av detaljerade slutsatser av tillsynen

---

### Det övergripande säkerhetsarbetet

- Ett säkerhetsarbete bedrivs, men det bör vara mer framåtsyftande och långsiktigt

### Risakanalys och riskhantering

- Alla tillhandahållare av nät och tjänster bör regelbundet genomföra riskanalyser och ha dokumenterade rutiner
- Riskanalysen bör omfatta alla delar av verksamheten, såväl teknisk infrastruktur som mjuka faktorer
- Riskhanteringen är ofta informell, vilket kan leda till otydlighet och bristande uppföljning

### Hantering av avbrott och störningar

- Alla tillhandahållare av nät och tjänster bör ha dokumenterade rutiner för hantering av avbrott och störningar
- Övervakning dygnet runt behövs för att snabbt upptäcka avbrott och störningar
- Beredskap dygnet runt behövs för att snabbt kunna påbörja felavhjälpning
- Enhetlig driftinformation behövs för kunder, samarbetspartners, allmänhet och samhällets alarmeringstjänst
- Dokumenterade rutiner för uppföljning av avbrott och störningar saknas i stor utsträckning

### Åtgärder för att förebygga vanliga orsaker till avbrott och störningar

- Reservkraft finns för viktiga funktioner, tester bör genomföras regelbundet
- Redundans behöver säkerställas i viktiga funktioner och i centrala nät
- Arbetet med riskanalyser och tester innan installationer och uppgraderingar bör förbättras
- Avtal och samarbete är vanligt för att säkerställa god funktion och teknisk säkerhet i fastighets- och områdesnät

## **4.1 Det övergripande säkerhetsarbetet**

I detta kapitel redovisas resultaten från enkäten och intervjuer avseende frågor om det övergripande säkerhetsarbetet. I enkäten motsvarar det frågorna 1-2. Bestämmelser och PTS allmänna råd som relaterar till dessa frågor framgår av kapitel 2.

### **4.1.1 Ett säkerhetsarbete bedrivs, men det bör vara mer framåtsyftande och långsiktigt**

I PTS allmänna råd anges att tjänstetillhandahållaren bör bedriva ett kontinuerligt och systematiskt säkerhetsarbete. Säkerhetsarbetet bör i huvudsak vara framåtsyftande och långsiktigt samt bör omfatta såväl normala driftsförhållanden som extraordinära händelser.

Alla stadsnät som omfattades av tillsynen bedriver ett säkerhetsarbete. Detta är ofta praktiskt inriktat. När det gäller framåtsyftande och långsiktigt säkerhetsarbete så finns det dock utrymme för förbättringar. I flera fall är säkerhetsarbetet mer reaktivt och baserat huvudsakligen på inträffade avbrott och störningar. Det förebyggande säkerhetsarbetet med t.ex. riskanalyser, riskhantering och planering för avbrott och störningar är inte lika utvecklat.

Tillsynen visar också på goda exempel av ett kontinuerligt och systematiskt säkerhetsarbete. En nätägare anger t.ex. att de bedriver ett säkerhetsarbete i samarbete med sina leverantörer. I avtalen med dessa har de angivit grundläggande krav för hur säkerhetsarbetet ska genomföras. Detta arbete vidareutvecklar de sedan i samverkan med leverantörerna. Som exempel på långsiktigt arbete nämns årsvisa planer för att förbättra robustheten i nätet. Månadsvis gör de en genomgång av alla uppkomna ärenden (fel, störningar, planerade arbeten, aktuella leveranser m.m) för att dra lärdom av dessa och förhindra att störningar uppstår igen. Behov av förändringar och utbyggnader diskuteras också. På veckobasis hålls möten där de går igenom uppkomna störningar och problem. PTS anser att detta är ett bra exempel på hur säkerhetsarbetet kan göras mer framåtsyftande och långsiktigt.

### **4.1.2 Säkerhetsarbetet bör beslutas om av ledningen**

Resultatet av tillsynen visar att i de flesta fallen fattas beslut om säkerhetsarbetet på ledningsnivå. Det kan bero på att de organisationer som driver näten ofta är små vilket underlättar för ledningen att vara involverad i säkerhetsarbetet. Detta är positivt och i linje med PTS allmänna råd som anger att upprättade dokument för säkerhetsarbete bör beslutas om på ledningsnivå i organisationen och följas i verksamheten.

I vissa fall tas beslut om rutiner och handlingsplaner av kommunstyrelsen. När så sker är det viktigt att arbeta med förankring hos dem som utför det löpande arbetet. Ett stadsnät i tillsynen konstaterade t.ex. att rutiner och handlingsplaner finns på en övergripande nivå, men att säkerhetsarbetet behöver ytterligare implementering ute i organisationen för att bli mer levande och systematiskt.

Om säkerhetsarbetet sker löpande utan beslutsfattande på ledningsnivå är risken stor att det blir personberoende och inte enhetligt. Det finns även en risk att ledningen inte blir medveten om de risker som finns och de åtgärder som behöver vidtas, och därmed inte ger frågorna tillräcklig prioritet. Att säkerhetsarbetet blir beroende av nyckelpersoner är en risk i sig. Om dessa försvinner och säkerhetsarbetet inte är inarbetat och dokumenterat riskerar det att urholkas. Detta är beskrivet mer utförligt i avsnitt 3.3.

PTS anser att säkerhetsarbetet bör beslutas om på ledningsnivå. Oavsett verksamhetens storlek, inriktning och förutsättningar behöver ledningen involveras och känna ett ägarskap för säkerhetsarbetet. De styrdokument och policyer som ledningen beslutar om behöver också konkretiseras till nivåer som kan tillämpas i det löpande arbetet. Annars finns en risk att personalen inte känner till dem och att de inte används. Ett sätt att undvika detta kan vara att integrera styrdokument och policyer i andra dokument och processer.

#### **4.1.3 Det finns goda exempel på lokal och regional samverkan**

Samverkan med andra tillhandahållare av nät och tjänster är ett sätt att få tillgång till mer resurser och kompetens och för att få en gemensam, enhetlig syn på god funktion och teknisk säkerhet.

Tillsynen visar på goda exempel av lokal och regional samverkan. I ett fall sker en viss koordinering av säkerhetsarbetet på regional nivå. Inga avtal tecknas mellan stadsnäten (kommunerna) utan samverkan sker genom samordning och kontinuerlig dialog. T.ex. så drivs för närvarande ett gemensamt projekt där ett syfte är att undersöka kvaliteten och säkerheten i stadsnäten. I ett s.k. hälsotest görs en bedömning om nätet klarar kraven för att distribuera tjänster, t.ex. triple play tjänster, och att det lever upp till de s.k. SKA-kraven. Vid behov föreslås åtgärder för att leva upp till dessa krav. I regionen poängteras vikten av att få ett enhetligt kvalitetstest för att få en jämförbarhet. Samverkan i form av liknande hälsotester nämndes av ett annat stadsnät i tillsynen som tillhör en annan region. I ett tredje fall finns en lokal samverkan mellan grannkommuner för att säkerställa prestanda i stadsnätet vid utrullning av TV-tjänster.

PTS ser positivt på lokal, regional och nationell samverkan. Som nämndes i kapitel 3 kan samverkan t.ex. vara ett sätt att minska personberoende, att utveckla och uppdatera anpassad dokumentation samt att utveckla och formalisera beredskapsfunktionen.

## **4.2 Riskanalys och hantering av identifierade risker - en förutsättning för säkerhetsarbetet**

I detta avsnitt redovisas resultaten från enkäten och intervjuer avseende frågor om stadsnätens arbete med riskanalyser och hantering av identifierade risker. I enkäten motsvarar det frågorna 3-8. Bestämmelser och PTS allmänna råd som relaterar till dessa frågor framgår av kapitel 2, se t.ex. avsnitt 2.2.1 och 2.2.2.

### **4.2.1 Alla tillhandahållare av nät och tjänster bör regelbundet genomföra riskanalyser och ha dokumenterade rutiner**

4 av 10 stadsnät i tillsynen svarade att de inte genomför riskanalyser. Av de sex stadsnät i tillsynen som genomför riskanalyser svarade hälften att de inte har dokumenterade rutiner för hur riskanalysen ska genomföras. Tillsynen indikerar således att det finns utrymme för förbättringar. Två av stadsnäten som svarade att de inte genomför riskanalyser anger liknande anledningar till detta, nämligen att de anser att verksamheten är under uppbyggnad och har en mer praktisk och informell riskhantering. Någon dokumentering av risker eller uppföljning görs inte.

PTS menar att denna argumentation inte håller utan anser att samtliga tillhandahållare av nät och tjänster bör genomföra riskanalyser. Detta oavsett vilken typ av nät eller tjänst som tillhandahålls eller vilken storlek och inriktning verksamheten har. Riskanalys är en grundförutsättning för ett kontinuerligt och systematiskt säkerhetsarbete eftersom det innebär att identifiera och analysera de risker en verksamhet är utsatt för. Hur riskanalyser genomförs och i vilken omfattning bör dock anpassas till den enskilda verksamhetens förutsättningar och behov.

Tillsynen visar också på några goda exempel på hur riskanalyser genomförs. Ett stadsnät anger t.ex. att de inventerar scenarier och bedömer konsekvenser (tillgänglighet och kostnader) värderad utifrån typ av kommunikation. Riskanalyser genomförs vid nya affärer, nya tekniska lösningar, i samband med förstärkningsarbete eller som konsekvens av störningar. Ett annat stadsnät har en modell för risk- och sårbarhetsanalys. De genomför riskanalyser vid förändringar av arbetssätt och rutiner samt vid genomförande av större projekt. Deras kunder efterlyser ibland riskanalyser t.ex. vid större byggnationer. De genomför även riskanalyser när de ska samarbeta med viktiga partners, i samband med kontraktsskrivandet.

I PTS allmänna råd anges att riskanalyser bör genomföras avseende kommunikationsnätets och -tjänstens funktionsförmåga. De bör genomföras regelbundet samt vid förändringar som i betydande omfattning påverkar förutsättningarna för verksamheten. Vidare bör upprättade rutiner och handlingsplaner, resultat och bedömningar inom ramen för riskanalysen dokumenteras och hållas uppdaterade.

Det finns ett flertal olika metoder för genomförande av riskanalys, såväl enkla som mer omfattande. Exempel på olika metoder är minirisk, SBA<sup>4</sup>, Octave<sup>5</sup>, Lichtenberg<sup>6</sup>, FMEA<sup>7</sup> och Ishikawadiagram (fiskbensdiagram). 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. Att riskanalysarbetet utgör en del av den löpande verksamheten, som t.ex. projektmodeller och processbeskrivningar, har fördelen att det gör att riskanalyser genomförs med regelbundenhet. En av de enklaste modellerna för riskanalys 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 att 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. Hantering av risker beskrivs ytterligare i avsnitt 4.2.3.

För att strukturera riskanalysarbetet kan det också 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.

- Yttre hot (t.ex. av legal, politisk eller marknadsmässig karaktär)
- Interna processer (t.ex. metoder, styrparametrar, uppföljning)
- Ekonomiska/finansiella risker
- Humankapital (t.ex. personal, kompetens och kultur)
- Tekniska system och lösningar

#### **4.2.2 Riskanalysen bör omfatta alla delar av verksamheten, såväl teknisk infrastruktur som mjuka faktorer**

Resultatet av tillsynen visar att riskanalyser ofta inriktas på det som är konkret, i första hand teknisk infrastruktur som nätverk, förbindelser, noder, servrar, olika nätverkselement m.m. Den tekniska infrastrukturen är viktig. Men den är inte heltäckande i säkerhetsarbetet. De mjuka faktorerna glöms lätt bort i

---

<sup>4</sup> Riskanalysmetod (förkortning av sårbarhetsanalys), se t.ex. <http://www.dfs.se/products/sba/>

<sup>5</sup> Operationally Critical Threat, Asset, and Vulnerability Evaluation, se t.ex. <http://www.cert.org/octave/>

<sup>6</sup> Riskanalysmetod, se t.ex. <http://www.personly.dk/Lichtenberg1.htm>

<sup>7</sup> Failure Mode Effect Analysis, se t.ex. <http://www.sis.se/upload/632905563861067870.pdf>

sammanhanget trots att dessa i allra högsta grad bidrar till tjänsternas och nätens goda funktion och tekniska säkerhet. Med mjuka faktorer avses faktorer som personal, nyckelpersonsberoende, kompetens och processer.

Det finns några goda exempel på stadsnät i tillsynen som beaktar mjuka faktorer i sina riskanalyser. Ett stadsnät nämner t.ex. att riskanalyserna omfattar även organisation, rutiner och processer.

PTS anser att alla delar i verksamheten, såväl teknisk infrastruktur som mer mjuka faktorer, som har påverkan på tjänsternas och nätens goda funktion och tekniska säkerhet bör omfattas av riskanalyser.

#### **4.2.3 Riskhanteringen är ofta informell, vilket kan leda till otydlighet och bristande uppföljning**

Resultatet av tillsynen indikerar att riskhanteringen ofta är informellt inriktad. 7 av 10 nätägare uppgav att de saknar dokumenterade rutiner för riskhantering, t.ex. när säkerhetsåtgärder ska vidtas och vem som beslutar om dessa. I några fall tas identifierade risker upp direkt med driftansvariga personer eller tekniker. I vissa fall rapporterar driftansvarig till affärsansvarig person för beslut om hur risken ska hanteras.

PTS ser risker i att ha en informell riskhantering och anser att dokumenterade rutiner för riskhantering bör upprättas. En 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. I tillsynssvaren framgår att det ibland sker en överlämning av arbetet från den som identifierat risken till den som fattar beslut och ibland även till den som ska genomföra en åtgärd. I en sådan situation är dokumentationen viktig så att ingen väsentlig information går förlorad och att det går att följa upp.

Tillsynen visar också på goda exempel på hur risker hanteras. I ett sådant exempel anges att risker, som bedöms som akuta, åtgärdas skyndsamt efter en planering och analys av lämplig åtgärd. Efter beslut om åtgärd görs en uppföljning för att säkerställa att åtgärden är genomförd och att den gett önskat resultat. Samtliga åtgärder dokumenteras.

I PTS allmänna råd anges att identifierade risker bör hanteras på det sätt och i den utsträckning och omfattning som är skäligt med hänsyn till typen av risk samt den enskilda verksamhetens inriktning och förutsättningar, omfattning och betydelse. Rutinerna för riskhantering bör, på samma sätt som för riskanalyser, anpassas så att de går att tillämpa på såväl små som stora objekt eller företeelser.

Frageställningar som bör framgå i en riskhantering är bl.a.

- Vilka risker ska hanteras?  
Valet bör grundas på en bedömning och prioritering/klassificering utifrån genomförd riskanalys.
- Hur ska dessa risker hanteras?  
Ska säkerhetsåtgärder vidtas i syfte att undvika att risken inträffar, eller ska säkerhetsåtgärder planeras för att kunna vidtas i syfte att begränsa konsekvenser när risken väl inträffar?
- Vem äger risken?  
Vem ansvarar för att olika aktiviteter (t.ex. säkerhetsåtgärder) genomförs?
- När ska dessa aktiviteter vara klara?  
Detta kan t.ex. tydliggöras i en konkret handlingsplan.
- Hur ska aktiviteterna följas upp och verifieras?

Ett sätt att arbeta med riskhantering är att kvantifiera risker i ekonomiska termer. För respektive risk bedöms konsekvenserna av om risken inträffar och beräknas i ekonomiska termer. Genom att kvantifiera på detta sätt kan beslutsfattandet beträffande riskhanteringen förenklas. Detta eftersom det går att bedöma nyttan (undvikande av kostnaden om risken skulle inträffa) i förhållande till kostnaden av att genomföra en säkerhetsåtgärd för att eliminera eller begränsa risken.

#### **4.2.4 Uppföljning bör göras för att säkerställa att beslutade säkerhetsåtgärder genomförs och får avsedd effekt**

En viktig aktivitet i riskhanteringen är att följa upp att beslutade säkerhetsåtgärder genomförs och får den effekt som avsetts. Flera av stadsnäten i tillsynen uppgav att de har en regelbunden uppföljning. Den genomförs på olika sätt. Några hanterar det löpande i möten. Andra har projektstyrningsmodeller de följer för större åtgärder.

PTS anser att alla tillhandahållare av elektroniska kommunikationsnät och tjänster bör följa upp att beslutade säkerhetsåtgärder genomförs och får avsedd effekt. Genom att dokumentera och konkretisera riskhanteringen i aktiviteter och åtgärdsdokument underlättas uppföljningen. Ett sätt är att i regelbundna möten med riskägare och säkerhetsansvariga följa upp att beslutade säkerhetsåtgärder vidtas.

### **4.3 Hantering av avbrott och störningar**

I detta avsnitt redovisas resultaten från enkäten och intervjuer avseende frågor om hantering och uppföljning av avbrott och störningar. I enkäten motsvarar det frågorna 9-20. Bestämmelser och PTS allmänna råd som relaterar till dessa frågor framgår av kapitel 2, se t.ex. avsnitt 2.2.3 och 2.2.4.

#### **4.3.1 Alla tillhandahållare av nät och tjänster bör ha dokumenterade rutiner för hantering av avbrott och störningar**

Genom det förebyggande arbetet med riskanalyser och riskhantering kan många säkerhetsproblem förebyggas och konsekvenserna av dem begränsas. Risken för att störningar och avbrott trots allt uppstår kan dock aldrig elimineras helt. Det behövs därför en organisatorisk beredskap och planer för hur avbrott och störningar ska hanteras. I PTS allmänna råd anges att tjänstetillhandahållare bör upprätta dokumenterade rutiner och handlingsplaner med åtgärder som ska vidtas vid avbrott och störningar.

6 av 10 stadsnät i tillsynen uppgav att de har dokumenterade rutiner och handlingsplaner för att hantera avbrott och störningar. Av tillsynen framgår vidare att av dem som saknar dokumenterade rutiner i vissa fall har en mer informell hantering. Ett svar som indikerar detta var att ”alla känner alla i en liten organisation och de som arbetar med frågorna vet hur de ska agera”.

PTS anser dock att alla tillhandahållare av nät och tjänster, oavsett storlek, bör ha dokumenterade rutiner som tydliggör hur avbrott och störningar ska hanteras. Avbrott och störningar kan uppträda när som helst på dygnet och kräver ofta omedelbar hantering. Hanteringen behöver vara enhetlig, personoberoende och bygga på fastställda principer som bestämmer prioritering, ansvarsfördelning, eskalering osv. För att detta ska fungera är dokumentation nödvändig. I de fall större incidenter, avbrott och störningar inträffar så innebär det dessutom ofta en pressad situation för de inblandade. En konkret och vägledande dokumentation kan i sådana fall underlätta hanteringen.

#### **4.3.2 Rutiner och handlingsplaner bör hållas uppdaterade och testas regelbundet**

Det är viktigt att upprättade rutiner och handlingsplaner hålls uppdaterade. Ett sätt att verifiera detta är att kontinuerligt testa dem. Tester kan ske genom olika former av övningar och simuleringar. Hur ofta de bör testas beror bl.a. på hur ofta rutiner och handlingsplaner förändras och hur ofta de tillämpas. Så fort rutiner och handlingsplaner förändras bör nya tester genomföras. Inträffade avbrott och störningar utgör en tillämpning av rutiner och handlingsplaner och innebär ett test för att dessa fungerar.

Flera av stadsnäten i tillsynen nämnde detta praktiska sätt att verifiera rutiner och handlingsplaner. Ett stadsnät svarar t.ex. att de inte genomför några regelrätta tester av rutinerna utan istället utvärderar de rutiner de har efter varje incident. Därefter justeras handlingsplanen i förekommande fall.

PTS anser att alla tillhandahållare av nät och tjänster, även nyetablerade, bör testa rutiner regelbundet för att verifiera att de fungerar. Det praktiska förhållningssätt som beskrevs i exemplet ovan fungerar om incidenter sker med viss regelbundenhet och att en utvärdering av rutinerna sker i samband med dem. För incidenter som inträffar mindre frekvent eller incidenter som kan bli omfattande kan dock separata tester eller övningar vara nödvändiga.

#### **4.3.3 En fastställd prioriteringsordning bör framgå av rutiner och handlingsplaner**

PTS anger i de allmänna råden att rutiner och handlingsplaner bör innefatta en bedömning av i vilken prioriteringsordning åtgärder ska vidtas vid olika typer av avbrott och störningar.

7 av 10 stadsnät i tillsynen svarade att de har en prioriteringsordning. I några fall är dock prioriteringsordningen inte dokumenterad, utan mer uttalad. Det framgår att prioritering sker på olika sätt. I ett fall anges en prioriteringsordning som baseras på aktörskategori (landsting, kommun, operatör, företag, föreningar, enskilda kunder). I ett annat fall nämns en prioritering av olika tjänster.

PTS anser att alla tillhandahållare av nät och tjänster bör ha en fastställd prioriteringsordning som anger vilka åtgärder som ska vidtas vid avbrott och störningar. Prioriteringen bör bygga på en klassificering utifrån olika kriterier i verksamheten som säkerställer god funktion och teknisk säkerhet i kommunikationsnät och -tjänster. Prioriteringsordningen bör framgå av rutiner och handlingsplaner.

#### **4.3.4 Övervakning dygnet runt behövs för att snabbt upptäcka avbrott och störningar**

Samtliga stadsnät i tillsynen anger att de har en övervakning av avbrott och störningar dygnet runt, årets alla dagar. Detta innebär dock inte att övervakningen är bemannad dygnet runt.

6 av 10 stadsnät i tillsynen svarade att de har en bemannad övervakning dygnet runt, året runt. Några av dem har en driftcentral (benämns ibland Network Operation Center, NOC) i egen regi. Denna är ibland samarrangerad med annan övervakning i angränsande verksamhet, t.ex. övervakning av elnät.

Några har en lösning som innebär att övervakningen görs av annan part. Denna part är ofta en s.k. kommunikationsoperatör.

De som inte har en bemannad övervakning dygnet runt, året runt har i regel en bemannad övervakning under kontorstid. Övriga tider finns övervakning i form av automatlarm i kombination med jourverksamhet (beredskap).

Elektroniska kommunikationstjänster är tillgängliga och används dygnet runt. Beroendet till tjänsterna är stort. Avbrott och störningar kan också ske dygnet runt. Telefonitjänster används t.ex. för att ringa nödsamtal. Det är därför tidskritiskt att upptäcka eventuella avbrott och störningar och snabbt kunna påbörja felavhjälpning. Det finns också nödsamtalsföreskrifter<sup>8</sup> för tillhandahållare av telefonitjänster som innebär en skyldighet att vid avbrott och störningar omedelbart underrätta samhällets alarmeringstjänst (SOS Alarm).

PTS anser därför att en övervakning dygnet runt är väsentlig för att snabbt kunna upptäcka avbrott och störningar och påbörja felavhjälpning. Hur utformningen av övervakningen bör se ut beror av den enskilda verksamhetens förutsättningar.

För att stärka övervakningen kan olika åtgärder vidtas. Ett exempel som nämndes tidigare är att samarrangera övervakning med annan verksamhet, t.ex. övervakning av elnätet. En annan lösning kan vara att samverka med andra nätägare för att gemensamt övervaka näten. En tredje lösning kan vara att avtala med annan part om övervakning, t.ex. en operatör med regional eller nationell närvaro.

#### **4.3.5 Beredskap dygnet runt behövs för att snabbt kunna påbörja felavhjälpning**

Hur beredskapsverksamheten ser ut beror bland annat på hur övervakning sker, se tidigare avsnitt. Tillsynen visar på två olika huvudfall. Det första fallet är när det finns en bemannad driftcentral som övervakar dygnet runt, året runt. Det andra fallet är när det under vissa tider saknas en bemannad driftcentral som övervakar.

Om avbrott och störningar uppstår i det första fallet upptäcker den bemannade driftcentralen detta och försöker i första hand att åtgärda problemet, den utgör s.k. first line support. Vid behov sker en eskalering till specialister (s.k. second line support), fälttekniker eller leverantörer beroende på vad som behöver åtgärdas.

---

<sup>8</sup> PTS föreskrifter om förmedling av nödsamtal och tillhandahållande av lokaliseringssuppgifter till samhällets alarmeringstjänst, PTSFS 2008:2

Samma lösning gäller i regel även i det andra fallet så länge driftcentralen är bemannad. Om avbrott och störningar sker på tid då övervakningen inte är bemannad tar i regel jourpersonal (den s.k. beredskapen) emot automatiska larm. De automatiska larmen kommer vanligtvis som SMS och e-post. Beredskapen kan även ”larmas ut” via telefon av kundtjänst eller annan jourverksamhet. Till skillnad från det första fallet är det då upp till beredskapen att göra de första åtgärderna, dvs. att agera first line support.

Tillsynen visar att jourverksamheten (beredskapen) i regel består av teknisk personal (tekniska specialister och/eller fälttekniker). Jouren har i de flesta fall en inställelsetid på 1 timme. Inställelsetiden varierar mellan 30 minuter och 2 timmar. I princip samtliga som har en jourverksamhet anger att jourpersonalen har tillgång till övervakningssystem och andra tekniska system på distans, t.ex. från hemmet.

Hur beredskapen är organiserad skiljer sig dock. Några av stadsnäten i tillsynen har ett antal förutbestämda jourlag som alternerar. I ett exempel finns det sex olika jourlag som vart och ett består av två vakthavande montörer och en vakthavande driftledare. Planläggning sker på årsbasis där jourlagen går beredskap var sjätte vecka. Jourverksamheten är i detta fall densamma som den s.k. el-jouren och jourpersonalen är utbildade så att de kan åtgärda fel, t.ex. laga fiber om ett kabelbrott skulle uppstå.

I vissa fall bygger beredskapen till stor del på frivillighet bland tekniker i den ordinarie organisationen. De har inte samma formella organisation och rutiner som i exemplet ovan. Ett av stadsnäten i tillsynen uppgav t.ex. att jourverksamheten bygger mycket på frivillighet. På kvällar och nätter finns ingen bemannad övervakning. Om ett larm går under dessa timmar går det via SMS och e-post till de två tekniker som hanterar detta även under dagtid. Vid en större storm för en tid sen fick dessa tekniker över 90 olika larm. Ett annat stadsnät i tillsynen har en liknande lösning som till stor del bygger på frivillighet. På kvällar och helger finns en eljour samt en frivillig beredskap bestående av tre stadsnätstekniker som finns på en s.k. ringlista. I ett tredje fall finns en liknande situation. Där sköter en s.k. kommunikationsoperatör övervakningen. Om det blir avbrott eller störning i stadsnätet, t.ex. ett kabelbrott så ringer kommunikationsoperatören ett journummer som är sammanknutet med kommunens VA-jour. Dessa hanterar dock inte larmet utan vidarebefordrar det till stadsnätets ansvarige tekniker. Om larmet kommer nattetid så noteras det utan omedelbar åtgärd. Den ansvarige tekniker får detta på morgonen efter för åtgärd.

PTS ser risker i att beredskapen inte är ordentligt organiserad utan i vissa fall bygger på frivillighet. Den behöver utvecklas och formaliseras för att säkerställa snabb felavhjälpning. I stadsnäten finns elektroniska kommunikationstjänster som används dygnet runt. Beroendet och förväntan på tillgängligheten till tjänsterna är stort. Avbrott och störningar kan också ske dygnet runt. PTS anser därför att alla tillhandahållare av nät och tjänster behöver ha övervakning och beredskap dygnet runt för att snabbt kunna upptäcka avbrott och störningar och påbörja felavhjälpning.

Ett flertal åtgärder kan genomföras för att stärka jourverksamheten (beredskapen). Detta presenteras i avsnitt 3.4.

#### **4.3.6 Utbildning och övningar är viktiga för att öva färdigheter, sprida kompetens och förbättra samverkan**

7 av 10 stadsnät i tillsynen svarade att personalen är övad i hur den ska agera vid avbrott och störningar. Jämfört med större tillhandahållare av nät och tjänster är det inte lika vanligt att stadsnäten genomför övningar. Ett vanligt svar är att personalen övas kontinuerligt i och med att avbrott och störningar inträffar. Några anger dock att de genomför eller medverkar i övningar. Nationella övningar som Telö09, Samvete09 nämns, men även mer lokala övningar som kommunala krisövningar.

Den kontinuerliga hanteringen kan ses som ett sätt att öva. Flera av stadsnäten i tillsynen anger dock att de inte har haft så många avbrott och störningar. Vidare är det tveksamt om denna tillämpning är tillräcklig för större och mindre frekventa störningar. Eftersom organisationerna som driver stadsnät ofta är små och i vissa fall beroende av enskilda individer anser PTS att det är viktigt att kontinuerligt genomföra utbildningar och övningar. Detta för att öva färdigheter och testa rutiner, men även för att sprida kompetens till fler personer inom och utanför den egna organisationen. Samverkan med andra nätägare, leverantörer och samarbetspartners är också viktigt att öva.

#### **4.3.7 Enhetlig driftinformation behövs för kunder, samarbetspartners, allmänhet och samhällets alarmeringstjänst**

Resultatet av tillsynen visar olika kanaler används för att informera berörda aktörer om planerade och oplanerade avbrott och störningar. Vanligtvis ges driftinformation på stadsnätets webbplats. Driftinformation ges även via e-post, SMS och telefon. Tre av stadsnäten i tillsynen anger att de använder sig av GLU (gemensam lägesuppfattning)<sup>9</sup>.

---

<sup>9</sup> <http://www.pts.se/upload/Faktablad/SE/faktablad-glu-081024.pdf>

Om avbrott och störningar uppstår är det viktigt att information ges till kunder, samarbetspartners och allmänheten. Som exempel kan nämnas telefonitjänster. Vid avbrott och störning i telefonitjänsten har tjänstetillhandahållaren en skyldighet enligt PTS nödsamtalsföreskrifter att omedelbart underrätta samhällets alarmeringstjänst (SOS Alarm). Det är därför väsentligt att information om avbrott och störningar omedelbart kan sammanställas och delges till berörda parter.

PTS anser vidare att det är viktigt att den driftinformation som sammanställs presenteras på ett enhetligt sätt. GLU som några stadsnät använder är utvecklat för bl.a. detta ändamål. Syftet med GLU är bl.a. att minska effekterna av störningar och att öka samhällets förmåga att hantera konsekvenser av avbrott och störningar. Delar av GLU ska även kunna nyttjas av andra aktörer som SOS Alarm, länsstyrelser, kommuner, elsektorn, myndigheter, medier och allmänheten.

#### **4.3.8 Dokumenterade rutiner för uppföljning av avbrott och störningar saknas i stor utsträckning**

Tillsynen indikerar att dokumenterade rutiner för uppföljning av avbrott och störningar saknas i stor utsträckning. 7 av 10 stadsnät i tillsynen uppgav att de saknar detta och de flesta angav istället en mer informell hantering där driftstörningar tas upp i regelbundna möten. Ett stadsnät i tillsynen svarar t.ex. att uppföljning av inträffade avbrott och störningar görs på veckovisa möten som dokumenteras.

Tillsynen visar också på goda exempel av uppföljning. I ett sådant exempel bokförs alla störningar och avbrott i ett ärendehanteringssystem där varje ärende får ett unikt nummer. Varje åtgärd åtföljs av kontroll samt återkoppling av den som ansvarat för åtgärden. I systemet bokförs även orsaken till störningen och vad som kan göras för att motverka nya fel. Alla ärenden går igenom en gång per månad för analys och eventuell åtgärd.

I PTS allmänna råd anges att tillhandahållare av nät och tjänster regelbundet bör följa upp inträffade avbrott och störningar i verksamheten samt beakta deras orsaker vid planering och utbyggnad av infrastruktur. Vidare anges att rutiner för uppföljning bör upprättas och hållas uppdaterade.

För att säkerhetsarbetet ska bli systematiskt, enhetligt och kontinuerligt anser PTS att alla tillhandahållare av nät och tjänster bör upprätta rutiner för uppföljning. Rutinerna bör innefatta tillvägagångssätt för identifiering av orsak, planering och införande av åtgärder för att förhindra att avbrott eller störningar upprepas, samt former för vidare rapportering inom verksamheten.

#### **4.4 Åtgärder för att förebygga vanliga orsaker till avbrott och störningar**

I detta avsnitt redovisas resultaten från enkäten och intervjuer avseende åtgärder för att förebygga vanliga orsaker till avbrott och störningar. I enkäten motsvarar det frågorna 21-34. Bestämmelser och PTS allmänna råd som relaterar till dessa frågor framgår av kapitel 2.

##### **4.4.1 Reservkraft finns för viktiga funktioner, tester bör genomföras regelbundet**

Samtliga stadsnät i tillsynen anger att de har reservkraft till viktiga funktioner i deras verksamhet. Med viktiga funktioner avses bl.a. kunddatabaser, namnserverrar, centrala noder, knutpunkter för trafikutbyte och driftledningscentraler (se vidare avsnitt 2.2.3).

Vad som är viktiga funktioner beror på vilka tjänster som tillhandahålls. Flera stadsnät tillhandahåller bara svartfiber och nätkapacitetstjänster vilket begränsar antalet viktiga funktioner. Reservkraft finns normalt för centrala noder, utrustning och system. Reservkraften består i de flesta fall av batteribackup (Uninterruptible Power Supply, UPS) i första hand och dieselverk i andra hand. Samtliga stadsnät i tillsynen har automatisk inkoppling av reservkraften om den ordinarie elförsörjningen faller ifrån.

PTS anser att reservkraft för viktiga funktioner är nödvändiga för att upprätthålla god funktion och teknisk säkerhet i de nät och tjänster som tillhandahålls. Tillsynen visar också att reservkraft finns för viktiga funktioner, vilket är positivt. Exempel på hur reservkraft kan anordnas ges bland annat i SSNf:s rekommendationer för uppbyggnad av robusta noder<sup>10</sup>.

För att säkerställa att reservkraften fungerar tillfredsställande bör tester genomföras regelbundet. Test av reservkraft kan ske i olika stor omfattning. I ett mer fullständigt test så kopplas ordinarie elförsörjning bort för att säkerställa att reservkraften tar över och har tillräcklig effekt. Ett mindre omfattande test är att göra funktionstester av reservkraften, t.ex. att dieselverket startar. PTS anser att båda dessa typer av tester bör genomföras regelbundet.

Tillsynen visar att tester genomförs regelbundet. Flera stadsnät anger att de gör mer fullständiga tester enligt beskrivningen ovan. Detta är positivt. I tillsynen gavs ett bra exempel på hur test av reservkraften kan göras. Dieselaggregaten provköras varje månad. Provkörning sker skarpt genom att bryta inkommande ström. Då verifieras att dieselgeneratoren startar automatiskt och tar över den last som finns. Under uppstart används även batterierna i UPS.

---

<sup>10</sup> [http://www.ssnf.org/upload/Projektokument/robusta\\_noder.pdf](http://www.ssnf.org/upload/Projektokument/robusta_noder.pdf)

Dieselaggregaten körs i 30 minuter med den last som finns. Återgång sker genom att slå till inkommande brytare varvid dieselaggregatet efter en kort stund fasar över lasten till elnätet och stannar. På så sätt testas hela kedjan inklusive automatiken så verklighetsnära som möjligt. Test av UPS sker i samband med service 1-2 gånger per år och den jobbar då mot den aktuella lasten.

#### **4.4.2 Redundans behöver säkerställas i viktiga funktioner**

För att nät och tjänster ska ha en god funktion och teknisk säkerhet krävs redundans, inte bara i form av reservkraft och alternativa förbindelsevägar. Det är även viktigt att redundans i viktiga funktioner säkerställs.

Med redundans avses i detta sammanhang att om en viktig funktion slutar fungera så finns en parallell lösning som upprätthåller tjänstens funktion och kapacitet. T.ex. om en server för en telefonitjänst slutar fungera så finns det en annan parallell server som kan upprätthålla tjänstens funktion och kapacitet. En beskrivning av redundans i detta avseende finns i SSNF rekommendationer för uppbyggnad av robusta noder.

Det finns en viss spridning i svaren i tillsynen avseende redundans i viktiga funktioner. De flesta svaren indikerar att sådan redundans finns. I något fall tror PTS dock att frågan tolkats som redundans i elförsörjning till den viktiga funktionen. Som beskrevs i inledningen av detta avsnitt är det viktigt att se skillnaden mellan dessa olika typer av redundans. Vad som är viktiga funktioner är beroende av vilka tjänster som tillhandahålls.

Ett stadsnät i tillsynen ger ett bra exempel på redundans i viktiga funktioner. De anger att det för Internettjänsten finns två fysiskt skilda vägar till olika knutpunkter i Sverige. För TV-tjänsten har de redundanta TV-sändare. Vidare har de redundans i namnservrar, switchar och routrar, t.ex. full redundans i BGP-routrar.

PTS anser att det är viktigt att redundans finns för viktiga funktioner. Denna redundans är avgörande för att säkerställa tjänsters funktionalitet och säkerhet. Om viktiga funktioner som t.ex. adresseringsfunktioner eller kunddatabaser slås ut så kan tjänster sluta fungera för ett stort antal användare.

#### **4.4.3 Viktigt att säkerställa att förbindelser i centrala nät är redundanta**

Utöver elförsörjning och i den viktiga funktionen är det viktigt att säkerställa redundans i förbindelsevägar. Med redundans avses i detta sammanhang att det finns alternativa förbindelsevägar till samma viktiga funktion. Om det blir

avbrott eller störning i en förbindelseväg, t.ex. på grund av kabelbrott, så upprätthåller den alternativa förbindelsevägen tjänstens funktion och kapacitet.

Tillsynen visar likartade svar på hur redundansen ser ut i detta avseende. Förbindelser i centrala nät (s.k. backbone, core- eller stamnät) i regel är redundanta uppbyggda. Att säkerställa redundans är förenat med stora kostnader, i synnerhet för accessnät. Detta är anledningen till att accessnät normalt inte är redundanta, om inte kunder avtalar och betalar för det. Avbrott och störningar i viktiga funktioner och centrala nät drabbar ofta stora delar av tjänsten och många användare, medan avbrott och störningar i accessnät normalt drabbar ett begränsat antal användare.

Det är också viktigt att se till hur redundansen är uppbyggd. Av tillsynsvaren framgår att det är vanligt att ha fysisk separation i ringstruktur. Ett stadsnät i tillsynen nämner dock att merparten av redundansen är flera fiberpar i samma kabel. PTS menar att någon redundans i egentlig mening i detta fall inte har uppnåtts. Detta eftersom ett kabelbrott, t.ex. i form av en avgrävning, sannolikt leder till avbrott i alla fiberpar.

På samma sätt som redundans i elförsörjning och i viktiga funktioner är redundans i förbindelsevägar till centrala noder och funktioner avgörande för att säkerställa funktioners funktionalitet och säkerhet. Om denna redundans saknas kan tjänster sluta fungera för ett stort antal användare. PTS anser därför att det är viktigt att säkerställa att redundans finns i centrala nät.

#### **4.4.4 Arbetet med riskanalyser och tester före installationer och uppgraderingar bör förbättras**

Avbrott och störningar i samband med uppgraderingar är vanligt förekommande. PTS har de senaste åren uppmärksammat ett flertal exempel på hur uppgraderingar i hård- och mjukvara har lett till problem med tjänsters funktionalitet och tekniska säkerhet. Detta är tillsammans med avgrävningar de vanligaste orsakerna till att avbrott och störningar uppstår i elektroniska kommunikationstjänster. För att förebygga detta är riskanalyser och tester viktiga aktiviteter för att identifiera risker och verifiera tjänsters funktionalitet och säkerhet innan uppgradering genomförs.

Tillsynen indikerar att det finns en förbättringspotential i detta avseende. 7 av 10 stadsnät i tillsynen svarade att de saknar dokumenterade rutiner för installation av hård- och mjukvara. Det är heller inte så vanligt att riskanalyser genomförs. Endast ett fåtal uppgav att de genomför riskanalyser i samband med installationer och uppgraderingar. Däremot svarade i princip alla att de genomför olika typer av tester, t.ex. i särskilda labb och testmiljöer.

PTS anser att såväl riskanalyser som tester bör genomföras innan uppgraderingar sker. De tillhandahållare av nät och tjänster som inte uppgraderar eller testar i egen regi kan ställa krav i avtal med underleverantörer att så sker. Vidare anser PTS att genomförandet av uppgraderingar och ändringar bör göras enligt dokumenterade rutiner. T.ex. bör tester följa specificerade testförfaranden. I tillsynen som genomfördes 2007-2008 framgick att det är vanligt med processer och rutinbeskrivningar för förändringshantering, vilka ofta benämns med den engelska termen change management. Dessa rutiner innehåller vanligtvis en riskanalys, en planering och koordinering av uppgraderingar, samt att de beskriver hur beslutsfattande och acceptans av uppgraderingar och ändringar sker.

PTS anser vidare att alla tillhandahållare av nät och tjänster bör ha en plan för återställning om något skulle gå fel vid installation, ändringar eller uppgradering. Resultatet av tillsynen visar på olika metoder för att kunna återställa, t.ex. genom att ta säkerhetskopior (backuper) och arbeta i metodsteg.

#### **4.4.5 Användare och samarbetspartners bör informeras om installationer och uppgraderingar som kan påverka driftsäkerheten**

Det är viktigt att planering och koordinering av uppgraderingar görs för att minimera störningar för användare. Genomförandet av uppgraderingar och ändringar bör göras i särskilda servicefönster. Det är vanligt att uppgradering sker kvällar eller nätter och anpassas så att det finns tid till återställning om så skulle behövas. Tidpunkt för servicefönster är dock beroende av när tjänsterna i huvudsak används och när personal, som kan ta om hand eventuella problem, finns på plats. Ett annat sätt att minimera risker vid uppgraderingar är att om möjligt arbeta med stegvisa uppgraderingar. Ett exempel är att genomföra uppgradering i avgränsade geografiska områden och utvärdera denna innan en mer fullskalig uppgradering genomförs. Vid en avgränsad eller stegvis uppgradering är fördelen att antalet användare som drabbas av eventuella störningar begränsas och återställningsarbetet blir mindre omfattande.

PTS anser att alla tillhandahållare av nät och tjänster bör informera sina kunder och samarbetspartners om planerade installationer och uppgraderingar som kan påverka driftsäkerheten i större utsträckning. Beroendet av elektroniska kommunikationstjänster är stort och det är viktigt att informera användare om förändringar som kan påverka möjligheterna att nyttja dem. Detta kan göras via de kanaler som finns för driftinformation, se avsnitt 4.3.7.

#### **4.4.6 Erfarenheter och rutiner saknas för att hantera IT-incidenter som skadlig kod och överbelastningsattacker**

Avbrott och störningar i elektroniska kommunikationstjänster kan också orsakas av s.k. logiska störningar. Med logiska störningar avses t.ex. skadlig kod och överbelastningsattacker. Ibland används begreppet IT-incidenter.

Resultatet av tillsynen visar att flera stadsnät inte har några rutiner för att hantera logiska störningar av detta slag. Flera anger också att de inte har så stor erfarenhet av denna typ av störningar. De ser det mer som ett tjänsteleverantörsproblem. Några anger dock att de vidtar olika åtgärder för att upptäcka, förhindra och avhjälpa sådana störningar. T.ex. används olika inbyggda funktioner och instrument som övervakar om onormalt hög trafikbelastning inträffar. För att hantera eventuella logiska störningar anlitas i regel leverantörer, kommunikationsoperatörer eller andra teknikföretag om de inte besitter kompetensen själva. De flesta anger dock att de inte har något behov av att hantera logiska störningar.

Behovet av att kunna hantera logiska störningar beror på vilka tjänster som tillhandahålls. Tillhandahållare av nät och tjänster med egna tjänsteplattformar har ett större behov av att kunna hantera denna typ av störningar jämfört med dem som tillhandahåller svartfiber och nätkapacitetstjänster. Då logiska störningar kan påverka nät och tjänsters funktion och säkerhet anser PTS att det är viktigt att ha en beredskap för att kunna hantera dem. Ansvarsfördelningen mellan inblandade parter bör vara tydligt. Detta beskrivs ytterligare i avsnitt 3.5.

#### **4.4.7 Avtal och samarbete är vanligt för att säkerställa god funktion och teknisk säkerhet i fastighets- och områdesnät**

För att nå ut till användare av elektroniska kommunikationstjänster ansluts ofta stadsnätet till fastighets- och/eller områdesnät. För att tjänster ska ha en god funktion och teknisk säkerhet så är det viktigt att säkerställa att fastighets- och områdesnäten också har det.

En viktig fråga är således hur arbete kan bedrivas för att säkerställa god funktion och teknisk säkerhet i fastighets- och områdesnät, t.ex. gällande säkerhet i utrustning i enlighet med rekommendationerna i SKA, säker kundanslutning.

Av tillsynen framgår olika sätta att arbeta på i detta avseende. I vissa fall används avtal. Ett stadsnät svarade t.ex. att de avtalar med varje fastighetsägare och ägare av områdesnät där dessa förbinder sig att ha ett avtal om service. Om så behövs kan de hjälpa dem att hitta en lämplig servicepart. I avtalsvillkoren framgår skyldigheter för fastighetsägaren att på egen bekostnad

ständigt hålla fastighetsnätet i ett sådant skick att användarna felfritt och utan dröjsmål har tillgång till tjänsterna, att omedelbart åtgärda fel eller skada på fastighetsnätet och att anmäla sådana fel till en utpekad part. Vidare avtalas om tillgänglighet till lokaler där utrustning förvaras, t.ex. om nycklar till olika lokaler. I ett annat fall så avtals om samarbete. När avtal ska ingås så kontrollerar stadsnätet befintlig utrustning och vid behov görs utbyte till SKA certifierad utrustning. De ansvarar även för driftövervakning och underhåll.

Några stadsnät i tillsynen svarade att de inte ingår avtal fastighetsägare och ägare av områdesnät. En del ställer heller inga krav på fastighetsnätet då de inte upplevt några problem relaterade till fastighetsnät. Vanligtvis görs dock kontroller av fastighetsnätets prestanda före anslutning. Några nämner t.ex. att de kontrollerar teknisk dokumentation och mäter upp förbindelser. Skulle problem uppstå så är i regel stadsnäten behjälpliga, antingen genom att de löser problemet eller genom att föreslå olika åtgärder som fastighetsägaren kan vidta för att höja funktionaliteten och säkerheten.

Oavsett om avtal ingås eller inte så framgår av tillsynen att en faktor för att uppnå god funktion och teknisk säkerhet är att skapa incitament och stödja ägare av fastighets- och områdesnät.

PTS anser att det är viktigt att god funktion och teknisk säkerhet säkerställs i fastighets- och områdesnät. De avtal och samarbeten som nämnts här är exempel på hur stadsnäten kan arbeta för att säkerställa detta. Krav på respektive part och ansvarsfördelning är viktigt att tydliggöra. Detta beskrivs ytterligare i avsnitt 3.5

## **5 PTS fortsatta arbete relaterad till god funktion och teknisk säkerhet**

### **5.1 Fortsatt tillsyn, information och kunskapshöjande arbete**

Som beskrevs i avsnitt 1.2 har syftet med den planlagda tillsynen varit att få en generell uppfattning om hur bestämmelser om god funktion och teknisk säkerhet efterlevs och att sprida kunskap om hur säkerhetsarbetet kan bedrivas för att uppfylla bestämmelserna.

Den nu genomförda tillsynen visar på ett antal generella förbättringsområden som tillhandahållare av nät och tjänster behöver adressera. Det är viktigt marknadens aktörer fortsätter att öka det förebyggande arbetet, höja beredskapen och förmågan att hantera avbrott och störningar.

PTS kommer därför att fortsätta tillsynsarbetet och genomföra uppföljande tillsyn för att se att utvecklingen av säkerhetsarbetet går i önskvärd riktning. Arbetet kommer att bestå av planlagda tillsynsinsatser liknande denna, men även av händelsestyrda tillsynsinsatser vid inträffade incidenter, avbrott och störningar. PTS kommer även att fortsätta att arbeta med informations- och kunskapshöjande insatser.

Den förväntade effekten är att det säkerhetsarbetet som tillhandahållare av nät och tjänster bedriver fortsätter att utvecklas, och är kontinuerligt, systematiskt samt framåtsyftande och långsiktigt.

### **5.2 PTS verkar för robusta kommunikationer**

Bestämmelserna om god funktion och teknisk säkerhet ger uttryck för en grundläggande nivå av driftsäkerhet (se avsnitt 2.1). Nivån av grundläggande driftsäkerhet bestäms utifrån kommersiella överväganden och bestämmelserna i LEK. För att säkerställa samhällets samlade behov av säkerhet och beredskap kan denna grundläggande nivå behöva kompletteras dels genom privatoffentlig samverkan med delad finansiering dels med statliga beslut med statligt finansierade åtgärder.

PTS har som sektorsmyndighet ett ansvar för att samhällets behov av elektroniska kommunikationer tillgodoses och ett uppdrag att vidta åtgärder för att förebygga och motverka sårbarhet inom sitt sektorsområde. För arbetet har PTS en strategi för robusta elektroniska kommunikationer<sup>11</sup> Strategin

---

<sup>11</sup> Robust elektronisk kommunikation - Strategi för åren 2009-2011 - PTS-ER-2009:25

redovisar ett antal olika åtgärdsområden som PTS anser angelägna och grunder för prioritering av insatser. Åtgärdsområdena är:

1. Stimulans till ett ökat användaransvar inom elektronisk kommunikation
2. Ökad redundans och flexibilitet i nätverk
3. Förbättrat skydd mot både fysiska, elektromagnetiska och logiska hot
4. Öka kunskapen om informationssäkerhet
5. Robust elförsörjning för elektronisk kommunikation och fördjupad samverkan mellan el- och telekomområdena
6. Utveckla samverkan
7. Fördjupa internationell samverkan
8. Förbättrad förmåga till krishantering inom elektronisk kommunikation
9. Öka effekten av robusthetsåtgärder i näten

Som exempel på samverkan kan nämnas nationella telesamverkansgruppen (NTSG) som bildades 2005. Den är ett frivilligt samarbetsforum med syfte att stödja återställandet av den nationella infrastrukturen för elektroniska kommunikationer vid extraordinära händelser i samhället. Ett annat exempel är ett samverkansprojekt som PTS driver tillsammans med ledningsägare inom sektorn för att utveckla ett system för gemensam lägesuppfattning (GLU) i händelse av störningar i näten. Syftet med GLU är bl.a. att minska effekterna av störningar och att öka samhällets förmåga att hantera konsekvenser av avbrott och störningar. Delar av GLU kan även nyttjas av andra aktörer som SOS Alarm, länsstyrelser, kommuner, elsektorn, myndigheter, medier och allmänheten.

### **5.3 Sitic informerar och ger råd om IT-incidenter**

IT-incidenter är nära relaterat till god funktion och teknisk säkerhet då dessa kan leda till avbrott och störningar i elektroniska kommunikationstjänster. På PTS finns Sveriges IT-incidentcentrum (Sitic) som ansvarar för att Sverige har en nationell funktion med uppgift att stödja samhället i arbetet med att hantera och förebygga IT-incidenter. PTS ska, genom att driva Sitic, i detta arbete:

- agera skyndsamt vid inträffade IT-incidenter genom att sprida information samt vid behov medverka i samordning av åtgärder som krävs för att avhjälpa eller lindra effekter av det inträffade.
- samverka med myndigheter med särskilda uppgifter inom informationssäkerhetsområdet,
- lämna råd och stöd avseende förebyggande arbete till andra statliga myndigheter, kommuner och landsting samt företag och organisationer om nätets säkerhet,

- vara Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder samt utveckla samarbetet och informationsutbytet med dessa.

På Sitics webbplats<sup>12</sup> finns ytterligare information om uppdraget och verksamheten som bedrivs.

---

<sup>12</sup> <http://www.sitic.se/>



## Bilaga 1

### Stadsnät som omfattades av tillsynen

1. Bjäre Kraft Bredband AB
2. Gavlenet (Gävle Energi AB)
3. IT Norrbotten AB
4. Jämtkraft stadsnät (Jämtkraft Telecom AB)
5. Karlstad stadsnät (Karlstad Elnät AB)
6. LaNet, Landskrona stad
7. Storumans kommun
8. UmeNet (Umeå Energi UmeNet AB)
9. Värnamo Energi AB
10. VÖKBY Bredband AB



## Bilaga 2

### Utskickad tillsynsenkät

Följande tillsynsenkät skickades den 9 september 2009 ut till de stadsnätsoperatörer som omfattades av tillsynen.

#### **Tillsyn av bestämmelser om god funktion och teknisk säkerhet i lagen om elektronisk kommunikation**

Enkäten består av ett antal frågor som är indelade efter olika områden kring god funktion och teknisk säkerhet.

Anvisning för att fylla i enkäten:

- Spara ner enkäten på din dator (namnge gärna med företagets namn)
- Fyll i de gråmarkerade fälten (klicka dig fram med musen eller använd tabtangenter)
- Om ni anser att viss information är känslig bör ni markera i ert svar vilka uppgifter det är
- Spara den ifyllda enkäten
- Skriv ut och skicka den ifyllda enkäten till PTS, att. Staffan Lindmark, Box 5398, 102 49 Stockholm alternativt e-posta den som bifogad fil till: [staffan.lindmark@pts.se](mailto:staffan.lindmark@pts.se)

För att se definitioner av vissa begrepp som används i enkäten, se bilaga 1 (PTS allmänna råd) och bilaga 2 (information om PTS allmänna råd). Om begreppen inte förklaras i bilagorna har förklaringar lagts in i enkäten med kursiv stil.

Besvarad enkät ska vara PTS tillhanda senast den **7 oktober 2009**.

### Inledande frågor

Företagets namn:

Webbplats:

Kontaktperson för PTS vid frågor om enkäten (namn, telefon, e-post):

Tillhandahåller ni:

Fast telefoni

Mobil telefoni

IP-telefoni

Internetaccess

Nätkapacitet

E-post

Fast telefoni via mobilt accessnät

IP-tv eller digital-tv

Svart fiber

Annan kommunikationstjänst:

### Övergripande frågor om säkerhetsarbete

1. Beskriv övergripande det säkerhetsarbete ni bedriver.  
(För vad som avses med säkerhetsarbete, se PTS allmänna råd)
2. Beskriv hur ni beslutar om rutiner och handlingsplaner för säkerhetsarbetet.

### Riskanalys

3. Använder ni er av riskanalyser i ert säkerhetsarbete?  
Ja  Nej  (gå till fråga 6)
4. Använder ni er av dokumenterade rutiner för genomförande av riskanalys? Om ja, bifoga gärna dokumentationen till ert svar.  
Ja  Nej
5. Beskriv hur ni arbetar med riskanalyser.

- a. När genomförs riskanalyser? Vad föranleder genomförande av riskanalysarbete?
- b. Vilka delar av verksamheten omfattas av riskanalyser?
- c. Beskriv hur riskanalysen genomförs, t.ex. om en särskild metod används.
- d. Vilka åtgärder vidtas för att säkerställa att riskanalysen är aktuell?

#### **Riskhantering**

6. Har ni dokumenterade rutiner för riskhantering (t.ex. när säkerhetsåtgärder ska vidtas och vem som beslutar om dessa)? Om ja, bifoga gärna dokumentationen till ert svar.  
Ja  Nej
7. Beskriv hur identifierade risker generellt hanteras i verksamheten.
8. Beskriv hur beslutade säkerhetsåtgärder följs upp.

#### **Hantering av avbrott och störningar**

9. Har ni dokumenterade rutiner och handlingsplaner för att hantera avbrott och störningar? Om ja, bifoga gärna dokumentationen till ert svar.  
Ja  Nej
10. Hur ofta testas dessa rutiner och handlingsplaner?
11. Finns prioriteringsordning i era rutiner som anger vilka verksamheter som först ska avhjälpas vid avbrott och störningar?

Ja

Nej

12. Beskriv hur ni har organiserat er hantering av avbrott och störningar.

13. Har ni övervakning av avbrott och störningar dygnet runt under årets alla dagar?

Ja

Nej

Om nej, under vilka tider finns sådan övervakning?

14. Beskriv hur övervakning av avbrott och störningar sker (bemannad, obemannad, jour, etc.).

Om jourtjänstgöring tillämpas under vissa tider:

a. Hur är jousen bemannad?

b. Vilken inställetid har jousen?

c. Hur uppmärksammas jousen på avbrott och störningar (t.ex. automatiska larm, manuella kontroller etc.)?

d. Har jourpersonalen tillgång till övervakningssystem etc. på distans (t.ex. från hemmet)?

15. I vilka fall och hur informeras kunder om avbrott och störningar (pågående och planerade)?

16. Är personalen övad hur den ska agera vid avbrott och störningar?

Ja

Nej  (gå till fråga 18)

17. Hur ofta genomför ni övningar och vad ingår i dessa?

18. Beskriv i övrigt er hantering av avbrott och störningar.

### Uppföljning av inträffade avbrott och störningar

19. Har ni dokumenterade rutiner för uppföljning av avbrott och störningar? Om ja, bifoga gärna dokumentationen till ert svar.

Ja

Nej

20. Beskriv hur ni arbetar med uppföljning av avbrott och störningar (t.ex. för att förhindra att avbrott och störningar återkommer eller uppkommer vid nätutbyggnad och uppgraderingar)

### Viktiga funktioner

*PTS har kunnat konstatera att vanliga orsaker till avbrott i elektroniska kommunikationsnät och -tjänster är att tillhandahållare drabbats av avbrott i elförsörjningen eller råkat ut för någon form av avbrott i access- eller transportnätet.*

*Avbrott vid tillhandahållandet av elektroniska kommunikationstjänster kan också inträffa som en följd av att vissa viktigare funktioner, t.ex. basstationer, lokalstationer, register för att lokalisera användare, namnservrar och kunddatabaser drabbas av avbrott eller störningar. Dessutom inträffar avbrott och störningar som en följd av installationer och uppgraderingar av hård- eller mjukvara.*

*Nedan följer ett antal frågor som är inriktade mot denna typ av avbrottsorsaker.*

### Elförsörjning till viktiga funktioner

21. Finns reservkraft för viktiga funktioner i er verksamhet?

Ja

Nej  (gå till fråga 24)

22. Hur ofta genomförs tester av reservkraften och hur går dessa till?

23. Beskriv i vilken utsträckning ni har reservkraft för viktiga funktioner.

a. Vilka system och funktioner har reservkraft?

b. Hur är reservkraften uppbyggd?

c. Vilken automatik finns för inkoppling av denna?

**Redundans avseende viktiga funktioner**

24. Beskriv i vilken utsträckning ni har redundans för viktiga funktioner.

- a. För vilka funktioner finns redundans?
- b. Hur är redundansen uppbyggd?

**Redundans i förbindelsevägar**

25. Beskriv i vilken utsträckning det finns redundanta förbindelsevägar i ert elektroniska kommunikationsnät..

- a. Till vilka funktioner finns redundanta förbindelsevägar?
- b. Hur långt ut i näten finns redundans?
- c. Hur är redundansen uppbyggd?

**Installation och uppgradering av hård- eller mjukvara i viktiga funktioner**

26. Beskriv hur ni arbetar med riskhantering i samband med installation och uppgradering av hård- och mjukvara som används för viktiga funktioner.

27. Har ni dokumenterade rutiner för installation och uppgradering av hård- och mjukvara? Om ja, bifoga gärna dokumentationen till ert svar.

Ja

Nej

28. I vilka fall och hur genomförs tester före installation och uppgradering?

29. Hur planerar ni för att kunna utföra återställning om något skulle gå fel vid installation eller uppgradering?

**God funktion och teknisk säkerhet hos fastighets- och områdesnät m.m.**

30. Hur säkerställer ni god funktion och teknisk säkerhet hos samarbetspartners, exempelvis i fastighets- och områdesnät (t.ex. gällande säkerhet i utrustning i enlighet med rekommendationerna i SKA, säker kundanslutning)<sup>13</sup>?
31. Hur säkerställs hantering av avbrott och störningar hos sådana samarbetspartners (t.ex. i avtal eller drift i samverkan)?

**Hantering av logiska störningar**

32. Vilka rutiner finns för att hantera logiska störningar, såsom skadlig kod och överbelastningsattacker?
33. Vilka åtgärder vidtas för att upptäcka, förhindra och avhjälpa sådana störningar?
34. Tar ni rutinmässigt stöd av någon extern part när sådana störningar inträffar (t.ex. av Sveriges IT-incidentcentrum, Sitic)?

**Övrigt**

35. Beskriv vilka andra aktiviteter, dokument och rutiner som finns för att efterleva bestämmelsen om god funktion och teknisk säkerhet m.m.
36. Plats för synpunkter och förslag

---

<sup>13</sup> <http://www.ssnf.org/upload/Projektdokument/SKA.pdf>



## Bilaga 3

### PTS allmänna råd om god funktion och teknisk säkerhet m.m. (PTSFS 2007:2)

## Post- och telestyrelsens författningssamling

Utgivare: Eva Liljefors, Post- och telestyrelsen, Box 5398, 102 49 Stockholm  
ISSN 1400-187X

---

#### **Post- och telestyrelsens allmänna råd om god funktion och teknisk säkerhet samt uthållighet och tillgänglighet vid extraordinära händelser i fredstid;**

**PTSFS 2007:2**

Utkom från trycket  
den 3 maj 2007

beslutade den 25 april 2007.

Enligt 5 kap. 6a § lagen (2003:389) om elektronisk kommunikation skall den som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster, se till att verksamheten uppfyller rimliga krav på god funktion och teknisk säkerhet samt på uthållighet och tillgänglighet vid extraordinära händelser i fredstid.

PTS utfärdar följande allmänna råd om vad som bör beaktas vid bedömning enligt denna bestämmelse.

#### **Definitioner**

I dessa allmänna råd avses med:

*Tillhandahållare*: aktörer som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster.

*Kommunikationsnät*: allmänna kommunikationsnät i enlighet med 1 kap. 7 § lagen (2003:389) om elektronisk kommunikation.

*Kommunikationstjänst*: allmänt tillgänglig elektronisk kommunikationstjänst i enlighet med 1 kap. 7 § lagen (2003:389) om elektronisk kommunikation.

*Hot*: möjlig oönskad händelse med negativa konsekvenser för verksamheten.

*Risk*: en sammanvägd bedömning av sannolikheten för och konsekvenserna av att ett identifierat hot inträffar.

*Störning*: att kommunikationsnätet eller kommunikationstjänsten är tillgängliga, men med bristande funktion.

*Avbrott*: att kommunikationsnätet eller kommunikationstjänsten inte är tillgängliga.

## **Säkerhetsarbete**

Tillhandahållare bör bedriva ett kontinuerligt och systematiskt säkerhetsarbete. Ett sådant arbete bör bestå i de delmoment som närmare redogörs för nedan.

Säkerhetsarbetet bör i huvudsak vara framåtsyftande och långsiktigt samt bör omfatta såväl normala driftsförhållanden som extraordinära händelser.

Upprättade rutiner och handlingsplaner, resultat och bedömningar inom ramen för riskanalysen och riskhanteringen, samt uppföljningen av inträffade avbrott och störningar, bör dokumenteras och hållas uppdaterade. Med uppdaterad avses att dokumenten uppdateras i takt med förändringar som i betydande omfattning påverkar förutsättningarna för verksamheten.

De upprättade dokumenten bör vara beslutade på ledningsnivå i organisationen och följas i verksamheten.

### *Riskanalys*

Tillhandahållaren bör regelbundet samt vid förändringar som i betydande omfattning påverkar förutsättningarna för verksamheten, genomföra riskanalyser avseende kommunikationsnätets och kommunikationstjänstens funktionsförmåga.

Tillhandahållaren bör upprätta rutiner för genomförandet av riskanalyserna.

En riskanalys bör omfatta följande moment:

- Identifiering av det område som skall omfattas av analysen,
- identifiering av hot inom det aktuella området,
- bedömning av de identifierade hotens konsekvenser för verksamheten,
- bedömning av sannolikheten för att identifierade hot inträffar, samt
- identifiering av risker, dvs. den sammanvägda bedömningen av sannolikheten för att identifierade hot inträffar och de konsekvenser det kan medföra för verksamheten om de inträffar.

### *Riskhantering*

Tillhandahållaren bör bedöma på vilket sätt identifierade risker skall hanteras i verksamheten. Identifierade risker bör hanteras på det sätt och i den utsträckning och omfattning som är skäligt med hänsyn till typen av risk samt den enskilda verksamhetens inriktning och förutsättningar, omfattning och betydelse.

Tillhandahållaren kan exempelvis välja att avseende en viss risk vidta skyddsåtgärder i syfte att förebygga att ett avbrott eller en störning uppstår. Tillhandahållaren kan välja att avseende en annan risk i stället planera för vilka åtgärder som skall vidtas för att så långt som möjligt begränsa konsekvenserna när ett avbrott eller en störning väl inträffar.

Vid skälighetsbedömningen kan hänsyn tas till faktorer såsom exempelvis företagets storlek, geografiska verksamhetsområde och konkurrenskraft samt till om det är nyetablerat. Vidare kan i bedömningen exempelvis hänsyn tas till om risken är hänförlig till normal drift eller

extraordinära händelser, samt vilken funktion i kommunikationsnätet eller kommunikationstjänsten som risken avser.

Rutiner för riskhantering bör upprättas.

#### *Planering för avbrott och störningar*

Tillhandahållaren bör upprätta rutiner och handlingsplaner med åtgärder som skall vidtas vid avbrott och störningar i elförsörjning av, förbindelsevägar till samt funktionsförmågan hos viktiga funktioner, samt vid sådana avbrott och störningar i övrigt som verksamheten vid riskhanteringen beslutat att planera för.

Rutiner och handlingsplaner avseende avbrott och störningar i elförsörjning av och förbindelsevägar till samt funktionsförmågan hos viktiga funktioner, bör utformas på sådant sätt att avbrottens och störningarnas konsekvenser så långt som möjligt begränsas och inte leder till betydande avbrott och störningar i de elektroniska kommunikationerna. Utformningen bör ske utifrån vad som är skäligt med hänsyn till typen av avbrott och störning samt den enskilda verksamhetens inriktning, förutsättningar, omfattning och betydelse.

Vid skälighetsbedömningen kan hänsyn tas till faktorer som exempelvis företagets storlek, geografiska verksamhetsområde och konkurrenskraft samt till om det är nyetablerat. Vidare kan hänsyn exempelvis tas till om avbrottet eller störningen inträffar i normal drift eller vid extraordinära händelser, samt till vilken funktion i kommunikationsnätet eller kommunikationstjänsten som avbrottet eller störningen avser.

Exempel på vad som kan utgöra viktiga funktioner är lokalstationer, basstationer, knutpunkter för trafikutbyte och register för att lokalisera användare.

I bedömningen av vad som är betydande avbrott och störning kan hänsyn exempelvis tas till antal drabbade abonnenter, geografisk omfattning och avbrottet eller störningens längd.

Rutinerna och handlingsplanerna bör innefatta bl.a. följande:

- Definierade tillvägagångssätt och åtgärder för ett snabbt och effektivt avhjälpande av avbrott och störningar och återställande av verksamheten till normal drift,

- bedömning av i vilken prioritetsordning åtgärder skall vidtas vid olika typer av avbrott och störningar,

- rutiner för att säkerställa att extra resurser kan avsättas när det är nödvändigt, samt

- tydlig organisation för utförande av beslutade åtgärder, innefattande uppgifter om vem som är ansvarig för att olika åtgärder samt former för vidareapportering inom verksamheten.

Dessa rutiner och handlingsplaner bör vara kända och hållas tillgängliga för organisationens personal.

#### *Uppföljning av inträffade avbrott och störningar*

Tillhandahållaren bör regelbundet följa upp inträffade avbrott och störningar i verksamheten samt beakta deras orsaker vid planering och utbyggnad av infrastruktur. För dessa ändamål bör rutiner upprättas.

Rutinerna bör innefatta bl.a. följande:

- Tillvägagångssätt för identifiering av avbrottets eller störningens orsak,
- planering och införande av åtgärder för att förhindra att samma avbrott eller störning upprepas, samt
- former för vidareberapportering inom verksamheten.

---

Dessa allmänna råd tillämpas från och med den 7 maj 2007.

På Post- och telestyrelsens vägnar

MARIANNE TRESCHOW

Eva Liljefors