Rapportnummer PTS-ER 2018:17
Datum 2018-05-24

Rapport:

Arbete och normer för driftsäkra elektroniska kommunikationer

Arbete och normer för driftsäkra elektroniska kommunikationer

Rapportnummer
PTS-ER 2018:17

Diarienummer
18-5821

ISSN
1650-9862

Författare
Christina Hedlund
Karin Lodin
Anna Montelius

Post- och telestyrelsen
Box 5398
102 49 Stockholm

08-678 55 00
pts@pts.se
www.pts.se

Innehåll

Sammanfattning

Marknaden för elektronisk kommunikation kännetecknas av komplexa nät och många olika aktörer som är ömsesidigt beroende av varandra.

De grundläggande lagkraven på driftsäkerhet härrör från EU-direktiv, och ska säkerställa att operatörerna uppfyller grundläggande krav på driftsäkerhet. Post- och telestyrelsen, PTS, tar fram föreskrifter och utövar tillsyn med stöd av dessa regler.

Utöver den grundläggande nivån kan operatörernas kunder ställa krav på säkrare leveranser, och betala marknadsmässiga priser för detta. Det innebär ett ansvar för de användare som har behov av extra hög säkerhet att, till exempel genom avtal med operatören, säkerställa att få den nivå av driftsäkerhet som behövs.

Genom statlig finansiering bidrar PTS även till åtgärder som syftar till att stärka sektorn för elektronisk kommunikation, så att allvarliga händelser kan undvikas, eller att konsekvenserna av dessa kan hanteras bättre. Sådana så kallade robusthetshöjande åtgärder kommer i fråga endast där åtgärder inte krävs enligt lag och där det inte finns förutsättningar för investeringar på kommersiell grund.

För att förbättra förutsättningarna för god driftsäkerhet föreslår PTS liksom i en tidigare rapport, förstärkta befogenheter i vissa avseenden, bland annat vad gäller informationsinhämtning från operatörerna och sanktionsavgifter. Vidare framhåller myndigheten behovet av ökade resurser för robusthetshöjande åtgärder med anledning av det förändrade säkerhetsläget. Dessutom påpekar PTS utmaningen som ligger i att byalag och fiberföreningar bygger nät som är viktiga för Sveriges framtid, samtidigt som de ofta faller utanför lagens krav på driftsäkerhet.

1 Inledning

1.1 Bakgrund

PTS är en förvaltningsmyndighet med ansvar främst inom postområdet och området för elektronisk kommunikation. Myndigheten ska verka för att målen inom politiken för informationssamhället uppnås. PTS har bland annat till uppgift att arbeta för säkrare elektroniska kommunikationer i fred, kris och under höjd beredskap. I myndighetens regleringsbrev för 2018 har regeringen under punkten 8, Tillförlitliga elektroniska kommunikationer, givit PTS följande uppdrag:

> Post- och telestyrelsen ska beskriva det arbete som bedrivs av operatörer och andra intressenter samt redovisa vilka normer som styr deras insatser och åtgärder för att säkerställa tillförlitliga elektroniska kommunikationer (robusthet, driftsäkerhet, redundans m.m.). Identifierade utvecklingsmöjligheter och behov av förändringar ska särskilt redovisas. Uppdraget ska redovisas till Regeringskansliet (Näringsdepartementet) senast den 30 maj 2018.

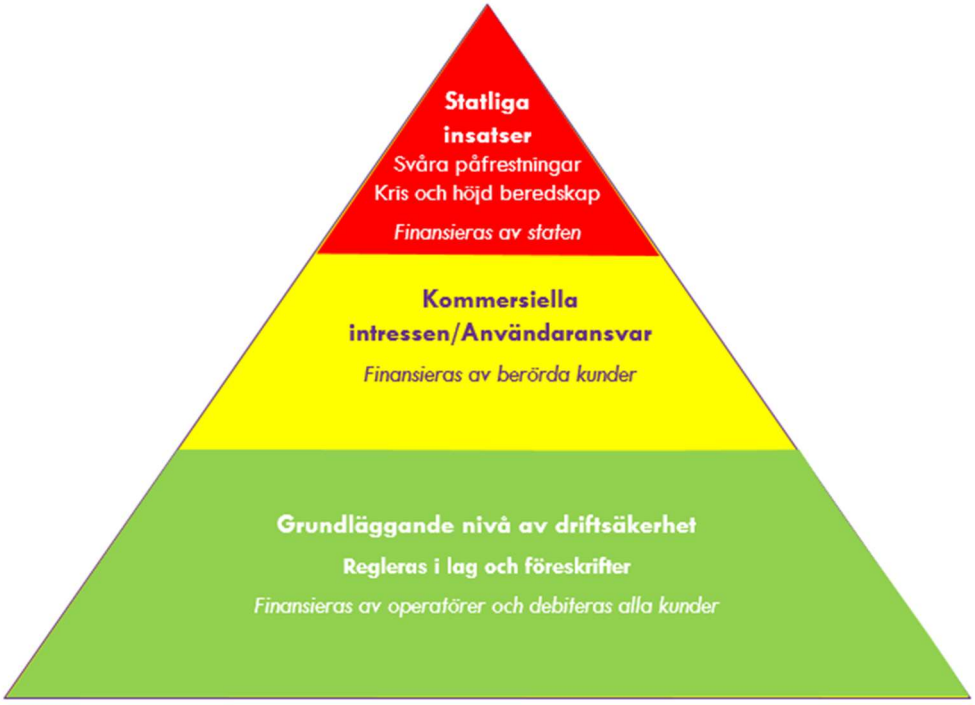
PTS har tolkat uppdraget så att det avgränsas till att omfatta normer och insatser inom driftsäkerhet och robusthet. Rapporten beskriver det arbete som bedrivs inom sektorn för att upprätthålla funktion och tillgänglighet samt uthållighet vid extraordinära händelser.

1.2 Övergripande om arbetet med driftsäkerhet och robusthet

Det är i första hand tillhandahållarna av elektroniska kommunikationsnät och tjänster (operatörerna) som har ansvar för att näten och tjänsterna fungerar. PTS ska med hjälp av tillsyn se till att operatörerna följer reglerna om driftsäkerhet i lagen (2003:389) om elektronisk kommunikation (LEK) med tillhörande föreskrifter. Reglerna ställer grundläggande krav på operatörernas driftsäkerhetsarbete. Det handlar om att de ska bedriva ett systematiskt arbete för att uppfylla rimliga krav på driftsäkerhet.

Ett stort ansvar vilar även på användarna själva. Den som har behov av driftsäkerhet utöver den lagstadgade (grundläggande) nivån, till exempel för att ett avbrott skulle kunna leda till betydande konsekvenser för samhällsviktig verksamhet eller näringsverksamhet, har ett eget ansvar att säkerställa en högre nivå av tillgänglighet. Det kan till exempel ske genom att betala ett högre pris till operatören för extra säkra lösningar eller högre servicenivå, eller genom att köpa redundanta förbindelser från flera operatörer.

Vidare bedriver PTS arbete med att genomföra så kallade robusthetshöjande åtgärder. Med robusthet avses förmåga att motstå, och återhämta sig ifrån, inre och yttre störningar. Åtgärderna syftar till att stärka sektorn för elektronisk kommunikation eller tillgången till elektronisk kommunikation, så att allvarliga händelser kan undvikas, eller att konsekvenserna av dessa kan hanteras bättre.



Operatörerna är enligt regelverket skyldiga att bedriva och bekosta driftsäkerhetsarbete för att nå upp till den grundläggande nivån. En högre driftsäkerhet tillhandahålls på marknadsmässiga villkor, och den användare som har behov av säkrare tjänster har ett ansvar att genom avtal se till att skaffa det. Statliga robusthetsåtgärder syftar till att stärka sektorn för elektronisk kommunikation eller tillgången till elektronisk kommunikation, så att allvarliga händelser kan undvikas, eller konsekvenserna av dessa kan hanteras bättre.

2 Aktörer och nät

Operatörer ska anmäla sin verksamhet till PTS. I januari 2018 fanns cirka 640 operatörer anmälda hos PTS.

Operatörerna i Sverige bedriver olika typer av verksamhet. Vissa operatörer tillhandahåller endast svartfiber, medan andra endast tillhandahåller tjänster, till exempel bredbandsaccess, traditionell fast telefoni eller ip-baserad telefoni. Det finns också operatörer som tillhandahåller hela kedjan, från kanalisation och fiber till slutkundstjänster. En del operatörer säljer tjänster som helt går i andras nät.

När det gäller marknadsandelar kan man konstatera att för såväl bredbands-anslutningar som mobila och fasta telefonitjänster så har en handfull leverantörer över 90 procent av det totala antalet abonnenter.[1] På nationell nivå finns alltså huvuddelen av abonnenterna hos ett relativt litet antal operatörer.

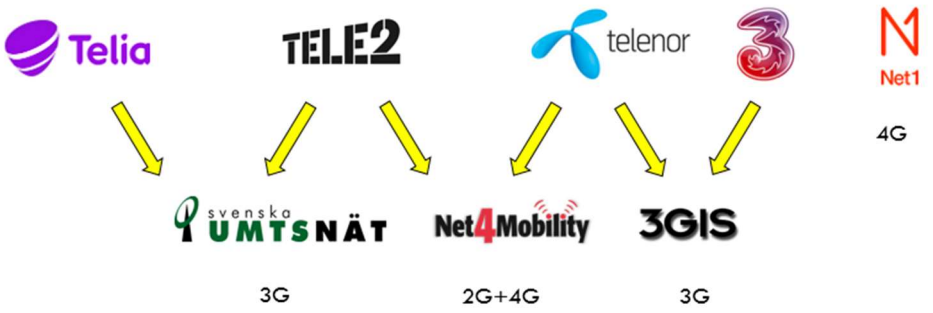
2.1 Mobiloperatörer

Mobilnäten består något förenklat av både en radiodel och en fast del. Radiodelen ansluter till användarnas mobilutrustning, den fasta delen av nätet kopplar samman radiodelarna med resten av operatörens nät. Ett mobilnät består alltså både av basstationer som ansluter användarnas terminaler till nätet och ett fast nät som sammanbinder dessa. Den fasta delen är huvudsakligen fiberbaserad men radiolänkar förekommer även i accessdelen av näten.

Den fasta delen av nätet kan vara helt ägd av en mobiloperatör, eller bestå helt eller delvis av förbindelser som hyrs av någon annan aktör. Här kan alltså andra fastnätsoperatörer ha en viktig roll för att mobilnäten ska fungera.

Det finns huvudsakligen fem operatörer som äger mobilnät i Sverige: Telia, Tele2, Telenor, Tre och Net1. För att spara kostnader samarbetar operatörerna i olika nätbolag. Nätsamarbeten mellan mobiloperatörerna har varit vanliga sedan 3G-utbyggnaden påbörjades i Sverige, och i dag har de flesta operatörer samägda nät med andra mobiloperatörer. Telia och Tele2 har ett gemensamt 3G-nät liksom Tre och Telenor, medan Telenor och Tele2 bygger gemensamma 2G- och 4G-nät.

[1] Källa, svensk telekommarknad första halvåret 2017, http://www.statistik.pts.se/media/1266/stm-1h2017_slut.pdf



Det finns möjlighet att köpa mobila tjänster också från andra operatörer än de fem nätägande bolagen. Så kallade virtuella mobiloperatörer levererar tjänster i nät som ägs av en annan operatör.

2.2 Fastnätsoperatörer

Fasta nät består av flera olika delar, och kan byggas med olika typer av teknik.

Det finns **nationella nät** som knyter samman landets olika regioner, och ansluter till internationella nät. Dessa nät ägs av landets stora operatörer eller är samarbeten mellan medelstora och mindre operatörer och benämns även fjärrnät, stomnät, stamnät eller backbonenät. De **regionala näten** knyter ihop nät inom en region, och ägs ofta av nationella eller regionala operatörer, såsom stadsnätskluster eller medelstora operatörer. **Anslutningsnäten** knyter samman regionnät med accessnät. De ägs till exempel av nationella operatörer eller lokala stadsnät och finns ofta inom en tätort eller en kommun. **Accessnät** kallas den sista delen av nätet som ansluter användarna till nätet. Accessnäten i Sverige har tidigare huvudsakligen bestått av kopparnät, men numera är fiber och radiolänkar de vanligaste teknikerna. Accessnäten ägs av stora nationella operatörer (t.ex. Telia och IP-only) eller lokala stadsnät.

Kommunikationen i fasta nät görs i flera nivåer. Näten består fysiskt av i första hand fiber- eller kopparledningar (passiv nivå) och aktiv utrustning. Ofta hyrs fiberledningar ut utan någon aktiv utrustning och kallas då svartfiber. Den aktiva utrustningen, såsom switchar och routrar förmedlar signaler i fibernätet.

I Sverige tillhandahålls tjänster ofta på två nivåer, så kallade kommunikations-operatörstjänster (KO-tjänster) och slutkundstjänster, till exempel bredband, telefoni eller TV. Modellen med kommunikationsoperatörer ger en möjlighet för användarna att välja mellan en rad olika tjänsteleverantörer utan att behöva göra någon omkoppling på fysisk nivå.

2.3 Stadsnätsoperatörer

På lokal nivå spelar mindre operatörer en stor roll främst vad gäller tillhandahållande av fast bredband. I många kommuner finns kommunalt ägda bredbandsnät, så kallade stadsnät. Det finns mer än 180 stadsnät i Sverige. Dessa varierar mycket i storlek och har väldigt olika förutsättningar beroende på bland annat kommunernas yta, geografi, befolkningstäthet och skatteunderlag. Förutsättningarna beror också på historiska orsaker, som vilken infrastruktur som tidigare funnits, samt vilket intresse och engagemang som funnits i kommunerna.

2.4 Fiberföreningar och byalag

I områden som inte nås av andra nät har användare ofta gått samman och med olika typer av bredbandsstöd har sådana sammanslutningar, byalag och fiberföreningar, byggt lokala bredbandsnät.

De nät som byggs av byalag och fiberföreningar vänder sig oftast till en begränsad krets av slutanvändare inom det aktuella byalaget eller den aktuella föreningen. De är därför normalt inte att anse som allmänt tillgängliga, och omfattas inte av kraven på driftsäkerhet i LEK. Vissa krav på robusthet och dokumentation ställs dock i samband med tilldelning av eventuellt bredbandsstöd.

2.5 Branschorganisationer

Det finns också branschorganisationer som arbetar för och tar till vara operatörernas intressen.

2.5.1 IT & Telekomföretagen

IT & Telekomföretagen är den bransch- och arbetsgivarorganisation som bland annat organiserar många av operatörerna. De har cirka 1 200 medlemsföretag. Deras huvudfokus är att tydliggöra nyttan av IT och telekom och stödja användningen i samhället samt att förenkla för IT- och telekomföretag och stimulera tillväxt i branschen. IT- och telekomföretagen har en samverkansgrupp för beslutsfattare inom branschen, Telekområdet.

2.5.2 Svenska Stadnätsföreningen

Svenska Stadnätsföreningen, SSNf, är en oberoende bransch- och intresseorganisation som organiserar 155 stadsnät och 117 leverantörer av tjänster och utrustning inom bredbandsområdet. Föreningen verkar bland annat för robusthet, men även för att säkerställa icke-diskriminerande villkor och god konkurrens i nätet. Stadsnätsföreningen är aktiv i flera forum, bland annat Bredbandsforum, Nationella Telesamverkansgruppen (NTSG), Stadsnätens infrastruktursamverkansgrupp (SiSG) och Telekområdet. Föreningen stöttar

också stadsnäten i regional och länsvis dialog i frågor om bredbandsinfrastruktur och digitalisering.

2.6 Samverkansgrupper

Det finns många grupper för samverkan inom telekomsektorn. Nedan beskrivs några av dessa och deras roll.

2.6.1 Regeringens Bredbandsforum

Regeringen beslutade i november 2009 om en bredbandsstrategi för Sverige. En viktig del av strategin är Bredbandsforum. Forumet främjar samverkan kring bredbandsutbyggnad. Företag, myndigheter och organisationer möts i Bredbandsforum för att tillsammans hitta lösningar som ökar tillgången till bredband i hela landet.

Regeringen beslutade i mars 2010 att inrätta forumet med mandat tom 2011, och har därefter konstaterat att forumet fungerar väl och förlängt mandatet först till och med 2015 och sedan till 2020.

Bredbandsforum leds av en styrgrupp där statsrådet med ansvar för digitaliseringsfrågor är ordförande. Relevanta frågor och områden behandlas i tidsbegränsade arbetsgrupper. Bredbandsforums löpande verksamhet drivs av ett kansli.

2.6.2 Nationella telesamverkansgruppen

Nationella telesamverkansgruppen, NTSG, är ett frivilligt samarbetsforum med syfte att stödja återställandet av den nationella infrastrukturen för elektroniska kommunikationer vid extraordinära händelser. Läs mer om NTSG i avsnitt 4.4.2.

2.6.3 Stadsnätens infrastruktursamverkansgrupp

Stadsnätens infrastruktursamverkansgrupp, SiSG, är ett forum för samverkan och utbildning inom säkerhetsområdet. SiSG håller genom SSNf kontinuerlig dialog med NTSG.

SiSG säkerställer att rätt och relevant information gällande stadsnätens driftläge under både normalläge och kris förmedlas och har ansvar för att förmedla relevant information från NTSG till medverkande stadsnät.

2.6.4 Näringslivets säkerhetsdelegation

Näringslivets Säkerhetsdelegation - Nätverket för lönsam riskhantering, NSD, är ett forum för idé-, erfarenhets- och kunskapsutbyte för säkerhetsfrågor. Det

är en grupp inom Svenskt Näringsliv som arbetar för att bidra till bättre säkerhets- och riskmedvetande i företagen och hos allmänheten.

2.7 Komplexa nät och ömsesidiga beroenden

De elektroniska kommunikationsnäten är ofta komplexa och en mängd aktörer bidrar genom att äga, hyra och driva nät och tillhandahålla tjänster på olika nivåer i dessa nät. Komplexiteten leder till att det ofta finns redundans, eftersom det finns flera sätt att lösa kommunikationen mellan två punkter i nätet. Det leder dock också till ömsesidiga beroenden som kan medföra en viss sårbarhet, eftersom en kedja aldrig är starkare än den svagaste länken.

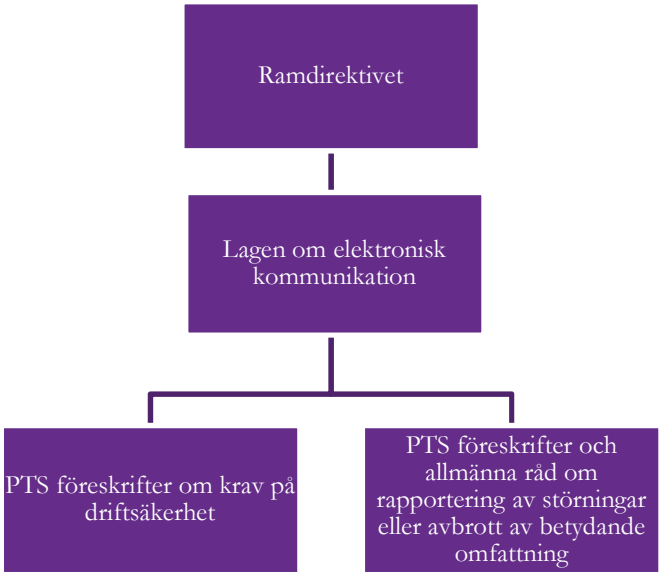
Om alla operatörer hade byggt helt egna parallella mobilnät hade det inte varit affärsmässigt möjligt att skapa så stor täckning som finns i dag. Nätsam-arbetena, som medför minskade kostnader för operatörerna, kan dock även medföra en större sårbarhet för störningar, bland annat genom att stora störningar i mobilnäten kan drabba flera operatörer samtidigt.

För att minska risken att drabbas av störningar och avbrott kan användare köpa tjänster från flera olika operatörer. Det är då viktigt att säkerställa att dessa operatörer inte är beroende av gemensam infrastruktur. När ett nät inte fungerar kopplas samtal till nödnumret 112 automatiskt via det eller de nät som fortfarande fungerar. Den möjligheten kan också påverkas av operatörernas ömsesidiga beroenden.

Basstationerna är ofta anslutna till fibernät, vilket innebär att ett brott på fibern inte bara drabbar de fasta näten, utan också kan innebära avbrott för mobilkunder i området om det inte finns redundans.

3 Normer

Det finns bindande regler om driftsäkerhet som har sitt ursprung i EU-direktiv och som har genomförts i den svenska lagen om elektronisk kommunikation och förtydligas och preciseras i PTS föreskrifter.



Hierarki över de bindande regelverken med driftsäkerhetsbestämmelser.

3.1 EU-direktiv

De bindande krav som finns för operatörerna när det gäller driftsäkerhet grundar sig på artikel 13a i det så kallade ramdirektivet, i dess lydelse efter de ändringar som gjordes i detta 2009[2].

Bestämmelsen säger bland annat att operatörerna ska vidta lämpliga tekniska och organisatoriska åtgärder för att på ett tillfredsställande sätt skydda säkerheten i sina nät eller tjänster. Åtgärderna ska utnyttja den senaste tekniken och säkerställa en lämplig säkerhetsnivå för den beräknade risken.

Operatörerna är även skyldiga att meddela den behöriga nationella regleringsmyndigheten, i Sveriges fall PTS, om överträdelser av säkerheten eller integriteten som i betydande omfattning påverkat driften av nät och tjänster.

[2] Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster, senast ändrat genom direktiv 2009/140/EG av den 25 november 2009.

PTS ska vid behov informera de nationella regleringsmyndigheterna i övriga medlemsstater och Europeiska byrån för nät- och informationssäkerhet (Enisa), och myndigheten kan även informera allmänheten eller kräva att företagen gör det, om den slår fast att ett avslöjande av överträdelsen ligger i allmänhetens intresse.

En gång om året ska PTS lämna in en sammanfattande rapport till kommissionen och Enisa om de anmälningar som kommit in och de åtgärder som vidtagits.

För närvarande pågår en översyn av de EU-direktiv som reglerar området för elektronisk kommunikation. Kommissionen kom i oktober 2016 med ett förslag till direktiv om inrättande av en europeisk kodex för elektronisk kommunikation[3] som för närvarande förhandlas inom EU. När det gäller ramdirektivet så kommer tillämpningsområdet för den bestämmelse som idag utgör artikel 13a (föreslagen artikel 40 i den föreslagna kodexen) troligen att utvidgas. Kodexen föreslås gälla för fler aktörer, exempelvis sådana som tillhandahåller kommunikationstjänster över internet (så kallade OTT-tjänster). Genom en ny definition av begreppet säkerhet i förslagets artikel 2 punkten 22 förtydligas att reglerna har ett större skyddsomfång än enligt tidigare. Utöver driftsäkerhet kommer de också att omfatta riktighet, integritet och konfidentialitet.

3.2 Svensk lag och förordning

Artikel 13a i ramdirektivet har genomförts i svensk rätt genom 5 kap. 6 b och 6 c §§ i LEK.

Av 5 kap. 6 b § LEK framgår bland annat att den som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att verksamheten uppfyller rimliga krav på driftsäkerhet. Med driftsäkerhet avses främst upprätthållande av funktion och tillgänglighet, men även uthållighet vid extraordinära händelser.

Det är värt att notera att reglerna omfattar nät som är allmänt tillgängliga. Vissa nät, som endast ansluter en begränsad krets av användare är inte allmänt tillgängliga och omfattas inte av kraven på driftsäkerhetsarbete.

[3] https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:52016PC0590&from=SV

De åtgärder som enligt lagens krav ska vidtas ska vara ägnade att skapa en säkerhetsnivå som, med beaktande av tillgänglig teknik och kostnaderna för att genomföra åtgärderna, är anpassad till risken för störningar och avbrott.

Syftet med bestämmelsen är att skapa en grundläggande driftsäkerhetsnivå för elektroniska kommunikationer. Reglerna innebär dock inte ett krav på att kommunikationerna alltid måste fungera för varje enskild användare. Det är inte heller reglerat hur långt ett avbrott får vara.

Av 5 kap. 6 c § LEK framgår bland annat skyldigheten för tillhandahållarna att rapportera in störningar och avbrott av betydande omfattning till tillsyns-myndigheten, det vill säga PTS. Vidare framgår möjligheten för PTS att kräva att operatören informerar allmänheten om inträffade incidenter.

Av förordningen (2007:951) med instruktion för Post- och telestyrelsen (instruktionen) framgår bland annat att PTS ska verka för robusta elektroniska kommunikationer och minska risken för störningar, inbegripet att upphandla förstärkningsåtgärder, samt verka för ökad krishanteringsförmåga. Det framgår av regleringsbrevet för PTS att myndigheten genom upphandling får

> - tillgodose totalförsvarets behov av posttjänster och elektroniska kommunikationstjänster under höjd beredskap, och
> - stärka samhällets beredskap mot allvarliga störningar av elektronisk kommunikation och posttjänster i fred.

Utöver de ovan nämnda reglerna finns ett antal andra lagregler och förordningar som främst är avsedda att hantera samhällsviktiga funktioner i händelse av kris, och höjd beredskap. Dessa faller utanför avgränsningen för denna rapport, men bidrar även till ökad driftsäkerhet i elektroniska kommunikationer och är bland annat:

- 1 kap. 8-9 §§ LEK reglerar kommunikationsverksamhet i krig m.m.
- lagen (1992:1403) om totalförsvar och höjd beredskap, som reglerar hur vissa företag och organisationer är skyldiga att fortsätta sin verksamhet i krig,
- förordningen (2015:1053) om totalförsvar och höjd beredskap och förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap som bland annat stadgar PTS ansvar för att minska sårbarheten i samhället och utveckla en god förmåga att hantera sina uppgifter, i samband med kriser eller höjd beredskap och

- säkerhetsskyddslagen (1996:627) gäller för myndigheter och enskilda vars verksamhet är av betydelse för rikets säkerhet eller särskilt behöver skyddas mot terrorism.

3.3 Föreskrifter om driftsäkerhet

PTS har enligt LEK och förordningen (2003:396) om elektronisk kommunikation bemyndigande att utfärda föreskrifter avseende på vilket sätt såväl 5 kap. 6 b § LEK som 5 kap. 6 c § LEK ska efterlevas. I PTS föreskrifter om krav på driftsäkerhet (PTSFS 2015:2) har myndigheten förtydligat vilka krav på skyddsåtgärder som gäller för att tillhandahållarna ska anses upprätthålla en rimlig nivå av driftsäkerhet. Av PTS föreskrifter och allmänna råd om rapportering av störningar eller avbrott av betydande omfattning (PTSFS 2012:2) framgår när och på vilket sätt rapportering av incidenter ska ske till PTS.

3.3.1 PTS föreskrifter med krav på driftsäkerhet

Föreskrifternas krav kan delas upp i tre olika kategorier beroende på vilken verksamhet som bedrivs av den operatör som omfattas av kraven. En operatör kan ha verksamhet som faller inom flera kategorier.

Den första kategorin avser generella krav som omfattar samtliga operatörer. Till dessa krav hör regler om övergripande driftsäkerhetsarbete (3 §), dokumentation av tillgångar och förbindelser (4 §), riskanalys och konsekvensanalys (5-6 §§), incidenthantering (7 §), kontinuitetsplanering (8 §), åtgärder efter riskbedömning (9-12 §§), åtgärder avseende åtkomst och behörighet (13 §) och åtgärder avseende övervakning och beredskap (14 §).

Den andra kategorin avser krav för operatörer med kännedom om hur många aktiva anslutningar som deras tillgångar betjänar. Inom denna kategori faller till exempel tjänstetillhandahållare och kommunikationsoperatörer, medan till exempel svartfiberleverantörer normalt inte omfattas. De operatörer som omfattas av kraven ska klassificera sina tillgångar efter hur många aktiva anslutningar som kan omfattas av en störning eller avbrott till följd av att tillgången upphör att fungera normalt (15 §).

Föreskrifterna innehåller en tabell för klassificering, där tillgångar klassas högre ju fler aktiva anslutningar som skulle påverkas om tillgången slutade fungera. Med utgångspunkt i tillgångarnas klassificering ska operatören efterleva krav på redundans och reservkraft (16-21 §§).

Den tredje kategorin avser operatörer för mobila kommunikationsnät och mobila kommunikationstjänster. Dessa ska, utöver de generella kraven på reservkraft enligt kategori två, även efterleva ett särskilt krav på reservkraft och yttäckning (22 §).

3.3.2 PTS föreskrifter och allmänna råd om rapportering av störningar eller avbrott av betydande omfattning

PTS har tagit fram föreskrifter som förtydligar när och på vilket sätt en operatör är skyldig att rapportera en driftsäkerhetsincident till PTS. Föreskrifterna ses för närvarande över av myndigheten. Incidentrapporteringen är enligt gällande föreskrifter uppdelad i en inledande och en kompletterande rapportering där den första rapporten ska inkomma till myndigheten senast vardagen efter det att incidenten avhjälpts. Den inledande rapporten ska bland annat innehålla uppgift om incidentens omfattning och varaktighet, samt angivelse av drabbade nät och tjänster.

En kompletterande rapport med mer fullständig information om till exempel vad som orsakat incidenten och vilka åtgärder som vidtagit för att hantera incidenten och undvika att den upprepas, ska sedan inkomma till PTS senast två veckor efter att incidenten avhjälpts.

Det är endast betydande störningar och avbrott som ska rapporteras till myndigheten. Föreskrifterna innehåller en tabell med gränsvärden för att avgöra om en incident är av så betydande omfattning att den ska rapporteras.

Tid som störningen eller avbrottet pågått	*Störningens eller avbrottets uppskattade omfattning*
≥ 1 timme	**≥ 150 000 abonnenter eller** **≥ 15 000 km² sammanhängande berört område eller** **≥ 50 % kapacitetsbortfall**
≥ 2 timmar	**≥ 30 000 abonnenter eller** **≥ 5 000 km² sammanhängande berört område eller** **≥ 30 % kapacitetsbortfall**
≥ 6 timmar	**≥ 5 000 abonnenter eller** **≥ 2 500 km² sammanhängande berört område eller** **≥ 20 % kapacitetsbortfall**
≥ 24 timmar	**≥ 2000 abonnenter eller** **≥ 1 000 km² sammanhängande berört område eller** **≥ 10 % kapacitetsbortfall**

Dessa gränsvärden är PTS tolkning av vad som utgör en betydande störning. Gränsvärdena har valts efter en avvägning av myndighetens behov av

information som underlag för tillsyn, och konsekvenserna i form av merarbete och kostnader för de rapporteringsskyldiga.

I samband med en pågående översyn av föreskrifterna har PTS övervägt om gränsvärdena borde vara lägre så att fler incidenter blir rapporteringspliktiga. PTS bedömer dock för närvarande inte att det är lämpligt att sänka dessa gränsvärden. För information om störningar som berör färre användare ser PTS att andra metoder, såsom omvärldsbevakning och inhämtning av statistik från operatörerna är mer ändamålsenligt.

3.4 Icke bindande regler

Utöver bindande regler finns också icke bindande normer och rekommendationer som ska bidra till en förbättrad driftsäkerhet.

3.4.1 Enisas rekommendationer

Den europeiska nät- och informationssäkerhetsbyrån Enisa har utfärdat tre rekommendationer som berör tillämpningen av artikel 13a i ramdirektivet.

I rekommendationen ”Technical Guideline on Security Measures”[4] anges ett antal övergripande sakområden vilka medlemsstaterna rekommenderas att ställa krav inom, för att uppnå en godtagbar säkerhetsnivå.

Rekommendationen ”Technical Guideline on Threats & Assets”[5] anger bl.a. en modell för klassificering av tillgångar och av vanliga hot mot näts och tjänsters driftsäkerhet. Därtill beskriver rekommendationen översiktligt hur operatörer bör arbeta med riskanalyser.

Slutligen har Enisa i rekommendationen ”Technical Guideline on Incident Reporting”[6] tagit fram ett stöd för incidentrapportering, främst beträffande hur medlemsländerna ska rapportera de mest betydande incidenterna till Enisa och Kommissionen.

3.4.2 Standarder och ledningssystem

Många operatörer liksom många andra organisationer, baserar sitt arbete med informationssäkerhet, där driftsäkerhet ingår, på etablerade standarder, såsom ISO/IEC 27000-serien - ledningssystem för informationssäkerhet.

[4] https://www.enisa.europa.eu/publications/technical-guideline-on-minimum-security-measures
[5] https://www.enisa.europa.eu/publications/technical-guideline-on-threats-and-assets
[6] https://www.enisa.europa.eu/publications/technical-guideline-for-incident-reporting

Svenska stadsnätsföreningens ledningssystem

Svenska stadsnätsföreningen har tagit fram ett särskilt ledningssystem för att hjälpa medlemmarna att följa PTS föreskrifter med krav på driftsäkerhet. Ledningssystemet -*Driftsäkerhetsarbete för elektroniska kommunikationsnät och tjänster* - är anpassat till stadsnätsverksamhet.

Ledningssystemet baseras på etablerade standarder som ISO/IEC 27000 serien och ITIL. Systemet består av:

1. Sammanställande presentation
2. Ledningssystem
3. Incidenthantering
4. Risk- och Sårbarhetsanalys (RSA)
5. Förändringshantering
6. Konsekvensanalys
7. Kontinuitetsplanering
8. Dokumentation av tillgångar och förbindelser

Stadsnätsföreningen har hållit en rad utbildningar och webinarier som beskriver ledningssystemet. Stadsnätsföreningen har genom samarbetspartners erbjudit utbildning och genomförandehjälp för stadsnät som behöver stöd i sitt driftsäkerhetsarbete. Detta metodstöd och det arbete föreningen lägger ned på utbildningar och stöd kan bidra till förbättrade möjligheter för mindre aktörer att efterleva reglerna.

3.4.3 MSB:s metodstöd för systematiskt informationssäkerhetsarbete

Myndigheten för samhällsskydd och beredskap, MSB, har tagit fram ett metodstöd som riktar sig till organisationer som avser arbeta systematiskt med informationssäkerhet.[7] Också detta metodstöd baseras på ISO/IEC 27000-serien.

3.4.4 Ledningskollen

En av de vanligaste orsakerna till störningar och avbrott i elektroniska kommunikationstjänster är att kablar skadas i samband med grävningsarbeten av olika slag. För att minska risken för dessa problem finns webbtjänsten

[7] https://www.informationssakerhet.se/metodstod-for-lis/

Ledningskollen. Tjänsten drivs av PTS och finansieras av PTS, Svenska Kraftnät och Trafikverket.

Ledningskollen är en kostnadsfri webbtjänst som underlättar kommunikation mellan ägare av ledningar, kablar och annan infrastruktur och de som vill veta var dessa finns. Genom webbtjänsten kan den som planerar att gräva få kontakt med cirka 1 000 ledningsägare. Den som planerar någon slags markarbete begär då ledningsanvisning/kabelanvisning av den som äger ledningar i området, för att minska risken för att ledningar grävs av. På så sätt behöver den som ska gräva i ett område endast ställa en fråga i webbtjänsten i stället för att identifiera och kontakta samtliga ledningsägare i ett område. Anslutna ledningsägare slipper också frågor som inte rör det område där de har ledningar. Både att registrera sina nuvarande och planerade ledningsnät samt skapa ärenden i Ledningskollen är kostnadsfritt.

Tjänsten bidrar till att skydda flera viktiga samhällsfunktioner, som el, tele och vatten, genom att minska risken för skador på infrastrukturen.

Av säkerhets- och sekretesskäl finns inte information om exakt placering av ledningar samlad i Ledningskollen. Ledningskollen kan också bara svara för infrastruktur från de deltagare som står bakom tjänsten. Ju fler som är med desto större blir de positiva effekterna i form av minskade avgrävningar och större samordningsmöjligheter. Idag finns närmare 1 000 ledningsägare med i Ledningskollen. Mer information finns på www.ledningskollen.se.

3.4.5 Robust fiber

Robust fiber

Behovet av bredband ökar ständigt i samhället. Den fiberinfrastruktur som byggs idag kommer vi att vara beroende av under lång tid framöver. Därför finns ett samhällsintresse av att den som anlägger fiber gör det på ett robust och driftsäkert sätt.

Flera av branschens aktörer har med stöd från PTS tagit fram anvisningar, kallade Robust fiber. Anvisningarnas syfte är att beskriva och kravställa en lägsta nivå för hur ett robust nät ska anläggas. Robust fiber bidrar till att höja robusthetsnivån i fiberanläggningar genom att branschens aktörer följer de krav som finns i anvisningarna.

Anvisningarna riktar sig till branschens intressenter, till exempel nätägare, fiberföreningar, leverantörer av materiel, entreprenadföretag som anlägger bredbandsinfrastruktur, tillverkare av anläggningsmaskiner, aktörer för hantering av utbildning och certifiering för företag och individer samt utförare av infrastrukturprojekt. Även handläggare vid myndigheter, kommuner och landsting är målgrupp för anvisningarna.

Robust fiber utgår från standarder och regelverk inom de olika delområden som berörs i anvisningarna.

Anvisningarna ska bland annat användas som:

- Underlag för utbildning.
- Tekniskt stöd vid upphandling.
- Informationsmaterial för tillståndsgivare.
- Beskrivning över tillvägagångssätt för besiktning.
- Beskrivning av momenten i ett fiberanläggningsprojekt.
- Grund för kravspecifikation vid ansökan om bidrag.

För att höja kompetensnivån om robusta fiberanläggningar hos företag och individer så erbjuds certifieringar och utbildningsbevis i olika nivåer.

All dokumentation rörande anvisningarna finns tillgänglig på www.robustfiber.se.

3.4.6 Krav i bredbandsstödsreglerna

För att främja bredbandsutbyggnaden i hela landet finns möjlighet att söka bidrag, så kallat bredbandsstöd. För närvarande tilldelas statligt stöd för bredbandsutbyggnad genom landsbygdsprogrammet främst till byalag och fiberföreningar. Detta program administreras av Jordbruksverket. De nät som byggs av byalag och fiberföreningar vänder sig till en begränsad krets av slutanvändare inom den aktuella föreningen. De är därför normalt inte att anse som allmänt tillgängliga nät, och omfattas inte av kraven på driftsäkerhet i LEK.

Jordbruksverket har dock föreskrifter som innehåller vissa krav på den som ska tilldelas bredbandsstöd. Kraven innefattar bland annat att den som får stöd ska genomföra vissa kontroller och upprätta dokumentation på visst sätt, upprätta en förvaltningsplan samt registrera bredbandsnätet på webbtjänsten Ledningskollen. Uppfylls dessa krav främjas driftsäkerheten, men det motsvarar inte de krav som finns i lag och föreskrifter för nät och tjänster som är anmälningspliktiga enligt LEK.

Bredbandsstöd tilldelas också genom regionalfonden som administreras av Tillväxtverket. Under perioden 2014-2018 har 29 projekt beviljats stöd från regionalfonden. Av stödmedelsmottagarna var 37,5 procent länsstyrelser, 22,5 procent kommuner, 22 procent aktiebolag och 17,5 procent regioner. Resterande 0,5 procent var ekonomiska föreningar.

Tillväxtverket har tagit fram en vägledning för bredbandsprojekt där myndigheten ställer en del krav. Tillväxtverket tillämpar också särskilda villkor för bredbandsprojekt som ska uppfyllas för alla delar av den stödfinansierade bredbandsanläggningen. Villkoren innefattar främst krav som ska säkerställa möjligheten till konkurrens i näten samt tillräcklig kapacitet. Det finns dock även vissa krav som påverkar driftsäkerheten i näten, bland annat krav på att den grundläggande infrastrukturen i bredbandsanläggningen ska vara dimensionerad och utformad för minst 40 års teknisk livslängd. Enligt villkoren ska också Ledningskollen användas vid projektering av bredbandsanläggningen. Efter slutfört arbete ska hela bredbandsanläggningen vara registrerad i Ledningskollen för att undvika skador och avgrävningar. Vidare ska bredbandsanläggningen som lägsta nivå uppfylla krav på dokumentation enligt IT & Telekomföretagens rapport Klassificering och dokumentation av fiberbaserad infrastruktur (2015-02-10) eller senare[8]. Tillväxtverket har tagit fram ”Vägledning för ett lyckat bredbandsprojekt” där information om hur nät kan anläggas på ett robust sätt ingår.

3.4.7 Krav i avtal

Som nämns ovan måste de användare som har behov av extra hög säkerhet, till exempel samhällsviktiga aktörer, säkerställa en högre nivå av tillgänglighet. Det kan till exempel ske genom att avtala om en högre servicenivå, så kallad Service Level Agreement (SLA).

Om användare med sådana behov ställer adekvata krav på driftsäkerhet genom sina avtal så kan det bidra till en generell ökning av driftsäkerheten i Sverige.

[8] https://www.itot.se/2015/02/rapport-klassificering-och-dokumentation-av-fiberbaserad-infrastruktur/

4 Hur arbetar PTS med driftsäkerhet och robusthet?

Ett av PTS övergripande mål är att främja tillgången till säker elektronisk kommunikation. Målet med PTS arbete med driftsäkerhetsfrågor är att nät och tjänster ska ha en nivå av driftsäkerhet som motsvarar användarnas behov. För att uppfylla målet arbetar PTS med såväl analysarbete som reglering, tillsynsaktiviteter och olika främjandeåtgärder.

4.1 Analysarbete

Som underlag för PTS arbete med driftsäkerhet görs analys av information från en rad olika källor. Bland annat analyseras de driftsäkerhetsincidenter som operatörerna rapporterar till PTS liksom de erfarenheter som dras i samband med myndighetens tillsyn på området. Vidare bedriver myndigheten en omfattande omvärldsbevakning, bland annat inom ramen för ett omvärldsnätverk. Omvärldsbevakning bedrivs också genom analys av tips och klagomål som inkommer till myndigheten, och genom den kontinuerliga bevakning av störningsläget inom sektorn som genomförs av myndighetens tjänsteman i beredskap. Identifierade trender analyseras och ligger till grund för planering och prioriteringar.

Enligt krisberedskapsförordningen (2015:1052) och MSB:s föreskrifter om statliga myndigheters risk- och sårbarhetsanalyser (MSB-FS-2016:7) finns en skyldighet för PTS att vartannat år genomföra en risk och sårbarhetsanalys (RSA) för sektorn elektronisk kommunikation. Denna RSA är också ett viktigt underlag när PTS väljer vilka åtgärder som ska prioriteras.

PTS analyser visar att de vanligaste orsakerna till betydande störningar och avbrott är:

1. avbrott eller störningar i samband med planerade förändringsarbeten, såsom felkonfigurationer,
2. avbrott i samband med längre strömavbrott, ofta i samband med extremt väder och
3. avbrott på grund av kabelbrott, ofta efter avgrävning eller annars i samband med entreprenadarbeten.

PTS arbetar på olika sätt för att förebygga dessa problem, såväl genom föreskrifter, som tillsyn och främjande arbete.

4.2 Reglering

En viktig del av PTS arbete med driftsäkerhet är framtagandet av föreskrifter och allmänna råd på området. Dessa beskrivs närmare ovan i avsnitt 3.3.

4.3 Tillsyn

Enligt 2 § i förordningen (2003:396) om elektronisk kommunikation är PTS tillsynsmyndighet enligt LEK. Enligt 7 kap. 1 § LEK ska tillsynsmyndigheten ha tillsyn över efterlevnaden av lagen och de beslut om skyldigheter eller villkor samt de föreskrifter som har meddelats med stöd av lagen.

PTS bedriver tillsyn över operatörernas driftsäkerhetsarbete. Tillsynen genomförs mot bakgrund av kända eller misstänkta problem på marknaden. PTS kan få vetskap om dessa problem på många olika sätt, det kan till exempel röra sig om anmälningar och klagomål från allmänheten eller andra myndigheter, omvärldsbevakning, incidentrapportering eller om slutsatser som dragits från en tidigare genomförd tillsynsinsats. Myndigheten avgör självständigt om den ska bedriva tillsyn i varje enskilt fall, och har således ingen skyldighet att bedriva tillsyn efter till exempel en anmälan om avbrott.

All tillsyn vid PTS ska utföras effektivt med god kvalitet, samt präglas av förutsägbarhet. PTS tillsyn är antingen händelsestyrd eller planlagd.

4.3.1 Händelsestyrd och planlagd tillsyn

När det inträffar incidenter av betydande omfattning ska operatörerna, som redogjorts för ovan, lämna incidentrapporter till PTS. Incidentrapporterna utgör ett underlag för PTS bedömning av om det finns tecken på allvarliga brister som behöver granskas omgående i en händelsestyrd tillsyn, eller om det är lämpligare att följa upp dem planlagt i ett senare skede. En händelsestyrd tillsyn riktar sig endast till den aktör som berörts av incidenten och begränsas oftast till de verksamhetsdelar eller tjänster som påverkats av händelsen. Även händelsestyrd tillsyn är framåtsyftande och fokuserar på att granska vilka åtgärder operatören vidtar för att undvika att liknande händelser inträffar igen.

En planlagd tillsyn omfattar ett urval operatörer och är ofta tematisk, till exempel genom att fokusera på en viss problematik.

PTS publicerar i slutet av varje år en **tillsynsplan** för driftsäkerhet som tar sikte på myndighetens tillsynsarbete under de kommande två åren.

PTS genomförda tillsynsinsatser och slutsatser från dessa sammanställs och publiceras varje vår i en **tillsynsrapport**. Dessutom publiceras information om pågående och nyligen avslutade tillsynsinsatser fortlöpande på pts.se.

PTS tillsyn bedrivs ofta i form av dialog, där påpekade brister normalt rättas till utan att myndigheten behöver vidta särskilda tillsynsåtgärder såsom underrättelse eller föreläggande.

I andra delar kan PTS konstatera att operatörerna inte fullt ut efterlever kraven. I fall då efterlevnad av reglerna kräver investeringar eller driver kostnader ser PTS ofta att operatörerna inte inleder arbetet med åtgärder förrän myndigheten inleder tillsyn.

4.3.2 Exempel på tillsyn på driftsäkerhetsområdet

1. Ett exempel på en återkommande planlagd tillsyn är den **årliga tillsynen** över incidentrapportering och inträffade incidenter. Den årliga tillsynen omfattar de fem största operatörerna och i tillsynen granskas såväl deras rutiner för incidentrapportering till PTS som samtliga inrapporterade incidenter under föregående år, hur de hanterats och vilka skyddsåtgärder som vidtagits för att undvika återkommande problem av samma slag. De incidenter som omfattats av en händelsestyrd tillsyn undantas dock, då de hanteras inom ramen för den tillsynen.

2. PTS har i början av år 2018 avslutat en tillsyn avseende **driftsäkerhet på landsbygden**. PTS studerade driftsäkerheten i kommunerna Sorsele, Storuman, Vilhelmina, Dorotea och Strömsund. Inom ramen för tillsynen besökte PTS dessa kommuner i slutet av september 2017. PTS begärde upplysningar från såväl nationella som lokala operatörer utifrån PTS föreskrifter om krav på driftsäkerhet. Slutsatserna från tillsynen publicerades i en särskild rapport[9].

3. PTS har en pågående planlagd tillsyn över operatörernas tillämpning av processer och planer för förändringshantering, med särskild inriktning mot **konfigurationshantering**. Det är en följd av att PTS konstaterat att en stor andel av de störningar och avbrott av betydande omfattning som inträffat i elektroniska kommunikationstjänster som telefoni och internet, helt eller delvis, har orsakats av fel som begås i samband med konfigurationsändringar. Ett av målen för PTS arbete med driftsäkerhet är att antalet störningar och avbrott som orsakas av fel och brister vid konfigurationsändringar ska minska.

4. Med anledning av att PTS driftsäkerhetsföreskrifter nyligen trädde i kraft granskade PTS under 2016 hur ett antal operatörer arbetar med **dokumentation av tillgångar och förbindelser**, vilket utgör ett av de

[9] Studie av driftsäkerhet på landsbygden, PTS-ER 2018:2.

grundläggande kraven i föreskrifterna. Varje operatör ska ha en aktuell och samlad bild över samtliga sina tillgångar och förbindelser, vilka funktioner de har och var de finns placerade. Det underlättar för operatören att vidta rätt åtgärder för att upprätthålla en hög skyddsnivå och följa upp driftsäkerheten över tid. Tillsynen visade att operatörerna uppfyller föreskrifternas krav på dokumentation av tillgångar och förbindelser. I kommande tillsyn planerar PTS att granska huruvida operatörerna har genomfört godtagbara riskanalyser för sina tillgångar och förbindelser.

4.4 PTS arbete med robusthetsfrämjande insatser

PTS ansvarar också för att med främjande insatser samordna och stödja aktörer som bedriver samhällsviktig verksamhet i sektorn elektronisk kommunikation. Ansvaret gäller både vid normala förhållanden och vid kris eller höjd beredskap. Staten, genom PTS, går därför in och bekostar vissa åtgärder för att skydda elektroniska kommunikationer mot allvarliga hot och påfrestningar i fredstid samt åtgärder för höjd beredskap. Syftet med dessa så kallade robusthetshöjande åtgärder är att tillförsäkra en högre nivå av säkerhet än den som föreskrivs i LEK och driftssäkerhetsföreskrifterna, och vad som efterfrågas på kommersiella grunder.

Sådana åtgärder är bland annat att arrangera och bidra till övningar och utbildningar, att främja olika typer av samverkan samt att finansiera robusthets-höjande åtgärder.

4.4.1 Övning och utbildning

PTS har inom ramen för sitt främjandearbete en strategi för utbildningar och övningar[10] som bygger på en helhetssyn där alla delar från individ- och företagsnivå, till övergripande sektorsnivå ingår.

Syftet med strategin och de utbildningar och övningar som genomförs inom ramen för denna är att öka sektorns förmåga att hantera större kriser och extraordinära händelser, så att konsekvenserna för hela samhället minimeras. Målgruppen för utbildningarna och övningarna är individer och företag eller organisationer inom sektorn som innehar egen teknisk utrustning, kunskap eller resurser som påverkar Sveriges kritiska infrastruktur för elektronisk kommunikation.

[10] Utbildnings- och övningsstrategi för krisberedskap för 2017-2021, sektorn elektronisk kommunikation, PTS-ER-2017:02

Strategin innehåller bland annat följande åtta strategiska mål för utbildning och övning

- Mål 1: Sektorn ska upprätthålla och utveckla sin förmåga att leda, samverka och kommunicera i extraordinära händelser
- Mål 2: Sektorn ska under perioden 2017-2021 bredda kunskapen om krisberedskapen i sektorn genom att involvera fler aktörer och fler roller från samma aktörer
- Mål 3: Under perioden ska sektorn ha förtydligat oklarheter i samhället kring roller, förväntningar och möjligheter avseende lägesbilder i en extraordinär händelse
- Mål 4: Sektorn ska under perioden bidra till utvecklingen av samhällets förmåga att prioritera samhällsviktig verksamhet
- Mål 5: Innan Totalförsvarsövning 2020 ska sektorns aktörer ha god kunskap om civilt försvar och god förmåga att uppnå de krav som ställs
- Mål 6: Innan Totalförsvarsövning 2020 ska sektorns aktörer ha god kunskap om samhällets aktörers roller och ansvar i höjd beredskap
- Mål 7: Nationella telesamverkansgruppens samarbete ska innan 2020 ha organiserats så att det även passar höjd beredskap och det nya säkerhetspolitiska läget
- Mål 8: Sektorns aktörer ska under perioden 2017-2021 uppnå en nivå av säkerhetsskydd anpassad till det förändrade säkerhetspolitiska läget

På sektorsövergripande nivå bidrar PTS även i externa övningar, såsom inom elsektorn och de samverkansövningar (SAMÖ) som Myndigheten för samhällsskydd och beredskap (MSB) anordnar.

PTS erbjuder även sektorns aktörer stöd att genomföra egna övningar och utbildningar för att höja aktörers enskilda krisberedskapsförmåga.

4.4.2 Samverkan

Samverkan inom NTSG

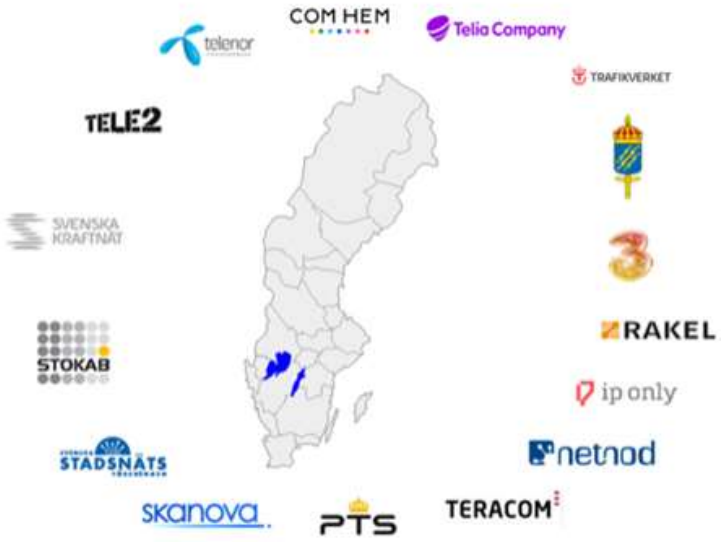
Operatörer hanterar dagligen störningar av större eller mindre karaktär. Vid större störningar, kriser eller extraordinära händelser kan det uppstå situationer som underlättas av att aktörerna bistår varandra.

Därför bildades Nationella telesamverkansgruppen (NTSG) år 2005. NTSG är ett frivilligt samarbetsforum med syfte att stödja återställandet av den nationella infrastrukturen för elektroniska kommunikationer vid allvarlig störning i samhället.

Kriteriet för medlemskap i NTSG är att operatören/organisationen har egen teknisk utrustning, kunskaper eller resurser som påverkar Sveriges kritiska infrastruktur för elektronisk kommunikation. De har genom sin roll möjlighet till stor påverkan på den kritiska nationella infrastrukturen för elektronisk kommunikation. Nya medlemmar kan komma att tillföras gruppen efter gemensamma beslut i NTSG.

För närvarande består NTSG av:

- Post- och telestyrelsen (PTS)
- Trafikverket
- Stokab
- Svenska Kraftnät
- Tele2 Sverige AB
- Telia Company AB
- Telenor AB Sverige
- Teracom
- Hi3G Access AB
- Stadsnätsföreningen
- Skanova
- IP-Only
- ComHem
- Netnod
- Försvarsmakten
- MSB Rakel



Gruppens arbete bygger på frivillighet och varje deltagare representerar sin egen organisation. PTS innehar för närvarande ordföranderollen och bistår med administrativt stöd.

Under en kris initieras gruppens arbete genom att någon gruppmedlem begär att gruppen samlas. Gruppen samlas därefter virtuellt eller fysiskt på en förutbestämd plats. Vid en kris sammanställer gruppen skadeläget, återrapporterar läget till berörda parter och ger vid behov förslag till åtgärder.

Gruppen kan också, om så krävs, koordinera insatser. Samverkan med andra aktörer i samhället är ett viktigt område för NTSG. Rutiner för samverkan med exempelvis länsstyrelser och andra viktiga aktörer i en krissituation utvecklas successivt.

Internationellt samarbete

I syfte att harmonisera tillämpningen av de nationella regler som genomför artikel 13a i ramdirektivet i EU:s medlemsländer leder Enisa en arbetsgrupp

med representanter från nationella tillsynsmyndigheter. PTS medverkar aktivt i denna arbetsgrupp. Gruppen håller regelbundna möten och syftet är att involvera samtliga medlemsstater i en öppen diskussion och fungerande kommunikation i frågor kring artikel 13a samt att underlätta kartläggning av betydande störningar och avbrott inom EU. Gruppen ska också stötta regleringsmyndigheterna i tillsynen, och har gjort så bland annat genom att bidra i Enisas arbete med att ta fram de riktlinjer som nämnts ovan i avsnitt 3.4.1.

PTS deltar också i ett nordiskt samarbete. Tillsammans med de nordiska systermyndigheterna hålls möten både på ledningsnivå och på handläggarnivå, där diskuteras bland annat erfarenheter från tillsyn och möjligheter att göra gemensamma studier eller insatser. Det nordiska samarbetet är värdefullt då det ger möjlighet att dra lärdomar från varandra, eftersom det finns liknande utmaningar och då operatörerna i många fall verkar i flera av de nordiska länderna.

4.4.3 Finansiering av robusthetshöjande åtgärder

Ytterligare en typ av åtgärd som PTS genomför för att främja tillförlitliga elektroniska kommunikationer är att helt eller delvis finansiera så kallade robusthetsåtgärder genom upphandling eller genom att utge ersättning för åtgärder.

Robusthetsåtgärderna syftar till att stärka sektorn för elektronisk kommunikation eller tillgången till elektronisk kommunikation, så att allvarliga händelser kan undvikas, eller konsekvenserna av dessa kan hanteras bättre. De åtgärder som genomförs ska så långt möjligt ge effekt för såväl krisberedskap som höjd beredskap.

De påfrestningar man vill kunna hantera i fredstid kan vara exempelvis natur-katastrofer, sabotage eller terrorism. Robustheten ska i fredstid primärt motverka omfattande och långvariga avbrott i de elektroniska kommunikationerna.

Åtgärder som syftar till att stärka de elektroniska kommunikationernas robusthet mot fredstida påfrestningar bidrar också oftast till skydd mot påfrestningar i höjd beredskap. Under höjd beredskap tillkommer krav på skydd från militära attacker. Mellan dessa stadier finns en gråzon, då attacker i fredstid kan ha militära syften.

Syftet med robusthetsåtgärderna är att tillförsäkra en högre nivå av säkerhet än den nivå som föreskrivs i LEK och driftssäkerhetsföreskrifterna och den som följer av användarnas ansvar att kravställa enligt kommersiella avtal.

Bedömningarna av om en robusthetsåtgärd är motiverad grundar sig på hur stor samhällsnytta den bidrar med. PTS risk- och sårbarhetsanalys för sektorn elektronisk kommunikation är ett av de underlag som ligger till grund för de åtgärder PTS låter genomföra.

De områden där myndigheten främst genomför åtgärder är:

- Fortifikatoriskt skyddade anläggningar
- Reservelförsörjning
- Redundans i nät och tjänster
- Reservnoder
- Reservmaterial
- Skydd mot naturhändelser
- Tillträdesskydd

Exempel på några av de åtgärder som har genomförts eller som pågår och som bekostas av PTS.

1. Vid långvariga och geografiskt omfattande elavbrott finns risk för störningar på mobil telekommunikation. Under 2014-2015 anskaffade PTS 100 stycken transportabla reservelverk till operatören Net4Mobility. Reservelverken är fördelade på 15 platser i landet och kompletterar operatörens befintliga stationära och transportabla reservkraftsystem.

2. Vid större avbrott eller störningar på elektronisk kommunikation kan det uppstå svårigheter för bland annat fältpersonal och nätövervakning att kommunicera, vilket försvårar återställningsarbetet. PTS har under 2015-2016 finansierat installation av antenner och terminaler för Rakel hos 15 aktörer som är medlemmar i NTSG. De flesta av dessa aktörer har terminalerna placerade på sina nätövervakningscentraler. Rakel är blåljusmyndigheternas kommunikationssystem för elektronisk kommunikation.

3. Vid brand i försörjningstunnlar finns en stor risk för störningar på elektronisk kommunikation. PTS har därför finansierat en studie för att stärka brandskyddet i nationellt viktiga försörjningstunnlar. Därefter

har PTS beslutat att finansiera omfattande åtgärder för att höja brandsäkerheten i ett antal försörjningstunnlar i storstadsområden. Finansieringen kommer att pågå i ett antal år och är en av myndighetens större insatser på området.

4. Tidigare har Sverige haft ett stort beroende av importerad tid från satelliter och utländska leverantörer (till exempel GPS). Dessa system kan påverkas av t.ex. solstormar, naturkatastrofer och störsändare. Tillgångar och förbindelser i elektronisk kommunikation är beroende av synkroniseringsinformation. PTS har bekostat utveckling samt produktion och distribution av spårbar tid och frekvens. Under perioden 2014 till 2016 har fyra produktionsnoder med två atomur vardera etablerats i Malmö, Göteborg, Stockholm och Sundsvall samt en utvecklingsnod i Stockholm. En femte produktionsnod är under uppförande i Luleå och beräknas färdigställd under 2018. Både operatörer och andra samhällsviktiga aktörer har möjlighet att ansluta sig. Åtgärderna bedöms minska beroendet av radiobaserade metoder, som exempelvis GPS. Projektet genomförs i samarbete med Netnod Internet Exchange i Sverige AB. Verifiering sker genom SP Sveriges Tekniska Forskningsinstitut.

5. Vid passage av vattendrag monteras kablar normalt på eller i brospannet. PTS finansierar förläggning av kanalisation genom borrning under vattendrag bredvid ett antal broar. Detta är för att minska konsekvenserna av ett eventuellt dammbrott uppströms en sådan passage, eller för att bron under höjd beredskap skulle kunna utgör ett militärt mål. Genom dessa åtgärder bidrar myndigheten till att kablar ska förläggas robust, istället för på det mest ekonomiskt fördelaktiga sättet i kanalisation på broarna. PTS arbetar även med att ta fram en process för generellt erbjudande gällande förläggning av kanalisation via borrning under vattendrag, så att fler aktörer inom sektorn kommer att bygga robust.

För att en robusthetsåtgärd ska kunna komma ifråga krävs ett underlag som innehåller grundläggande information så att myndigheten kan göra en initial bedömning. Sökande ska bland annat beskriva vad stödet kommer att användas till och vilka problem man förväntar sig att lösa eller förbättra, om stöd tidigare har tilldelats och i sådant fall hur uppföljning gjorts. Vidare ska sökanden beskriva hur den robusthetshöjande åtgärden skulle öka samhällsnyttan, vad som gör åtgärden lämplig, hur konkurrensen påverkas samt de uppföljningsåtgärder som kan göras för att säkerställa att robusthetssatsningen fått önskad effekt.

4.5 Närliggande arbete hos PTS

Utöver ovanstående arbetar PTS inom många områden som är nödvändiga för att elektronisk kommunikation ska fungera, till exempel frågor om nummer och adressering, om toppdomänen .se och frågor om operatörernas förmedling av nödsamtal och lokaliseringsuppgifter till samhällets alarmeringstjänst. Detta bedöms ligga utanför det aktuella uppdraget och redogörs inte närmare för i denna rapport.

5 Förslag till förändringar

5.1 Förstärkta befogenheter för PTS

Det ökade beroendet av elektronisk kommunikation medför att regleringen på området blir allt viktigare. Operatörer är vanligen vinstdrivande företag vars beslut i första hand baseras på kommersiella grunder. Regleringen måste därför vara utformad så att företagens kostnader för att efterleva lagen är lägre än deras kostnader för att inte göra det.

PTS har tidigare, i rapporten Förstärkta befogenheter för tillsynsmyndigheten på området elektronisk kommunikation[11] analyserat regleringen inom ett antal områden och identifierat vissa brister. Nedan beskrivs vissa av de förslag som lämnades i rapporten, och som har betydelse för arbetet med driftsäkerhet.

I rapporten har PTS bland annat konstaterat att krav på driftsäkerhetsåtgärder skapar kostnader för operatören och kan begränsa dennes möjligheter till vinstmaximering. Detta kan ge drivkrafter för operatörer att inte följa regleringen förrän PTS har uppmärksammat regelöverträdelsen och förelagt operatörerna att vidta rättelse.

Det finns idag ingen möjlighet för PTS att besluta om sanktioner för överträdelser i efterhand. PTS gör bedömningen att dagens befogenheter i vissa fall är otillräckliga för att uppnå målen med regleringen i LEK. PTS föreslår därför att lagstiftningen kompletteras med en möjlighet att fatta beslut om att ta ut en sanktionsavgift vid vissa överträdelser, bland annat på driftsäkerhetsområdet.

PTS har även konstaterat att myndigheten har behov av att inhämta, samordna och vidareförmedla information samt under vissa omständigheter ingripa, för att stärka samhällets tillgång till säker elektronisk kommunikation. Vidare behöver PTS kunskap om nätsäkerhetshändelser som påverkar överförda och genererade informationstillgångars tillgänglighet, konfidentialitet och riktighet för att kunna göra bedömningar av hur samhälleliga skyddsvärden påverkas.

I rapporten har PTS därför föreslagit att LEK kompletteras med en skyldighet för operatörer att lämna information som behövs för bedömning av bland annat motståndskraften vid påfrestningar, risker, sårbarheter och

[11] Förstärkta befogenheter för tillsynsmyndigheten på området elektronisk kommunikation, PTS-ER 2018:3

säkerhetsbrister, samt en skyldighet att ge in uppgifter om händelseutvecklingen, vid händelser som kan påverka säkerhet eller tillförlitlighet inom sektorn för elektronisk kommunikation.

Det är viktigt att kommersiellt motiverade åtgärder inte leder till plötsliga och kortsiktigt allvarliga konsekvenser för samhällsviktiga funktioner som är beroende av elektronisk kommunikation. Bredband kan, som nämnts tidigare, tillhandahållas genom en komplex kedja av operatörer. Hamnar en aktör i ett mellanled på obestånd kan förbindelser komma att kopplas ned, vilket kan få spridningseffekter och i förlängningen drabba samhällsviktig verksamhet.

PTS saknar idag förutsättningar att vidta åtgärder mot en operatör som inte på förhand lämnar information om problem som kan komma att påverka samhällsviktig verksamhet. PTS föreslår därför att det i LEK införs en skyldighet för operatörer att underrätta tillsynsmyndigheten vid risk för avstängning, upprätthålla berörda nät och tjänster under en viss tid samt i vissa fall underrätta slutanvändare om den förestående avstängningen.

5.2 Krav på driftsäkerhet för nät som inte omfattas av LEK

Som nämnts ovan har byalag och fiberföreningar byggt nät som utgör en viktig del av infrastrukturen för elektronisk kommunikation, särskilt på landsbygden. Många av dessa nät bedöms dock inte som allmänt tillgängliga, vilket innebär att de inte omfattas av reglerna om driftsäkerhet i LEK. De krav som ställts i samband med utdelning av bredbandsstöd har inte alltid kunnat säkerställa tillräcklig driftsäkerhet i dessa nät. Det finns alltså idag ingen reglering som möjliggör uppföljning av om det exempelvis görs riskanalyser, vidtas skyddsåtgärder eller om det finns kontinuitetsplanering för dessa nät.

Det kan finnas skäl att överväga om och på vilket sätt krav kan ställas för att även nät som idag faller utanför regleringen av driftsäkerhet i LEK ska byggas och förvaltas för att upprätthålla en rimlig driftsäkerhetsnivå. Det är dock viktigt att sådana åtgärder inte blir mer betungande än nödvändigt.

5.3 Ökade anslag för robusthetsåtgärder m.m.

PTS har vid fördelning av anslagsmedel för robusthetsåtgärder fokuserat på åtgärder som ger effekt för flera operatörer. Vidare har myndigheten i första hand genomfört åtgärder som förutom att ge en positiv effekt på förmågan att hantera kriser även förväntats ge effekter som bidrar under höjd beredskap.

PTS har hos regeringen hemställt om att regeringen ska utfärda en förordning gällande hantering av nämnda stödmedel, för att därigenom underlätta för PTS

vid bedömning, beslut och fördelning av anslagsmedel. En viss riktnings-skillnad kan noteras vad gäller bruket av medlen, då myndigheten har ett ökat fokus på åtgärder för höjd beredskap.

Anslaget för dessa åtgärder har under lång tid varit oförändrat, 100 Mkr årligen. Med anledning av det förändrade omvärldsläget bör anslaget komma att öka. En betydande del av medlen används till projekt som genomförs i privat-offentlig samverkan med operatörer. Detta är väldigt positivt och ger god effekt. Samtidigt är det utmanande, då det årliga utfallet är svårt att styra eftersom det påverkas av många faktorer. PTS tar idag in en beredskapsavgift från operatörerna för finansiering av åtgärder mot allvarliga fredstida hot och påfrestningar som gäller elektronisk kommunikation. Idag går denna avgift in i statskassan och PTS får anslag för att finansiera robusthetshöjande åtgärder. PTS önskan är att beredskapsavgiften i stället får disponeras direkt av myndigheten.