Myndigheten för samhällsskydd och beredskap

Sveriges Kommuner och Regioner

HANDBOK I KOMMUNAL KRISBEREDSKAP
3. SÄRSKILDA FUNKTIONER

Elektroniska kommunikationer

Handbok i kommunal krisberedskap – 3. Särskilda funktioner – Elektroniska kommunikationer

Det här kapitlet är en del av publikationsserien *Handbok i kommunal krisberedskap* där fler kapitel finns.

Produktion: Advant

Publikationsnummer: MSB1741 - juni 2021
ISBN: 978-91-7927-131-2

Innehåll

Övergripande beskrivning

Sverige ligger långt fram i digitaliseringen och är ett av världens mest uppkopplade länder. Elektroniska kommunikationer såsom datakommunikation och telefoni möjliggör digitaliseringen och är nödvändigt för att det moderna samhället ska fungera. Det gäller både för den enskilda individen och för företag och offentliga organisationer.

Beroendet av fungerande elektroniska kommunikationer kommer fortsatt öka i takt med förbättrad kommunikationskapacitet. Fiberutbyggnaden och 5G-tekniken gör det möjligt att skicka större datamängder och att förkorta svarstider, vilket bidrar till ökade möjligheter inom de flesta samhällssektorer. Det gäller i allra högsta grad också för kommunala verksamheter.

Elektroniska kommunikationer har en avgörande roll i krishantering och krisberedskap. Dels är de viktiga för att hantera samhällsstörningar samtidigt som störningar i elektroniska kommunikationer också kan ge upphov till samhällsstörningar.

Läs mer

Inriktning i totalförsvarsarbetet för sektorn elektronisk kommunikation 2020–2025 (pts.se)

Läsanvisningar och avgränsningar för kapitlet

Kapitlet innehåller relativt mycket bakgrundsinformation, till exempel om olika typer av elektroniska kommunikationer och hur de är uppbyggda samt vilka som tillhandahåller dem. Dessa inledande delar behöver inte läsas för att senare delar av kapitlet ska kunna förstås.

Informationssäkerhet kopplat till olika kommunikationslösningar tas inte upp här i någon större detalj, till exempel vilka lösningar som bör eller inte bör användas för att kommunicera sekretessbelagd information.

Signalskydd berörs också men i begränsad omfattning.

Marknaden för elektronisk kommunikation

Infrastrukturen och marknaden för elektronisk kommunikation har genomgått en omfattande förändring sedan avregleringen av marknaden i början på 1990-talet. Marknaden för elektronisk kommunikation kännetecknas av komplexa nät och många olika aktörer med ömsesidiga beroenden. Leverantörer av elektroniska kommunikationsnät och -tjänster (operatörer) konkurrerar sinsemellan men köper också tjänster av varandra.

Operatörerna i Sverige bedriver olika typer av verksamhet. Vissa tillhandahåller endast svartfiber (den mest grundläggande infrastrukturen), medan andra endast tillhandahåller tjänster, till exempel bredbandsaccess, traditionell fast telefoni eller ip-baserad telefoni. Det finns också operatörer som tillhandahåller hela kedjan, från den grundläggande infrastrukturen till de tjänster som konsumeras av slutkunden.

Även om det finns över 600 operatörer anmälda till PTS är det en handfull leverantörer som har över 90 procent av alla abonnenter av bredbandsanslutningar samt mobila och fasta telefonitjänster. På nationell nivå finns alltså huvuddelen av abonnenterna hos ett relativt litet antal operatörer.

Uppbyggnaden av elektroniska kommunikationer

Begreppet ”elektroniska kommunikationer” är omfattande och innefattar samtliga delar som möjliggör kommunikation genom överföring av elektroniska signaler. Det är en kedja som består av fysisk infrastruktur som överför signaler (till exempel optisk fiber, radiolänknät, trådnät eller andra fysiska medium) och tjänster och system som är nödvändiga för att den fysiska infrastrukturen ska fungera. Kedjan innefattar också de tjänster som riktar sig till slutanvändarna (alltså kunder som köper mobiltelefoni, internetaccess med mera).

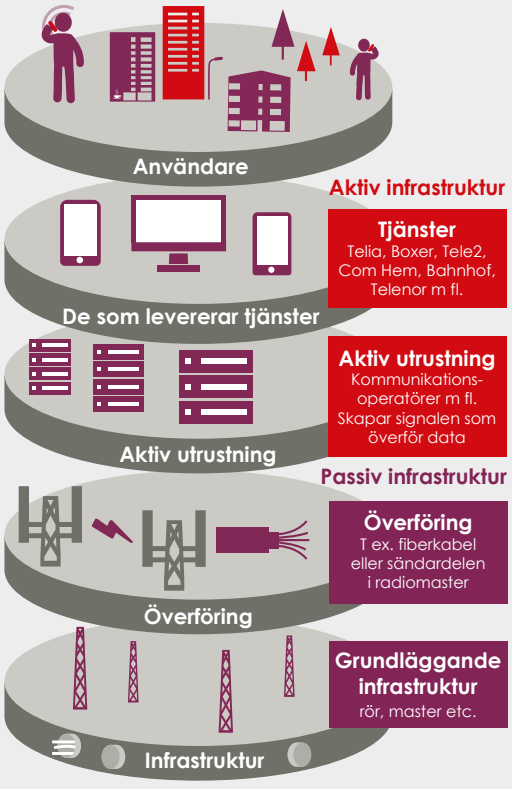
Informationen i form av elektroniska signaler överförs i både fasta nät och mobilnät. Information från avsändare till mottagare rör sig ofta både i fasta nät och i mobilnät – något som exempelvis alltid är fallet med mobiltelefoni. Störningar i det fasta nätet kan därför mycket väl påverka mobilnätet.

Fasta nät

Fasta nät består av flera olika delar och kan byggas med olika typer av teknik. Man brukar dela upp näten i tre nivåer: nationella, regionala och lokala.

- **Nationella:** Det finns flera nationella fibernät med varierande geografisk täckningsgrad. Dessa knyter samman landets olika regioner och ansluter till internationella nät. De ägs av ett fåtal stora operatörer.
- **Regionala:** Regionala nät knyter ihop nät inom en region. De ägs ofta av nationella eller regionala operatörer såsom stadsnätskluster eller medelstora operatörer.
- **Lokala:** Lokala accessnät är de som ansluter användarna till nätet. Accessnäten ägs av nationella operatörer eller lokala stadsnät och består numera oftast av fiber. Dessutom finns ett antal små föreningsägda fibernät, främst i glesbygden.

Kommunikationen i fasta nät görs i flera nivåer, se bild nedan. Den passiva infrastrukturen består av grundläggande infrastruktur, exempelvis master och kanalisation (tomrör), samt infrastruktur för överföring, exempelvis fiberkablar eller sändardelen i radiomaster. Den aktiva infrastrukturen består av aktiv utrustning, exempelvis routrar som förmedlar signaler i fibernätet, samt tjänster som levereras till användarna.



Figur 1. Schematisk bild över internetleverans i Sverige (källa: Ny IVA-rapport: Detta krävs för att öka konkurrenskraften när Sverige digitaliseras, iva.se)

Mobilnät

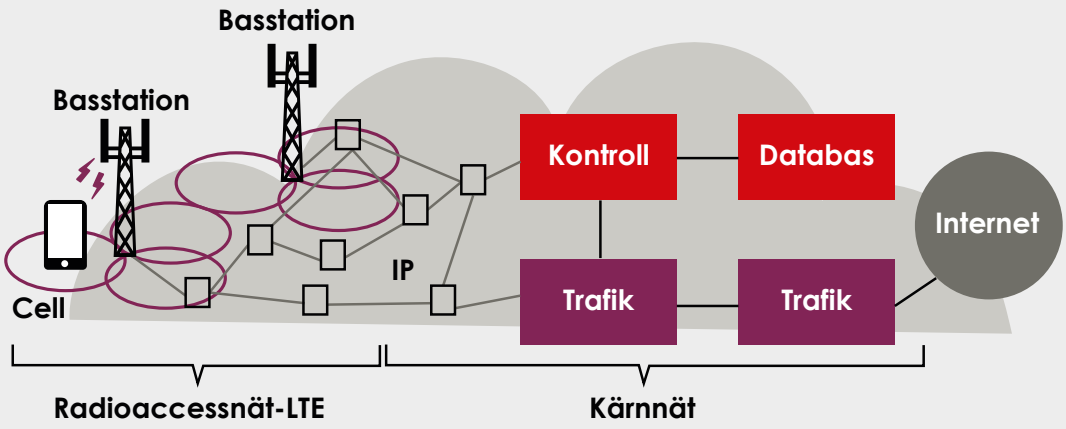
Mobilnäten består något förenklat av både en radiodel och en fast del. Radiodelen ansluter till användarnas mobilutrustning medan den fasta delen av nätet kopplar samman radiodelarna med resten av operatörens fasta nät. Ett mobilnät består alltså både av basstationer som ansluter användarnas mobilutrustning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

Det finns huvudsakligen fem operatörer som äger mobilnät i Sverige: Telia, Tele2, Telenor, Tre och Teracom. En operatör kan äga ett eget nät eller samäga ihop med andra operatörer.

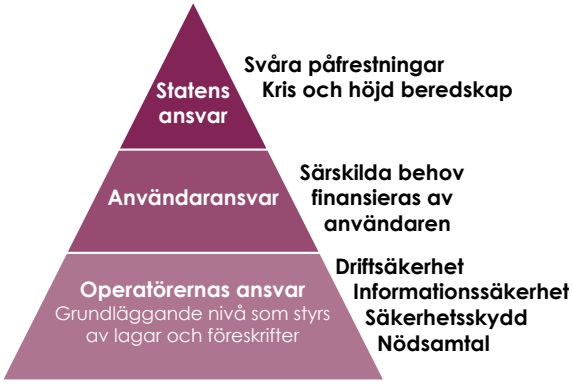
Den fasta delen av nätet kan vara helt ägd av en mobiloperatör eller bestå helt eller delvis av förbindelser som hyrs av någon annan aktör. Här kan alltså andra fastnätsoperatörer än kundens leverantör ha en viktig roll för att mobilnäten ska fungera.

IoT (Internet of Things)

Allt fler vardagsföremål, fordon, maskiner, byggnader, industriella styrsystem med mera är på olika sätt uppkopplade mot internet. IoT är ett samlingsbegrepp för dessa. Uppkopplingen sker främst genom olika typer av wifi-nät, exempelvis 2,4 GHz-bandet och 5,7 GHz-bandet som av PTS (Post- och telestyrelsen) är undantagna från tillståndsplikt. Men även genom mobilnäten eller speciella nät för just IoT, exempelvis nät som LoRaWAN och Sigfox. Framöver kommer det att bli vanligt att koppla upp saker mot internet genom 5G-nät som ger högre datahastigheter och lägre fördröjning än dagens mobiltelefoninät.



Figur 2. Mobilnätets struktur. Källa: PTS



Figur 3. Nätsäkerhetspyramiden och aktörers ansvar för robusthöjande arbete. Källa: PTS

Arbete för ökad robusthet

Elektroniska kommunikationer är nödvändiga för samhällets funktionalitet och kräver därför åtgärder för att säkerställa funktionaliteten. Detta robusthetshöjande arbete åskådliggörs i nätsäkerhetspyramiden (figur 3) som sammanfattar ansvaret för operatörerna, användarna och staten.

Operatörer har ansvar för att nät och tjänster fungerar. Post- och telestyrelsen (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 användare av kommunikationstjänster. 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.

Bättre och högre nivå av tillgänglighet kan till exempel åstadkommas genom att köpa extra säkra lösningar/högre servicenivå från operatör eller genom att köpa redundanta förbindelser från flera operatörer. Det kan också innebära att ha en alternativ kommunikationslösning. En viktig sak att tänka på är att inte använda trådlösa nät som av PTS är undantagna från tillståndsplikt för anslutningar som kräver en hög nivå av robusthet och driftsäkerhet. Detta eftersom dessa radiosystem delar samma frekvensområde med andra användningar vilka kan störa varandra.

Med statens ansvar högst upp i nätsäkerhetspyramiden ovan avses det arbete som PTS bedriver kring 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.

Exempel på statens åtgärder kan vara åtgärder som stärker reservkraftsförmågan i mobilnätet, skalskydd för viktiga noder i kommunikationsnäten och att förlägga ledningar under istället för över vattendrag. Stadsnät kan i vissa fall också ansöka om medel och finansiering för åtgärder som har samhällsnytta.

Elektroniska kommunikationer som verktyg i krisberedskapsarbetet

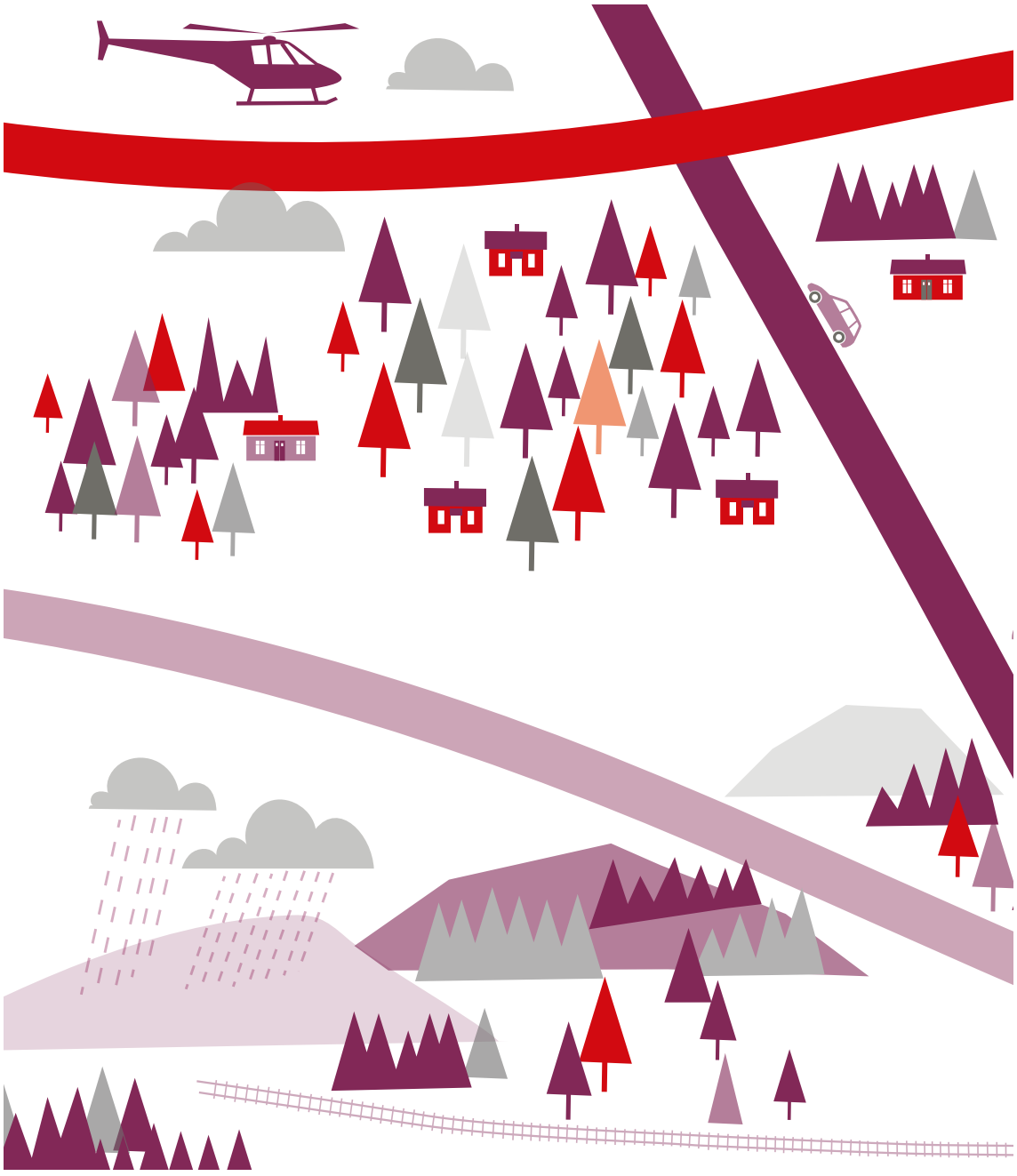
Fungerande elektroniska kommunikationer är en förutsättning för ett fungerande krisberedskapsarbete före, under och efter en samhällsstörning. Det beror bland annat på vikten av samverkan mellan aktörer. Sådan samverkan bygger i stort sett alltid på fungerande kommunikationstjänster.

Många tjänster som används i krisberedskapssammanhang går i samma kommunikationsnät som övriga aktörer i samhället också använder (till exempel mobiltelefoninät och fiberförbindelser). WIS som används för informationsdelning inom och mellan organisationer, är ett exempel på en tjänst som är beroende av fungerande internettillgång. Ett annat exempel är möjligheten att via sms skicka Viktigt meddelande till allmänheten (VMA) till telefoner inom ett visst geografiskt område.

Generellt har de allmänna elektroniska kommunikationsnäten fungerat bra under olika typer av kriser, exempelvis under corona-pandemin (pågående) och skogsbränderna (2018). Störningar och avbrott kan dock uppstå i vissa krissituationer, till exempel vid händelser som medfört elavbrott (såsom stormar och skogsbränder). Stormen Alfrida under 2019 är ett sådant exempel. I vissa situationer kan det även krävas förstärkning av nätets kapacitet under hanteringen av en samhällsstörning – något som skedde under skogsbränderna 2014.

Utöver allmänna kommunikationsnät finns helt separata kommunikationsnät som inte används av andra än aktörer inom kris- eller totalförsvarsområdet. Rakel är ett exempel. Swedish Government Secure Intranet (SGSI) är ett annat och Försvarsmakten har i sin tur egna kommunikationsnät.

Kommunen bör planera för olika typer av kommunikationsmöjligheter i sitt krisarbete – se mer om det i avsnittet Planering.



Ansvar och roller

Kommunen

Kommunens geografiska områdesansvar inkluderar även situationer med störningar i elektroniska kommunikationer. Eftersom störningar inte sällan är av regional karaktär och det kan vara utmanande att få kontakt med alla relevanta aktörer är det ofta lämpligt att vid sådana störningar kontakta länsstyrelsen.

Länsstyrelser och kommuner, som är anslutna till SOS Alarm, har också möjlighet att kontakta SOS Alarm och bli vidarekopplad till relevanta aktörer inom sektorn. Kommunernas egna leverantörer kan givetvis kontaktas enligt ordinarie rutiner.

Kommunen som användare av kommunikationstjänster

En kommuns verksamheter har ett stort beroende av elektroniska kommunikationer. I stort sett varje verksamhet är direkt eller indirekt beroende av fungerande mobiltelefonnät/telefoni samt internet. Digitaliseringen gör dessutom beroendet större.

Kommunen eller dess bolag har alltid ett ansvar för att upprätthålla och säkerställa viktiga samhällsfunktioner enligt ett antal lagar (till exempel socialtjänstlagen (2001:453), livsmedelslagen (2006:804), skollagen (2010:800), lagen (2006:412) om allmänna vattentjänster). Samma ansvar gäller även vid en samhällsstörning.

En samhällsstörning med störningar eller avbrott i elektroniska kommunikationer påverkar hela samhället, från den enskilda invånaren till samhällsviktiga verksamheter och näringsliv. För att hantera en svår situation med störningar eller avbrott i elektroniska kommunikationer bör analys och planeringsarbete bedrivas utifrån kommunens geografiska områdesansvar på lokal nivå.

Kommunen ansvarar även för att upphandla säkra och robusta kommunikationer för sin egen verksamhet där grundläggande krav inte räcker till.

Kommunen som leverantör av elektronisk kommunikation

Samtidigt är kommunen inte bara användare utan ofta också tillhandahållare av elektroniska kommunikationer – detta i form av stadsnät. I dessa fall gäller samma krav som för övriga operatörer, alltså de krav som följer av lagen om elektronisk kommunikation och tillhörande föreskrifter.

Kommuner och kommunala bolag kan också tillhandahålla kommunikationsnät för Internet of Things (IoT). IoT är ett samlingsbegrepp för saker som har en inbyggd elektronik och uppkoppling. MSB har tagit fram en vägledning om risker med IoT samt hur de kan hanteras. Även Stadsnätföreningen har tagit fram en vägledning om robust och säker IoT. Om nätet används för att erbjuda tjänster även till icke-kommunala verksamheter bör det sannolikt anmälas till PTS.

Läs mer

Generell information om IoT (iotsverige.se)

MSB:s vägledning om risker med IoT samt hur de kan hanteras.(msb.se)

Robust digital infrastruktur (ssnf.org)

Länsstyrelsen

Länsstyrelsen har ett regionalt geografiskt områdesansvar. Ansvaret omfattar det förebyggande, förberedande och hanterande arbete som sker i länet när en samhällsstörning berör eller kan beröra flera aktörer. Ansvaret handlar om att samordna länets aktörer samt att vara en länk mellan lokal och nationell nivå.

I hanteringen av en större störning av elektroniska kommunikationer aktualiseras det regionala områdesansvaret. För kommunens del kan det yttra sig i att låta länsstyrelsen ta ansvar för kontakter med centrala myndigheter, NTSG (Nationella telesamverkansgruppen) och andra relevanta aktörer. Detta för att undvika en situation där många aktörer på lokal nivå tar direktkontakter med aktörer på central nivå. Givetvis kan och bör kommunen ha kontakt med sina leverantörer.

Länsstyrelsen beslutar även om civila skyddsobjekt enligt skyddslagen (2010:305), vilket ibland är aktuellt för infrastruktur för elektronisk kommunikation.

Länsstyrelsen stödjer också kommunernas utveckling av signalskyddsorganisationer, inklusive att tillhandahålla tekniska lösningar i form av kryptodator Signe.

Post- och telestyrelsen (PTS)

PTS är en statlig myndighet som är verksam inom områdena radio, telefoni, internet och fysisk post. Myndigheten ska bland annat

- främja tillgången till säkra och effektiva elektroniska kommunikationer, inbegripet att se till att samhällsomfattande tjänster finns tillgängliga samt främja tillgång till ett brett urval av elektroniska kommunikationstjänster
- främja utbyggnaden av och följa tillgången till bredband och mobiltäckning i alla delar av landet
- svara för att möjligheterna till radiokommunikation och andra användningar av radiovågor utnyttjas effektivt
- verka för robusta elektroniska kommunikationer och minska risken för störningar, inbegripet att upphandla förstärkningsåtgärder, och verka för ökad krishanteringsförmåga
- verka för ökad nät- och informationssäkerhet förelektronisk kommunikation
- lämna råd och stöd i frågor om nätsäkerhet.

PTS är därtill en bevakningsansvarig myndighet enligt krisberedskapsförordningen och ingår i samverkansområdet Teknisk infrastruktur. Tillsammans med länsstyrelserna ska PTS också bidra till att alla i landet har tillgång till grundläggande betaltjänster (fysiska och digitala).

PTS genomför årligen flera olika åtgärder för att stärka krisberedskapen i sektorn. Många av de åtgärder som genomförs för att stärka förmågan i kris bidrar även till att stärka förmågan vid höjd beredskap. Åtgärderna genomförs ofta i privat-offentlig samverkan.

Läs mer

Förordning (2007:951) med instruktion för Post- och telestyrelsen (riksdagen.se)

Myndigheten för samhällsskydd och beredskap (MSB)

MSB ansvarar för förvaltning och utveckling av kommunikationstjänsterna Rakel, SGSI och WIS. Rakel och SGSI beskrivs översiktligt nedan. Utöver det bidrar MSB med vägledning för bland annat informationssäkerhet kring kommunikationstjänster och signalskydd. Myndigheten deltar också i samverkansområdet Teknisk infrastruktur.

Rakel

Rakel är ett digitalt radiokommunikationssystem för säker kommunikation inom samhällsviktig verksamhet. Rakel används bland annat av Polisen, räddningstjänsten, sjukvården och Försvarsmakten men också av ett stort antal andra myndigheter, energibolag och verksamheter som exempelvis hanterar farliga ämnen. Alla landets länsstyrelser, kommuner och regioner är också anslutna till Rakel.

Rakels infrastruktur är byggd för att klara svåra väderförhållanden och långa elavbrott. Rakel ska även fungera när andra system ligger nere, till exempel vid elavbrott, överbelastningar eller andra störningar i mobiltelefoni och it-system. Med tilläggstjänsten ”Rakel sekretess” finns möjlighet att kommunicera även sekretessbelagd information (dock inte säkerhetsskyddsklassificerade uppgifter).

MSB leder arbetet med att ta fram en kommunikationslösning som ska ersätta Rakel. Lösningen ska bland annat tillföra nödvändig ökad dataöverföringskapacitet och därmed göra det möjligt att skicka större mängder data, bilder och video. Den ska samtidigt uppfylla höga krav på informationssäkerhet, robusthet, skydd, tillgänglighet och statlig rådighet. Målsättningen är att den nya lösningen (vad gäller att sända mobildata i högre grad än idag) ska vara möjlig att använda hösten 2022. Den nya lösningen och dagens Rakelsystem kommer också att fungera parallellt under ett antal år.

Det finns omfattande stödmaterial som kan användas av kommuner, både skriftligt material och undervisningsfilmer.

Swedish Government Secure Intranet (SGSI)

SGSI är ett nätverk för säker kommunikation mellan organisationer i Sverige samt mellan organisationer i Sverige och i andra EU-länder. SGSI har en egen infrastruktur som är skild från internetinternet och påverkas därför inte av sådant som överbelastningsattacker. Mellan anslutna parter sker trafiken i VPN-tunnlar som krypteras med Försvarsmaktens krypto (vilket är ett signalskyddssystem). Under rätt förutsättningar kan säkerhetsskyddsklassificerade uppgifter upp till nivån begränsat hemlig hanteras.

Med SGSI kan anslutna parter få åtkomst till andra anslutna parters databaser, skicka skyddad e-post och ha skyddade videokonferenser. Det ger också möjlighet att kommunicera med EU-administrationen eller med en annan medlemsstat genom EU:s säkerhetsskyddade kommunikationsnät.

Arbete pågår med att utöka de tjänster som erbjuds centralt via SGSI. Exempel på detta är bland annat videokonferens för hemlig information samt att göra WIS tillgängligt över SGSI för att öka robustheten vid händelser som påverkar internet. En möjlig utveckling i framtiden är även en separat version av WIS som endast nås över SGSI, vilket ger möjlighet att hantera sekretessbelagd information.

I dagsläget är det framförallt myndigheter som använder SGSI. Det finns dock förslag om att utvidga användarkretsen – och bland annat kommuner nämns som möjliga användare.

För att få ansluta sig till SGSI ställs höga krav på organisationens informationssäkerhet och signalskydd (både tekniska och organisatoriska lösningar). I takt med att kommuner bygger upp signalskyddsorganisationer för att hantera kryptodator Signe kan det vara möjligt också för dessa att leva upp till krav som ställs för anslutning till SGSI.

Läs mer

WIS (msb.se)

SGSI (msb.se)

Remiss av promemorian Kommunikationstjänsten SGSI – utvidgad användarkrets och förtydligande av MSB:s uppdrag (regeringen.se)

Försvarsmakten

Försvarsmaktens telekommunikations- och informationssystemförband, FMTIS, säkerställer Försvarsmaktens förmåga att kommunicera och leda. FMTIS är Försvarsmaktens nätoperatör med ansvar för försvarets eget nät för tele- och datatrafik. Förbandet har ett samlat ansvar för Försvarsmaktens tekniska ledningssystem som stödjer militära insatser i Sverige och utomlands. Försvarsmakten har också stöttat civil krishantering med kommunikationsresurser, till exempel vid skogsbränder 2018.

Frivilliga Radioorganisationen

Frivilliga Radioorganisationen (FRO) rekryterar och utbildar personal (förstärkningsresurser) till sambands- och ledningsstödsbefattningar. FRO stödjer främst inför och vid händelser i höjd beredskap men kan även stödja akörer vid fredstida krissituationer.

FRO personal kan förstärka aktörer genom befattningarna:

- **Sambandsoperatör,** som hanterar reservsambandssystem och kan förstärka ordinarie elektroniska kommunikationer och ledningsstödsystem med inriktning på lägesinformation.
- **Sambandsspecialist,** med fördjupade kompetenser till exempel inom Rakel, HF-radio, WIS och sambandslösningar för räddningstjänst. Sambandsspecialister kan till exempel planera och utvärdera sambandssystem.
- **Sambandsledare,** leder sambandsenhet samt är regional resurs för utbildning.
- **Radiooperatör,** hanterar enklare radiosystem vid exempelvis en trygghetspunkt.

Myndigheter och kommuner kan ingå avtal med FRO och dess medlemmar. För kommuner kan FRO bland annat hålla utbildning inom sambands- och ledningsstödsystem samt utbilda personal som ska använda Rakel.

Läs mer

Frivilliga Radioorganisationen (fro.se)

Så kan du som aktör få stöd av frivilliga (msb.se)

Operatörer

Alla som avser att tillhandahålla allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster i nämnda nät måste göra en anmälan till PTS. Det finns fler än 600 operatörer anmälda.

Nationella operatörer i fasta och mobila nät

Operatörerna som tillhandahåller elektroniska kommunikationsnät- och tjänster har ansvar för att dessa fungerar. Reglerna om driftsäkerhet återfinns i lagen (2003:389) om elektronisk kommunikation med tillhörande föreskrifter. Reglerna ställer bland annat grundläggande krav på operatörernas driftsäkerhetsarbete. Det handlar om att de ska bedriva ett systematiskt driftsäkerhetsarbete samt ställer krav på reservkraft och redundans för centrala delar av näten.

Stadsnätsoperatörer

På lokal nivå spelar mindre operatörer en stor roll, främst vad gäller tillhandahållande av bredband. I många kommuner finns kommunalt ägda bredbandsnät, så kallade stadsnät. Det finns idag fler än 180 stadsnät i Sverige. Stadsnäten omfattas av reglerna som återfinns i lagen (2003:389) om elektronisk kommunikation med tillhörande föreskrifter.

Fiberföreningar och byalag

I områden som inte nås av andra nät har användare ofta gått samman i byalag och fiberföreningar och 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 därför inte av kraven i LEK. Vissa krav på robusthet och dokumentation ställs dock i samband med tilldelning av eventuellt bredbandsstöd.

Samverkansgrupper

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

Nationella telesamverkansgruppen

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

I gruppen ingår de stora nationella nätägarna. Deltagare är Hi3G (3), Global Connect, Netnod, Skanova, Stokab, Svenska kraftnät, Svenska Stadsnätsföreningen, Tele2, Telenor, Telia Company, Teracom, Trafikverket, Försvarsmakten FMTIS, MSB Rakel och PTS (ordförande). Samverkan sker efter behov också med andra aktörer.

Gruppen arbetar med att förebygga, förbereda och hantera störningar. I det förebyggande och föreberedande arbetet handlar det bland annat om

- diskussioner om sektorns verksamhet för att kunna hantera störningar och kriser
- analyser och utvärderingar av allvarliga störningar
- att genomföra utbildningar/övningar i krishantering
- att verka för att skapa nätverk och utbyta information, nationellt och internationellt.

Under en samhällsstörning eller större störning startas gruppens arbete på begäran av en medlemsorganisation. Vid händelser sammanställer gruppen skadeläget och rapporterar det till berörda parter samt kan ge förslag till åtgärder. Gruppen kan också koordinera och hjälpas åt med insatser. Till exempel vid långvariga elavbrott vid stormar då operatörer kan hjälpas åt att tanka varandras reservkraftverk.

Läs mer

Nationella telesamverkansgruppen (pts.se)

Stadsnätens infrastruktur-samverkansgrupp

Stadsnätens infrastruktursamverkansgrupp, SiSG, är ett forum för samverkan och utbildning inom säkerhetsområdet. SiSG håller genom Svenska Stadsnätsföreningen en kontinuerlig dialog med NTSG. SiSG säkerställer att rätt och relevant information förmedlas om stadsnätens driftläge under både normalläge och kris och har ansvar för att förmedla relevant information från NTSG till medverkande stadsnät.

Branschorganisationer

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

IT&Telekomföretagen

IT&Telekomföretagen är den bransch- och arbetsgivarorganisation som organiserar många av operatörerna. De har cirka 1 300 medlemsföretag. Deras huvudfokus är att tydliggöra nyttan av it och telekom, stödja användningen i samhället samt förenkla för medlemmarna och stimulera tillväxt i branschen. It- och telekomföretagen har en samverkansgrupp för beslutsfattare inom branschen, Telekområdet.

Svenska Stadsnätsföreningen

Svenska Stadsnätsföreningen är en oberoende bransch- och intresseorganisation som organiserar cirka 150 stadsnät och drygt 100 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. Svenska Stadsnätsföreningen är aktiv i flera forum, bland annat Bredbandsforum, Nationella Telesamverkansgruppen, Stadsnätens infrastruktursamverkansgrupp (SiSG) och Telekområdet. Föreningen stöttar också stadsnäten i regional och länsvis dialog i frågor om bredbandsinfrastruktur och digitalisering.

Föreningen verkar för robusthet inom den digitala infrastrukturen. Ett exempel är föreningens medverkan i projektet Robust fiber (se avsnitt om det nedan). Projektet kan bidra till att stärka robusthetsarbetet hos kommunens stadsnätsaktör.

Svenska Stadsnätsföreningen bedriver också annat säkerhets- och robusthetsarbete. Bland annat finns vägledningen ”Robust och säker IoT”. Den kan användas för att öka säkerheten när kommunala verksamheter använder IoT inom till exempel kommunalteknisk infrastruktur, fastighetsautomation, välfärdsteknik med mera.

Läs mer

Robust fiber (robustfiber.se)

Robust digital infrastruktur (ssnf.org)

Förstärkningsresurs samverkan och ledning

MSB erbjuder förstärkningsresurser inom området samverkan och ledning. Det övergripande syftet är att stärka mottagande organisations ledningsförmåga. En del av det stöd som kan ges är för att säkerställa fungerande samband för berörda aktörer. I stödet ingår hjälp med sambandsplanering, kompetens och nätförstärkning i Rakelnätet samt Rakelterminaler. Vid behov av förstärkningsresurser kontaktar räddningsledaren eller länsstyrelsen MSB:s tjänsteman i beredskap.

Läs mer

MSB:s förstärkningsresurs för stöd till Samverkan och ledning (FSOL) (msb.se)

Stöd till samverkan och ledning (FSOL), delresurs Samband – MSB:s förstärkningsresurs (msb.se)

Mobila basstationer

I vissa situationer räcker inte kapaciteten i mobilnätet. Därför finns transportabla mobilbasstationer som kan användas i både förebyggande syfte, till exempel när mycket trafik förväntas vid stora event eller för att korta avbrottstiden vid en större samhällsstörning. PTS har tillsammans med operatörerna införskaffat ett antal transportabla mobilbasstationer. Operatörerna ansvarar för att de mobila basstationerna utnyttjas på bästa sätt. Det är operatören själv som avgör om och när de mobila basstationerna ska nyttjas.

Det är viktigt att arrangörer av olika tillställningar i god tid informerar operatörerna om kommande evenemang (till exempel stadsfestivaler, stora idrottsevenemang och liknande). Det ger operatörerna möjlighet att tillfälligt dimensionera sina nät efter det förväntade behovet.

Detta kan också vara bra att känna till för räddningsledare. Vid händelser när kapaciteten och/eller täckningen i mobilnäten inte räcker till för en räddningsinsats kan operatörerna kontaktas om behovet beräknas kvarstå under en längre tid. Den naturliga kontaktvägen är då via aktuell länsstyrelse.

Läs mer

Mobila basstationer (pts.se)

Krisroaming

PTS har förberett så att det finns ett antal sim-kort med roamingfunktion – de kan alltså använda flera olika operatörers nät. De är avsedda att användas i krissituationer som innebär eller kan innebära risk för allvarliga störningar i elektroniska kommunikationsnät- eller tjänster. Avsikten är dock inte att denna typ av roaming ska ersätta de möjligheter som finns att upphandla driftsäkra kommunikationer.

Det är länsstyrelserna som begär att få tillgång till dessa sim-kort och PTS som fattar beslut.

Läs mer

Krisroaming (pts.se)

Lagstiftning

Lagen om elektronisk kommunikation

Lagen om elektronisk kommunikation trädde i kraft år 2003. I lagen omfattar begreppet elektronisk kommunikation alla typer av elektroniska kommunikationsnät som telenätet, internet och kabel-tv-nätet. Enligt lagen ska den som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att verksamheten uppfyller rimliga krav på driftsäkerhet. De åtgärder som vidtas ska vara ägnade att skapa en säkerhetsnivå som, med beaktande av tillgänglig teknik och kostnaderna för att genomföra åtgärderna, är anpassad till risken för störningar och avbrott.

Det pågår arbete med en ny lag som ersätter den befintliga. Den nya lagen genomför EU:s direktiv om inrättande av en kodex för elektronisk kommunikation och förväntas träda i kraft 2021.

Post- och telestyrelsens föreskrifter om krav på driftsäkerhet

Syftet med föreskrifterna (PTSFS 2015:2 med ändringar enligt PTSFS 2020:1) är främst att förtydliga vilka tekniska och organisatoriska åtgärder som tillhandahållare ska vidta för att säkerställa en rimlig nivå av driftsäkerhet vid tillhandahållande av allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster. Det handlar bland annat om krav på riskhantering, planering för att hantera störningar samt krav på reservkraft och andra redundanslösningar med mera.

Föreskrifterna kommer att uppdateras bland annat som en följd av den nya lagen som nämns ovan.

Planering

Det finns ett antal saker en kommun bör göra inom det förberedande och förebyggande krisberedskapsarbetet. Planeringen behöver uppmärksamma både hur samhällsviktig verksamhet upprätthålls på en acceptabel nivå vid avbrott men också hur kommunens krishanteringsförmåga upprätthålls i sådana situationer. Det finns också åtgärder som kan minska sannolikheten för störningar samt minska konsekvenser vid störningar i en kommunikationstjänst.

Några centrala områden att uppmärksamma i kommuners planering beskrivs nedan.

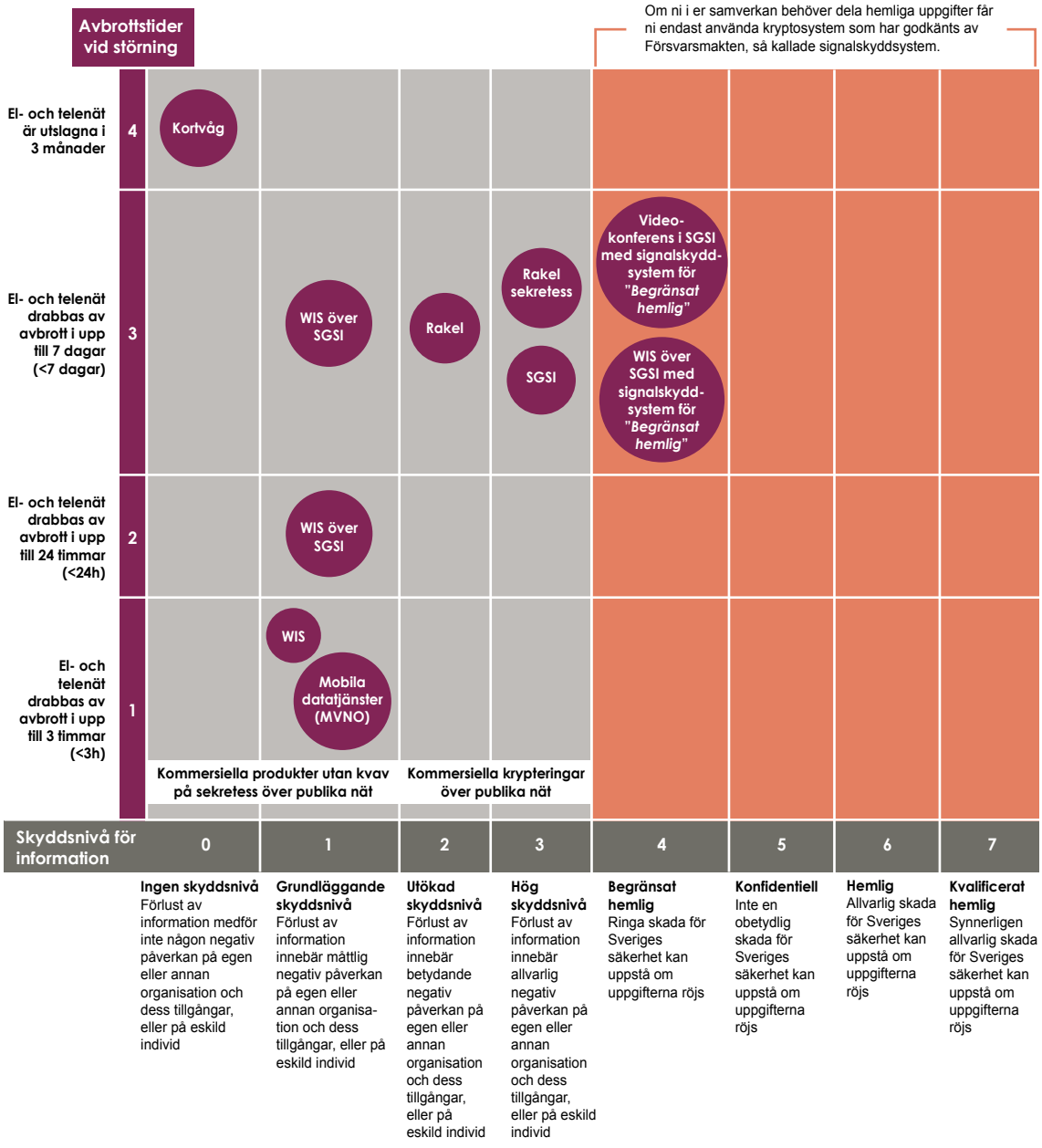
Sambandsplanering för krisledning

Samverkan inom och mellan organisationer behöver ofta ske på distans genom elektronisk kommunikation. För en kommun är det därför viktigt att ställa sig frågor som vilka de kommer behöva kommunicera med, om vad, vid vilka tillfällen samt från vilka platser. För praktisk vägledning i hur en analys av lednings- och sambandsbehov kan göras, se MSB:s ”så gör du en lednings- och sambandsanalys för rakel”. Materialet är skrivet framförallt utifrån ett Rakelperspektiv men kan användas även för mer generell sambandsanalys.

Det är viktigt att också analysera vilka kommunikationsmetoder som är lämpliga för olika typer av samverkan och typ av information. Det handlar till stor del om att bedöma hur viktigt det är att kommunikationen kan upprätthållas utan avbrott (robusthet/tillgänglighet), hur viktigt det är att informationen inte når obehöriga (konfidentialitet) samt hur viktigt det är att informationen inte förvanskas (riktighet).

I MSB:s ”Vägledning för säker och robust samverkan” finns råd om hur man går tillväga med analysen. Där ges också förslag på olika kommunikationslösningar som kan användas beroende på kraven på robusthet och konfidentialitet. Vägledningen innehåller dock bara kommunikationstjänster som tillhandahålls av MSB. En analys över lämpliga sätt att kommunicera behöver inkludera även andra kommunikationstjänster, till exempel mobiltelefoni. Rådgör gärna med kommunens ansvariga för säkerhetsskydd och informationssäkerhet.

Matrisen (figur 4) nedan visar hur olika verktyg förhåller sig till varandra utifrån aspekterna robusthet och sekretess.



Figur 4. Matris med verktyg för säker och robust samverkan källa: Vägledning för säker och robust samverkan, MSB.

I krisberedskapsarbetet är det också lämpligt att gemensamt med andra aktörer planera för att arbeta tillsammans i situationer när elektroniska kommunikationer är störda. Hur ska samverkan och samordning uppnås vid samhällsstörningar under störda förhållanden för både aktörer inom och utanför kommunen. I denna planering ingår även att analysera hur en inriktnings- och samordningsfunktion (ISF) påverkas av samt kan upprätthållas på adekvat nivå.

Läs mer

Lednings- och sambandsanalys (msb.se)

Vägledning för säker och robust samverkan (msb.se)

Kriskommunikation under kommunikationsstörningar

När kommunikationstjänster som vanligtvis används i kriskommunikationsarbete är störda uppstår särskilda utmaningar. Kommunen och andra organisationer kan då behöva ta till andra metoder än att kommunicera via kanaler som hemsida, sociala medier och sms.

Läs mer

När de ordinarie kanalerna inte fungerar eller räcker till Kriskommunikation under svåra förhållanden – en vägledning (lansstyrelsen.se)

Kommunens behov av och avtal kring robusta kommunikationer

Många verksamheter i en kommun har höga krav på fungerande elektroniska kommunikationer. Det gäller både organisationsövergripande tjänster och verksamhetsspecifika. Exempel på det förstnämnda är telefoni och internet. Verksamheter som bedriver samhällsviktig verksamhet är ofta beroende av fungerande elektroniska kommunikationer, från välfärdsteknik i vård och omsorg till styrning och övervakning i kommunalteknisk infrastruktur.

När det finns ett förhöjt robusthetsbehov kan olika strategier väljas/kombineras. Ett par exempel är att använda:

- olika leverantörer inom samma kommunikationstjänst. Till exempel använda flera olika mobiltelefonioperatörer eller flera olika internetleverantörer
- olika kommunikationstjänster. Till exempel att vid databaserade tjänster använda kommunikationstjänster via både mobiltelefoninät och fiber. Det kan vara en lösning vid styr- och kontrollsystem inom kommunalteknisk infrastruktur.

Oavsett vilka strategier som väljs är det viktigt att ta hänsyn till att olika operatörer/leverantörer kan vara beroende av samma infrastruktur. Ett misstag kan vara att välja två telefonileverantörer som använder samma nät/infrastruktur och som skulle kunna drabbas av avbrott på grund av ett gemensamt fel. Därför är det viktigt att säkerställa att det verkligen blir en redundant lösning som köps. Likaså är det viktigt att kontrollera att redundansen upprätthålls över tid eftersom det sker förändringar i operatörernas användning av olika nät.

Läs mer

Den robusta sjukhusbyggnaden (msb.se)

Se kap. 18. It, telefoni och Rakel för stöd vid kravställning mot leverantörer av it, telefoni och Rakel. De grundläggande tankegångarna går att använda på ett generellt plan även om rapporten handlar om sjukhus.

Förstärkt inomhustäckning

Täckning inomhus har blivit allt viktigare för både telefoni och datatrafik. Samtidigt är det vanligt med bristande täckning från mobilnäten inne i byggnader. Det finns dock flera saker som kommunen kan göra för att stärka detta.

Läs mer

Inomhustäckning (pts.se)

Kontinuitetshantering som stärker kommunikationsförmåga

I kommunernas kontinuitetshantering för både kommunövergripande processer (till exempel krisledning) och för verksamheternas processer bör det finnas planering för störningar i elektroniska kommunikationer.

Läs mer

Kontinuitetshantering (msb.se)

Vägledning för kontinuitetshantering, SS 22304:2014, tillgängliggörs kostnadsfritt (sis.se)

Statligt stöd stärker kommunal ledningsförmåga

MSB stödjer åtgärder som stärker ledningsförmågan i kommunen och räddningstjänsten. Stöd ges genom teknisk rådgivning och ekonomiska bidrag till tekniska åtgärder som kan vidtas för att stärka ledningsförmågan och säkerställa robusta ledningsfunktioner.

Det inkluderar bland annat:

- robusthetshöjande åtgärder för data- och telekommunikationssystem som är viktiga vid samhällsstörningar. Exempel på åtgärder är utomhusantenn för Rakel, stationärt reservelverk för kommunledning, inklusive server-/telerum, viktig tekniknod eller liknande
- avbrottsfri strömförsörjning
- redundans för telefoni/data eller andra säkerhetshöjande åtgärder inom kommunikationsområdet
- automatisk släckutrustning, skalskydd, brandklassning, larm och inpasseringsskydd till server-/telerum
- övriga åtgärder som kan anses vara av vikt som stärker den lokala ledningsförmågan i kommunen och som inte bedöms som ett baskrav för den normala driften.

Läs mer

Kommunens ledningsplats (msb.se)

Information om störningar i elektroniska kommunikationer

Det bör finnas etablerade och testade rutiner för hur kommunens leverantörer av kommunikationstjänster informerar vid både planerade och oplanerade störningar. Samtidigt finns det behov av att kunna uppmärksamma störningar som drabbar andra leverantörer än de kommunen använder. SOS Alarm driver webbtjänst SOS.nu som bland annat visar pågående störningar i telefoni. Kommuner får använda tjänsten gratis efter att ha tecknat avtal.

Läs mer

SOS.nu (sosalarm.se)

Undvik infrastrukturskador vid grävningsarbeten

En av de vanligaste orsakerna till störningar och avbrott i elektroniska kommunikationstjänster är att kablar skadas i samband med grävningsarbeten. För att minska risken för det finns tjänsten 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 behöver veta var dessa finns. Den som planerar något slags markarbete begär då ledningsanvisning/kabelanvisning av den som äger ledningar i området, för att minska risken för att ledningar grävs av. Tjänsten bidrar till att skydda flera viktiga samhällsfunktioner, som el, tele och vatten, genom att minska risken för skador på infrastrukturen. Tjänsten kan med fördel användas av såväl kommuner som entreprenörer, både operativt (inför grävningar) och strategiskt (vid projektering och samhällsplanering).

Läs mer

Webbtjänst som skyddar och underlättar, (ledningskollen.se)

Bygg robusta fibernät

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

Den funktion i kommunen som arbetar med krisberedskap kan med fördel kontakta både stadsnätsoperatören och eventuella fiberföreningar och höra efter hur de arbetar med robusthet.

Läs mer

Robust fiber (robustfiber.se)

Uppmärksamma att kopparnätet avvecklas

Det gamla kopparnätet för telefoni avvecklas stegvis av dess ägare Telia. Kommuner bör se över vilka verksamheter som eventuellt berörs av det.

Läs mer

Avvecklingen av kopparnätet (telefonnätet) (pts.se)

Risker och sårbarheter

PTS tar fram risk- och sårbarhetsanalyser för sektorn. Analyserna identifierar och värderar de hot som kan få nationella konsekvenser. I analysen ingår inte kommunikationsnät- och tjänster som hanteras av MSB och försvarsmakten.

Det konstateras att bränder i vissa försörjningstunnlar, långvariga nationella elavbrott och tillgänglighetsattacker är de tre största riskerna. Fel och brister i hantering, programvara och hårdvara samt avbrott i förbindelser kan fortfarande leda till allvarliga avbrott men risken för dessa bedöms vara låg. Gemensamt för de flesta riskerna är att konsekvensen blir tillgänglighetsstörningar i en eller flera kommunikationstjänster.

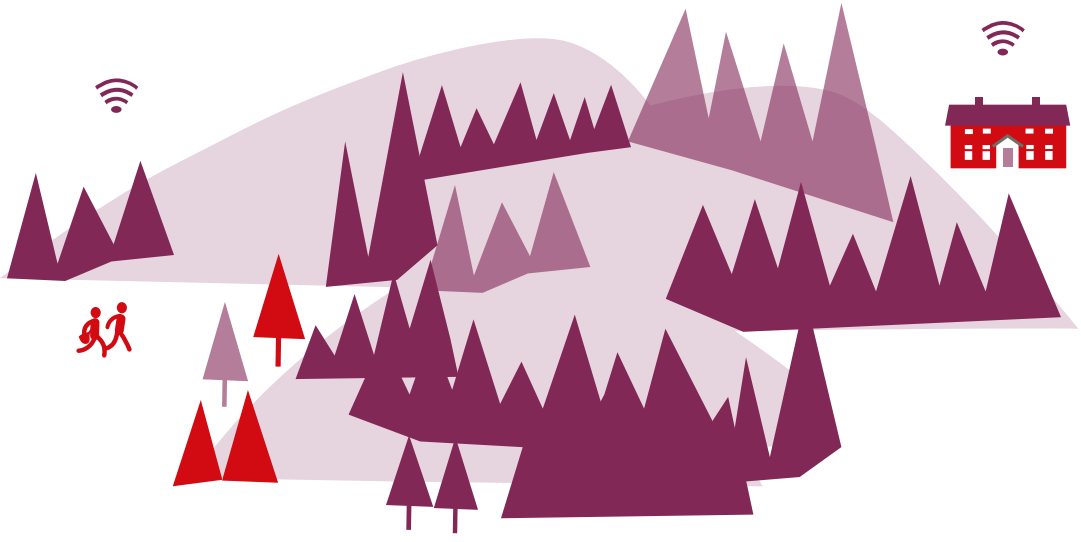
På regional nivå är det vanligt att störningar i elektronisk kommunikation uppmärksammas som en av de allvarligare riskerna i risk- och sårbarhetsanalyser.

Ur ett lokalt perspektiv kan konsekvenserna bli stora också vid incidenter som inte har en nationell konsekvens (till exempel lokala eller regionala störningar i elförsörjning, telefoni eller internetjänster). Det torde därför vara vanligt att elektroniska kommunikationer uppmärksammas i den kommunala risk- och sårbarhetsanalysen.

Läs mer

Risk- och sårbarhetsanalys för PTS och dess verksamhetsområden 2018 – PTS-ER-2018-23 (pts.se)

Risk- och sårbarhetsanalys för PTS och dess ansvarsområden 2020 – PTS-ER-2020:32 (pts.se)



Risker som identifierats av PTS

Nedan ges exempel på några olika risker som PTS lyft fram i risk- och sårbarhetsanalys från 2018.

Elavbrott

Nätinfrastrukturen för kommunikationstjänster är beroende av el. Vid elavbrott finns viss reservkraftsförmåga, både fast och mobil, som kan upprätthålla funktionaliteten i nätet. Men uthålligheten handlar om timmar och inte dagar (förutsatt att bränsle inte fylls på). Rakel har dock en uthållighet på flera dagar vid strömavbrott.

Vid ett omfattande och långvarigt elavbrott på nationell nivå räknar PTS med att det kommer uppstå störningar på nationell nivå inom elektronisk kommunikation. Sannolikheten för nationell påverkan bedöms dock som låg. I sammanhanget är det viktigt att uppmärksamma att Rakel har en uthållighet på flera dagar vid elavbrott. Regionala och lokala elavbrott kan medföra att en eller flera kommuner drabbas av kommunikationsproblem. Stormen Alfrida (2019) är ett exempel på när elavbrott skapade störningar i eletroniska kommunikationer.

Läs mer

Stormarna Alfrida och Jan: utredning och sammanställning av några viktiga erfarenheter (msb.se)

Avbrott som orsakas av fel och brister i hantering, programvara eller hårdvara

Elektronisk kommunikation bygger på komplexa tekniska system där mänsklig hantering, programvara och hårdvara samverkar. Inom alla dessa områden kan det inträffa fel som leder till avbrott. Att denna typ av problem ska leda till störningar på nationell nivå bedömer PTS dock som mindre sannolikt.

På lokal och regional nivå kan störningar i tillgång till internet och telefoni orsakade av hantering, programvara eller hårdvara både leda till och försvåra hanteringen av samhällsstörningar.

Överbelastningsattack

Det finns sätt för antagonister att störa eller avbryta elektroniska kommunikationer utan att behöva göra det fysiskt. Ett exempel på en större överbelastningsattack (mirai-botnätet) drabbade hösten 2016 ett företag som ansvarar för delar av internetinfrastrukturen. Det ledde till att många stora internettjänster inte var tillgängliga.

Denna typ av attacker kan också ske på lokal nivå. Ett exempel på det är när Skellefteå Krafts stadsnät utsattes för en överbelastningsattack våren 2020, vilket ledde till störningar i kundernas internettillgång.

Läs mer

DDoS attack that disrupted internet was largest of its kind in history, experts say (theguardian.com)

Skellefteå krafts stadsnät utsatt för ”attack” – fler kan vara drabbade (sverigesradio.se

Se även

IT

Bristande konfidentialitet

En risk är att innehållet i kommunikation sprids till obehöriga. Det kan orsakas både av medvetna angrepp eller omedvetna fel. Hotet kan komma utifrån eller inifrån den egna organisationen.

Att hantera denna typ av risk kan exempelvis göras genom att använda rätt verktyg för känslig information, att kravställa rätt säkerhetsnivå på köpta kommunikationstjänster för informationens skyddsvärde samt att ha ett väl fungerande internt informationssäkerhetsarbete.

Riskerna ur ett kommunalt perspektiv

Störningar i elektroniska kommunikationer kan påverka exempelvis larmfunktioner såsom trygghetslarm och automatiska brandlarm, innebära problem att nå 112, göra det svårt att få ut krisinformation/kommunikation samt ge upphov till problem för kommunalteknisk infrastruktur. Särskilt utmanande kan situationen bli om störningarna inträffar parallellt med en annan samhällsstörning, till exempel ett långvarigt elavbrott som kan vara föranlett av en storm eller en översvämning.

Hantering av risker

Generellt sett kan risker hanteras på olika sätt. De kan undvikas genom att inte ägna sig åt den aktivitet som ger upphov till risken. Men eftersom stora delar av den kommunala verksamheten enligt författning ska bedrivas är det inte en möjlig hantering. Risker kan också mildras genom att minska riskens sannolikhet eller konsekvens – något som är desto vanligare.

När kommunen är användare av en kommunikationstjänst är det svårt att påverka sannolikheten för att en störning inträffar eftersom kommunen inte har någon roll i driften. Det ansvaret ligger på leverantören. Däremot kan kommunen vidta åtgärder som minskar sannolikheten att en störning hos en leverantör drabbar kommunen negativt (utöver att ställa krav på sin tjänsteleverantör). Sådana åtgärder kan vara att ha redundanta fiberförbindelser för internettillgång och att ha roaming-sim-kort (krisroaming) från olika mobiloperatörer i verksamhetskritiska mobiltelefoni-/mobildatalösningar. Den typen av redundanslösningar kan göra att en störning i en kommunikationstjänst inte får negativ påverkan.

Konsekvensdämpande åtgärder behöver också vidtas. Det handlar då om sådant som mildrar konsekvenserna av störningar i en kommunikationstjänst. Exempelvis avbrott hos kommunens telefonleverantör eller om internetförbindelsen går ner. Detta är något som bör hanteras inom ramen för kontinuitetshantering- och planering.

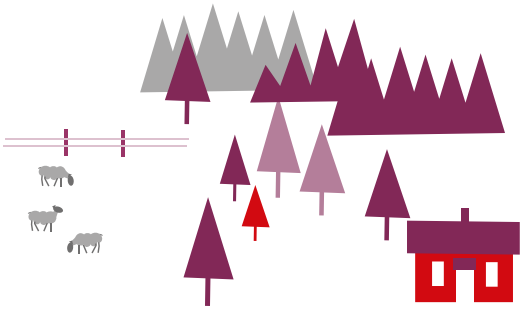
Som tidigare beskrivits är kommuner och/eller kommunala bolag leverantörer av kommunikationstjänster. Det ställer krav på en annan typ av riskhantering, bland annat enligt de krav som ställs upp av lagen om elektroniska kommunikationer och PTS föreskrifter (PTSFS 2015:2 med ändringar enligt PTSFS 2020:1).

Läs mer

Riskhantering - Vägledning (ISO 31000:2018, IDT), (sis.se)

Upphandling till samhällsviktig verksamhet: en vägledning, (msb.se)

Robust elektronisk kommunikation – vägledning för användare vid anskaffning (pts.se)



Utbildning och övning

Utbildningsverksamhet

För kommuner finns möjlighet att få utbildning i de särskilda kommunikationstjänster som används i krisberedskapsarbete. MSB har samlat utbildnings- och informationsmaterial om Rakel på sin hemsida. MSB erbjuder också utbildning i WIS samt generellt kring övningar. Också länsstyrelserna erbjuder ofta utbildningar i både Rakel och WIS.

PTS arbetar med utbildningar för sektorns aktörer (till exempel stadsnät) som ska stärka förmågan att hantera större kriser, extraordinära händelser och höjd beredskap. Utbildningarna ska bidra till att aktörerna inom sektorn ska kunna hantera kriser med så små konsekvenser som möjligt för samhället. Under perioden 2017–2021 ligger fokus på sektorns roll i totalförsvaret.

För stadsnät finns olika alternativ. Stadsnätsföreningen har anordnat utbildningar inom driftsäkerhetsområdet åt sina medlemmar. Sådana utbildningar kan anordnas även framöver. Det finns också krishanteringsutbildningar som arrangeras av Energiföretagen (delvis finansierade av PTS). Utbildningarna är gjorda för organisationer inom energiområdet samt elektroniska kommunikationer.

Läs mer

Utbildning, riktlinjer och rekommendationer (om Rakel msb.se)

WIS – grundutbildning, (msb.se)

Signalskydd – en introduktion (webbkurs), (msb.se)

Vad är signalskydd? (informationssakerhet.se)

Utbildnings- och övningsstrategi för krisberedskap 2017-2021, (pts.se)

Utbildning, (ssnf.org)

Övningsverksamhet

Övningar som arrangeras av andra än kommunen

PTS genomför regelbundet en övning med sektorn elektroniska kommunikationer. Telö 19 och Telö 17 var båda inriktade på att öva hur sektorn kan stödja totalförsvaret under höjd beredskap. Kommande Telö-övning planeras genomföras 2022.

Förmåga att använda kommunikationstjänster för samverkan inom krisberedskapsarbetet övas bland annat genom länsstyrelsers regelbundna övningar i att hantera Rakel och WIS. I dessa inkluderas ofta kommuner. Förutom regionala övningar är det viktigt att uppmärksamma samverkansövningar på nationell nivå, där kommunen kan ha anledning att delta. I nationella samverkansövningar som SAMÖ och TFÖ (Totalförsvarsövning) används oftast kommunikationstjänster för samverkan mellan olika aktörer.

Stadsnätens infrastruktursamverkansgrupp genomför övningar för stadsnätsoperatörer. Utöver att kommunala stadsnät deltar kan övningarna merutnyttjas, exempelvis genom att återanvända scenarier för kommunala övningar eller att parallellt med SiSG:s övningar öva krisledning på central nivå i kommunen.

Under 2020 arrangerade SiSG tillsammans med PTS tre övningar med stadsnät under paraplynamnet Telö 2020 Stadsnät. Tre sambandstest genomfördes under året för att testa och utvärdera ett arbetssätt för att rapportera lägesinformation. Lägesinformationen skickas, sammanställs områdesvis och rapporteras till en säkerhetsstab hos SiSG. Staben hos SiSG sammanställer en lägesbild för samtliga deltagande stadsnät, vilken utgör den lägesrapportering som görs till NTSG.

Läs mer

Utbildningar och övningar för stärkt krisberedskap, (pts.se)

Utvärderingsrapport Telö 19, (pts.se)

Utbildningar och konferenser, (energiforetagen.se)

Övningar som kan arrangeras av kommunen

För en kommun kan följande typ av övningar vara relevanta:

- Funktionsövning för krisledningsfunktion med fokus på att öva alternativa sätt att kommunicera. För att förbättra förmåga att hantera situationer när allmänna kommunikationstjänster inte är tillgängliga. Kan med fördel inkludera andra organisationer än den egna kommunen.
- Övning av kontinuitetsplaner i olika kommunala verksamheter. Exempelvis att öva bortfall av mobiltelefoni, vilket skulle kunna leda till avbrott i trygghetslarm och annan välfärdsteknik eller i styr- och kontrollsystem för kommunalteknisk infrastruktur.

Ett samarbete mellan:

Myndigheten för samhällsskydd och beredskap

Sveriges Kommuner och Regioner

651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publ.nr MSB1741 - juni 2021 978-91-7927-131-2