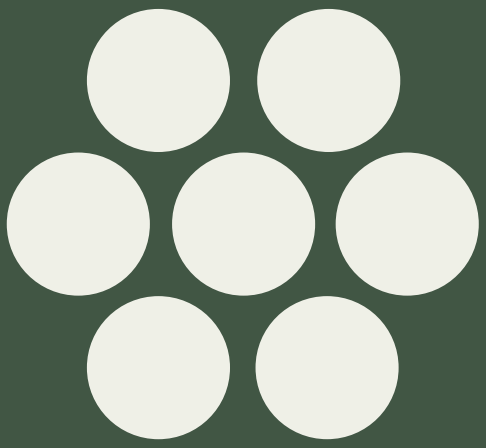
Anläggningar med förhöjd säkerhet och funktion

Huvuddokument

Version 1.2.2



Anläggningar med förhöjd säkerhet

Innehåll

1 Inledning

För anläggandet av elektroniska kommunikationsnät har berörda organisationer med stöd av PTS arbetat fram anvisningar och vägledningar i syfte att säkerställa en bassäkerhet i anläggningarna. Utöver bassäkerheten har denna kompletterande anvisning för Anläggningar med förhöjd säkerhet och funktion tagits fram. Aktuella anvisningar och vägledningar framgår av nedanstående bild.

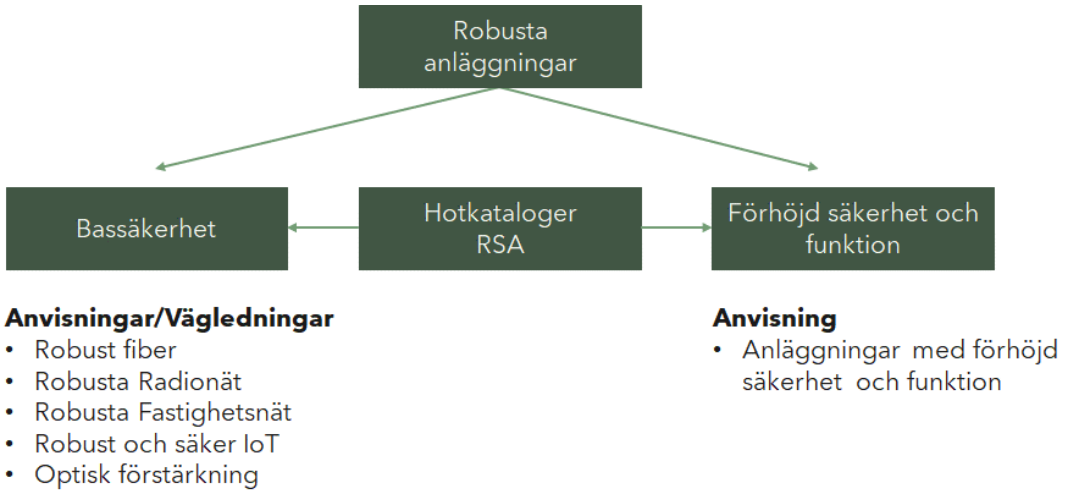


Bild. Robust digital infrastruktur

Detta dokument riktar sig till nätägare som tillhandahåller en fiberbaserad infrastruktur inom sektorn elektronisk kommunikation och utgör referensramar för nätägarens utveckling av nätinfrastruktur för kunder som har krav på förhöjd och/eller hög säkerhet.

2 Bakgrund

Sveriges *Nationella säkerhetsstrategi* anger att tillgången till en digital infrastruktur är av nationellt intresse. I takt med att den digitala infrastrukturen hanterar allt större mängder information, vilken i allt större utsträckning är kritisk för samhällets funktion, krävs en kontinuerlig och planerad anpassning av säkerheten i denna infrastruktur. Anpassning gäller både den fysiska och funktionella säkerheten i den nationella- regionala- och lokala infrastrukturen.

Genom lagar, förordningar och föreskrifter utfärdar våra myndigheter övergripande krav på hanteringen av den fysiska och funktionella säkerheten i den digitala infrastrukturen och på dess ägare. Dessa krav ska tillsammans skapa förutsättningar för en gemensam och säker hantering av den grundläggande digitala infrastrukturen.

Utöver dessa övergripande krav på hanteringen av den digitala infrastrukturen krävs också en kontinuerlig fysisk och funktionell anpassning till ny teknik och förändrade kundkrav.

De förändringar som skapar behov av förstärkningar i den digitala infrastrukturen och på utveckling av tjänster utgörs främst av:

- den förändrade yttre hotbilden mot Sverige ställer krav på förstärkningsåtgärder i våra teleanläggningar,
- användningen av molntjänster ökar på grund av kostnadseffektivitet, tillgänglighet och smarta backuplösningar,
- utbyggnaden och förtätningen av 5G ökar på grund av eskalerande driftkostnader på befintlig mobil infrastruktur och säkerhetskrav på mobila tjänster,
- den snabba utvecklingen av digitala system för styrning och övervakning av distribuerade anläggningar, smarta samhällen och viktiga samhällssystem (t.ex. elnäten) kräver hög säkerhet i den passiva infrastrukturen,
- arbetsplatsen är utflyttad till hemmet vilket innebär utökade krav motsvarande de krav som gäller för kontoret.

Ansvaret för hur de tekniska och funktionella lösningarna för den digitala infrastrukturen ska utformas och implementeras mot bakgrund av den nya tidens kund- och samhällskrav ligger hos respektive nätägare.

3 Definitioner

Elektroniskt kommunikationsnät
Ett system för överföring och i tillämpliga fall utrustning för koppling eller dirigering samt passiva nätdelar och andra resurser som medger överföring av signaler, via tråd eller radiovågor, på optisk väg eller via andra elektromagnetiska överföringsmedier, oberoende av vilken typ av information som överförs.

Elektronisk kommunikationstjänst
En tjänst som vanligen tillhandahålls mot ersättning via elektroniska kommunikationsnät och som, *med undantag för dels tjänster i form av tillhandahållande av innehåll som överförs med hjälp av elektroniska kommunikationsnät och elektroniska kommunikationstjänster, dels tjänster som innebär utövande av redaktionellt ansvar över sådant innehåll*, är en:

1. internetanslutningstjänst enligt artikel 2.2 i Europaparlamentets och rådets förordning om åtgärder rörande en öppen internetanslutning och slutkundsavgifter för reglerad kommunikation inom EU.
2. interpersonell kommunikationstjänst, eller
3. tjänst som utgörs helt eller huvudsakligen av överföring av signaler, såsom överföringstjänster som används för tillhandahållande av maskin-till-maskin-tjänster eller för rundradio.

Tillgångar
funktion som utgörs av en avgränsad del av ett kommunikationsnät eller en kommunikationstjänst och som är nödvändig för att tillhandahålla ett sådant nät eller en sådan tjänst, samt som används för att sända, motta, bearbeta eller lagra information.

Informationsbehandlingstillgångar
system, databaser och fysiska resurser som används för informationsbehandling.

Förbindelser
del av kommunikationsnät mellan två tillgångar eller mellan en tillgång och en anslutning till ett kommunikationsnät.

Skyddsnivå
Den specificerade nivån av fysiska säkerhetsåtgärder som krävs för att skydda förbindelser mot oönskade händelser

Säkerhetsnivå
Den specificerade nivån av tekniska säkerhetsåtgärder som krävs för att skydda en site mot oönskade händelser.

4 Säkerhetsdomäner

En nätägare ska arbeta med säkerhetsfrågor inom flera olika områden. Vi benämner dessa områden för säkerhetsdomäner. Dessa säkerhetsdomäner har på olika sätt inbördes relationer vilket illustreras i nedanstående bild. En generell och övergripande information om de olika säkerhetsdomänerna redovisas i detta avsnitt.

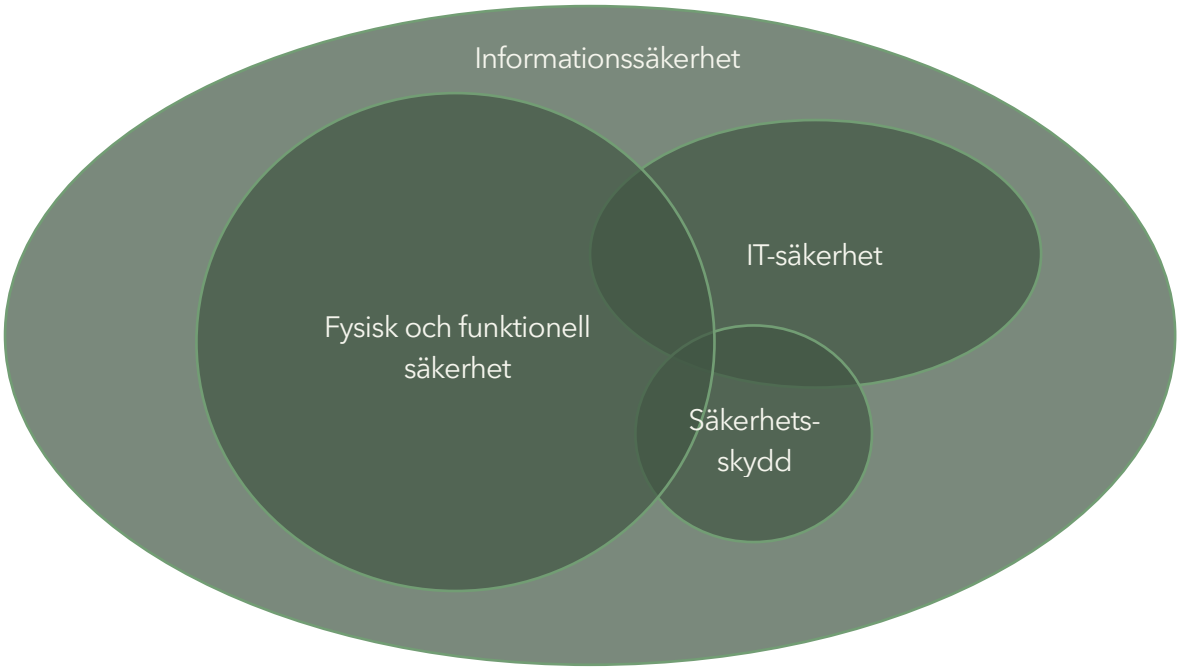


Bild. Säkerhetsdomäner

4.1 Informationssäkerhet

Informationssäkerhet är en säkerhetsdomän som ställer krav på övriga säkerhetsdomäner och utgör därför ett samlingsnamn för samtliga säkerhetsdomäner som ska hanteras av nätägare.

Målet med informationssäkerhetsarbetet är att säkerställa informationens konfidentialitet, riktighet och tillgänglighet så att:

- endast behöriga personer, entiteter eller processer får ta del av informationen (konfidentialitet),
- det går att lita på att informationen är korrekt och inte manipulerad eller förstörd (riktighet),
- informationen alltid finns när den behövs (tillgänglighet).

När det gäller styrning och övervakning av produktions- och distributionsmiljöer kallas detta för Operational Technology eller OT. OT-säkerhet handlar om att undvika att fysiska skador eller störningar inträffar i produktions- eller distributionsmiljöer och att minimera risken för svåra konsekvenser om de ändå inträffar. Det handlar om hur vi arbetar, hur våra system skyddas och hur man utvecklar systemkomponenter för OT-världen.

Ett exempel på en produktions-och distributionsmiljö är fastighetsstyrning i den smarta staden.

Rekommenderade standarder inom domänen är:

- ISO 27000 serien – Ledningssystem för cyber- och informationssäkerhet.
- ISA/IEC 62443 standards - Security for industrial automation and control systems (IACS).

4.2 Fysisk och funktionell säkerhet

För en nätägare omfattar området tillgångar, informationsbehandlingstillgångar, förbindelser och system för styrning och övervakning av nät och tjänster.

- Den fysiska säkerheten omfattar åtgärder för att hantera fysiska hot mot tillgångar, informationsbehandlingstillgångar, förbindelser och system för styrning och övervakning.
  Fysiska hot kan till exempel omfatta stöld, brand, kabelbrott och strömavbrott. Även hot om brist på utrustning och reservdelar till kritiska nätverk och informationssystem omfattas.*
- Den funktionella säkerheten omfattar åtgärder för att hantera logiska hot mot tillgångar, informationsbehandlingstillgångar, förbindelser och system för styrning och övervakning.
  Logiska hot kan till exempel omfatta kända sårbarheter i mjukvara, logiska överbelastningsattacker, logiska intrång, otillåtna förändringar av DNS-data, konfigurationsfel, fel och brister i hårdvara eller mjukvara (såväl egenutvecklad som utvecklad av annan) samt bristfällig segmentering av nätverk. Med DNS-data avses uppgifter om bl.a. vilken IP-adress ett efterfrågat domännamn motsvarar, en officiell namnserver för en zon, parametrar för och information om zonen samt vilket domännamn som motsvarar en efterfrågad IP-adress.*
- Den organisatoriska säkerheten för den verksamhet som svarar för den fysiska och funktionella säkerheten är en viktig komponent i säkerhetsarbetet.
  Organisatoriska hot kan till exempel kritiska personberoenden, otillräcklig kompetensförsörjning, bristfälliga processer för att uppnå en hög säkerhet i nätverk och informationssystem (särskilt bristfälliga rutiner vid förändringshantering), bristfällig incidenthantering och bristfällig behörighets- och åtkomsthantering.*

**Post- och telestyrelsens föreskrifter och allmänna råd om säkerhetsåtgärder för samhällsviktiga tjänster inom sektorn digital infrastruktur;*

4.3 IT-säkerhet

IT-säkerhet omfattar skyddet av ett företags eller en organisations IT-system. IT-säkerhet avseende en nätägares kommunikationsnät och tjänster handlar om att säkerställa att information som överförs, lagras och hanteras i nätet är skyddad och att uppgifter som behandlas i samband med tillhandahållande av nät eller tjänster är skyddade.

Det handlar om åtgärder för att skydda IT-systemet och aktiv utrustning från exempelvis brand, den mänskliga faktorn, stölder, sabotage och buggar eller brister i mjukvara och hårdvara. För att skydda IT-system och aktiv utrustning krävs inte bara tekniska åtgärder utan också åtgärder som omfattar organisation, personal, processer och rutiner. Några av de byggstenar som utgör IT-säkerheten är:

- **Organisation** – en organisation där behörighet och ansvar för vem som hanterar vad är tydligt reglerat.
- **Kunskap, policy, säkerhetstänk och rutiner** – utbildning och medvetenhet om säkerhetshot och säkerhetstänk om hur medarbetarna kan bidra till IT-säkerheten.
- **Utrustning** – skydd av den hård- och mjukvara som skyddar företagets IT-system och aktiva utrustningar.
- **Underhåll och drift** – rutiner för uppföljning av hotbilder, underhåll och säkerhetsuppdateringar.
- **Backup** – rutiner och lösningar för backup.

Rekommenderad vägledning för området är ***MSB Vägledning - säkerhetsåtgärder i informationssystem*** (www.msb.se).

4.4 Säkerhetsskydd

Med säkerhetsskydd avses skydd av säkerhetskänslig verksamhet som är av betydelse för Sveriges säkerhet till exempel mot spionerі, sabotage, terroristbrott och andra brott som kan hota verksamheten samt skydd i andra fall av säkerhetsskyddsklassificerade uppgifter.

Säkerhetspolisen utövar tillsyn över säkerhetsskyddet hos ett flertal myndigheter enligt säkerhetsskyddsförordningen

Läs mer ***om säkerhetsskydd*** på Säkerhetspolisens hemsida (www.sakerhetspolisen.se).

5 Nätägarens ansvar

5.1 Allmänt

Att ansvara för en fiberanläggning ställer stora krav på nätägaren och den organisation som ska planera, bygga och förvalta anläggningen. Säkerhetsarbetet styrs av olika lagar, förordningar, föreskrifter och kundkrav som sammantaget kan vara svåra att överblicka.

edan redovisas en sammanställning över de lagar och förordningar som en nätägare har att förhålla sig till i sitt säkerhetsarbete. Sammanställning visar också de analyser som krävs för att identifiera de åtgärder av olika slag som krävs för att säkerställa att nätägarens anläggningar och verksamhet svarar mot ställda krav.

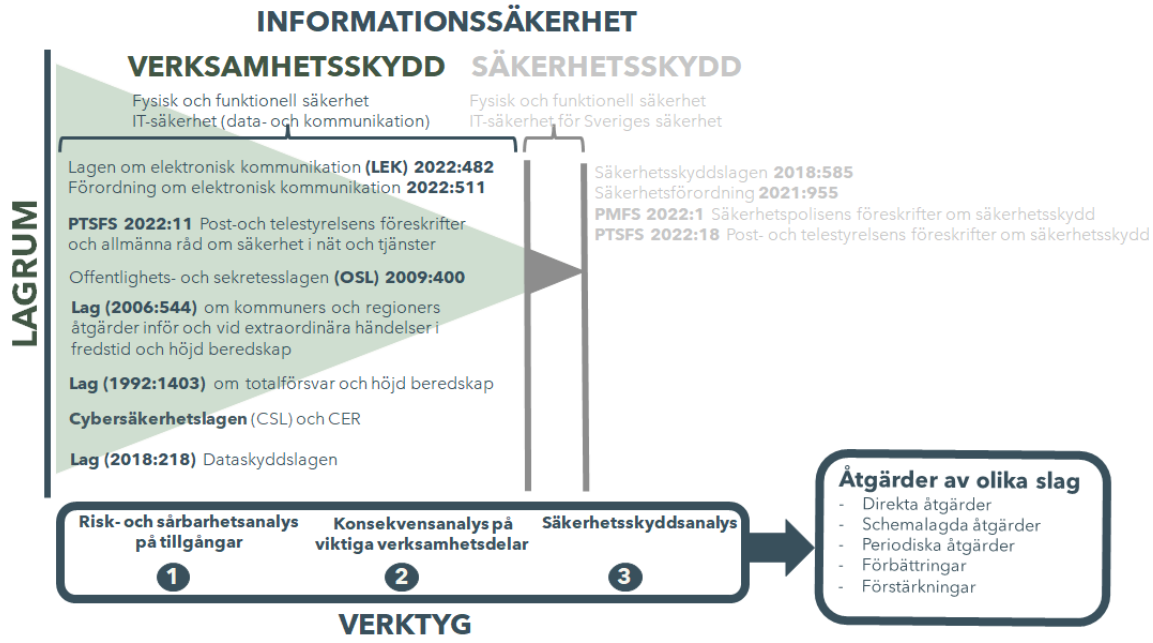


Bild. Sammanställning över lagar och förordningar

5.2 Skydd

En nätägare ska bedriva ett kontinuerligt och långsiktigt arbete med att skydda sin verksamhet och den elektroniska kommunikation som verksamheten tillhandahåller. De skyddsbegrepp som nätägaren behöver förhålla sig till är verksamhetsskydd och säkerhetsskydd.

Verksamhetsskydd
Skydd av personal, kunder, information, lokaler och utrustning för att säkerställa förmågan att planera och genomföra verksamhetens uppgifter och handlingar, för att behålla en ostörd produktion.

Säkerhetsskydd
Skydd av information och verksamheter som är av betydelse för Sveriges säkerhet mot spionerі, sabotage, terroristbrott och vissa andra hot. Säkerhetsskydd handlar också om att skydda verksamhet som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd

De analyser och de åtgärder av olika slag som krävs för att säkerställa skyddet av nätägarens anläggningar och förbindelser ryms i huvudsak inom begreppet verksamhetsskydd.

5.3 Lagrum

5.3.1 Lagen om elektronisk kommunikation

5.3.1.1 Tillhandahållande av nät och tjänster
För en nätägare gäller *lagen om elektronisk kommunikation (LEK)* om nätägaren tillhandahåller *"Allmänna elektroniska kommunikationsnät som vanligen tillhandahålls mot ersättning eller allmänt tillgängliga elektroniska kommunikationstjänster"*. Sådana nät och tjänster får tillhandahållas endast efter anmälan till tillsynsmyndigheten.

Det finns undantag från kravet om anmälan för:

1. nummeroberoende interpersonella kommunikationstjänster, eller
2. verksamhet som består enbart i överföring av signaler via tråd för utsändning till allmänheten av program som avses i 1 kap. 2 § yttrande-frihetsgrundlagen.

När det gäller krav på säkerhet i nät och tjänster anger lagen att den som tillhandahåller ett allmänt elektroniskt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst ska vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att på ett lämpligt sätt hantera risker som hotar säkerheten i nät och tjänster. Åtgärderna ska säkerställa en nivå på säkerheten i nät och tjänster som är lämplig i förhållande till riskerna. Åtgärder ska vidtas särskilt för att förebygga och minimera säkerhetsincidenters påverkan på användare och på andra nät och tjänster.

5.3.1.2 Säkerhet i nät och tjänster
För att precisera lagens krav på säkerhet i nät och tjänster har Post-och telestyrelsen (PTS) utgett föreskriften *Post- och telestyrelsens föreskrifter och allmänna råd om säkerhet i nät och tjänster*.

Med referens till lagen om elektronisk kommunikation innehåller föreskriften bestämmelser om:

- tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nät och tjänster,
- rapportering av säkerhetsincidenter som har haft en betydande påverkan på kommunikationsnät och kommunikationstjänster,
- skyldighet för tillhandahållare att informera användare vid ett konkret och betydande hot om en säkerhetsincident,
- särskilda tekniska och organisatoriska åtgärder som ska vidtas i samband med lagring och annan behandling av uppgifter för brottsbekämpande ändamål,
- tekniska och organisatoriska åtgärder som ska vidtas för att säkerställa att uppgifter som behandlas i samband med tillhandahållandet av kommunikationstjänsten skyddas,
- innehållet i förteckningen över integritetsincidenter, och
- fredstida planering för totalförsvarets behov av elektroniska kommunikationer.

5.3.1.3 Totalförsvar och höjd beredskap
Post- och telestyrelsens föreskrifter och allmänna råd om säkerhet i nät och tjänster anger i kapitlet *Fredstida planering för totalförsvarets behov av elektroniska kommunikationer* att den som tillhandahåller ett kommunikationsnät eller en kommunikationstjänst under angivna förutsättningar ska fram kontinuitetsplaner för höjd beredskap och krig. Post- och telestyrelsen kan komma att informera tillhandahållare om ytterligare krav avseende beredskapsåtgärder.

Tillhandahållaren ska också ta fram planer för att vid höjd beredskap och i krig kunna ställa personal till förfogande för samverkan med Post- och telestyrelsen i den omfattning som krävs. Tillhandahållaren ska planera för att upprätthålla samverkansfunktionen dygnet runt i 90 dagar.

5.3.2 Lagen om kommuners och regioners åtgärder
Lagen om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap omfattar även kommunala och regionala bolag, exempelvis stadsnät och regionnät.

Extraordinär händelse, händelse som avviker från det normala, innebär en allvarlig störning eller överhängande risk för en allvarlig störning i viktiga samhällsfunktioner och kräver skyndsamma insatser av en kommun eller en region.

Förberedelser för och verksamhet under extraordinära händelser i fredstid

- Analys, RSA och planering avseende extraordinära händelser. Krisledningsnämnd leder vid händelse.
- Geografiskt områdesansvar, verka för att olika aktörer i kommunen samverkar och uppnår samordning i planerings- och förberedelsearbetet, krishanteringsåtgärder som vidtas av olika aktörer under en sådan händelse samordnas, informationen till allmänheten under sådana förhållanden samordnas.
- Utbildning och övning.

Förberedelser för och verksamhet under höjd beredskap (kommunstyrelsen)

- Förberedelser för verksamheten under höjd beredskap. Ledningsansvar hos kommunstyrelsen.
- Geografiskt områdesansvar, verka för att den verksamhet som bedrivs i kommunen av olika aktörer samordnas och för att samverkan kommer till stånd mellan dem som bedriver verksamheten.

6 Samhällsviktig verksamhet

6.1 Samhällsviktig verksamhet

En nätägare som har anmält och bedriver en verksamhet i enlighet med LEK bedriver också en samhällsviktig verksamhet.

Med samhällsviktig verksamhet avses verksamhet, tjänst eller infrastruktur som upprätthåller eller säkerställer samhällsfunktioner som är nödvändiga för samhällets grundläggande behov, värden eller säkerhet.

Viktig samhällsfunktion: samhällsfunktion som är nödvändig för samhällets grundläggande behov, värden eller säkerhet, till exempel omsorg av barn, betalningsförmedling och vägtransporter. Dessa upprätthålls och säkerställs av samhällsviktiga verksamheter.

MSB har tagit fram en metod för ***Identifiering av samhällsviktig verksamhet*** och en ***Lista med viktiga samhällsfunktioner*** som ska vara vägledande för identifieringen. Listan är framtagen i samsyn med centrala myndigheter, länsstyrelser, regioner och kommuner. Identifiering av samhällsviktig verksamhet. Lista med viktiga samhällsfunktioner.

Listan omfattar olika typer av områden med viktiga samhällsfunktioner och där Infrastruktur och tjänster för elektroniska kommunikationer utgör en funktion inom området Information och kommunikation.

- **Infrastruktur och tjänster för elektroniska kommunikationer**
  Verksamhet som möjliggör elektroniska kommunikationsnät och kommunikationstjänster. Detta är till exempel verksamhet som möjliggör transmissions- och accessnät, anläggningsförvaltning av master, byggnader, noder och knutpunkter samt kanalisation och fysiska ledningar. Det är även verksamhet för styrning och övervakning av nät och tjänster, felavhjälpande underhåll och nybyggnation, verksamhet som möjliggör tillhandahållande av DNS-tjänster samt tjänster för tid och frekvens.

Det är även önskvärt att de verksamheter som inte är uppenbart samhällsviktiga fortsätter fungera så långt som möjligt även under en störning.

För fördjupad information om samhällsviktig verksamhet, besök www.msb.se.

6.2 Skydd av samhällsviktig verksamhet

Att bedriva en samhällsviktig verksamhet innebär att verksamheten ska bedriva ett systematiskt arbete för att skydda verksamheten. MSB har tagit fram ett stöd för ett ***Systematiskt arbete med skydd av samhällsviktig verksamhet: stöd för arbete med riskhantering, kontinuitetshantering och att hantera händelser*** (www.msb.se). Arbetet omfattar riskhantering, kontinuitetshantering och hantering av händelser.

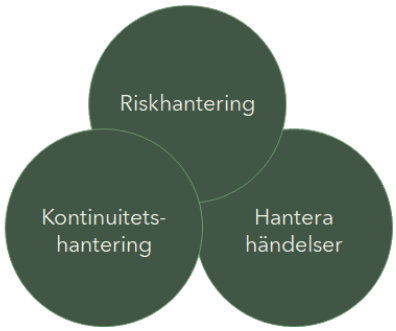


Bild. Omfattning samhällsviktig verksamhet

Riskhantering
Inkluderar att identifiera, bearbeta, värdera, hantera och kontrollera risker.

Kontinuitetshantering
Fokuserar på att planera för att kunna upprätthålla verksamhet och processer för att skapa en nödvändig förmåga till funktionalitet, oavsett händelse.

Hantera händelser

Genom att planera för att kunna hantera olika händelser, allt från incidenthantering till krishantering, skapas förutsättningar för att en händelse effektivt ska kunna tas om hand och för att den samhällsviktiga verksamheten kan upprätthållas. Genom att implementera PTS säkerhetsföreskrift uppfyller nätägaren också MSB krav på ett systematiskt arbete för skydd av den samhällsviktiga verksamheten.

Bild. Skydd av samhällsviktig verksamhet

7 Anläggningar med förhöjd säkerhet och funktion

7.1 Anvisningen för Anläggningar med förhöjd säkerhet och funktion

Anvisningen för Anläggningar med förhöjd säkerhet och funktion omfattar detta huvuddokument med bilagor och utgör ett komplement till anvisningarna för robust fiber.

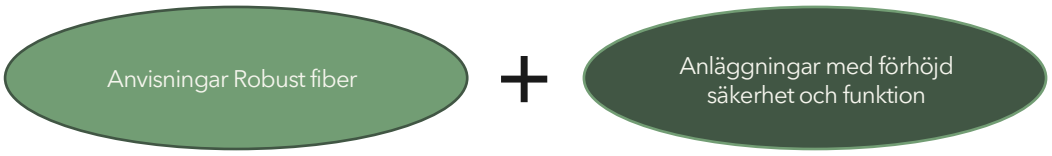


Bild. Kompletterande anvisningar

Bilagorna *Robust site för samhällsviktig digital infrastruktur* och *Passiv säker fysisk förbindelse* redovisas övergripande i *kapitel 8 Krav på anläggningar med förhöjd säkerhet*.

För de kompletta versionerna, besök https://stadsnatsforeningen.se/branschstod/robust-digital-infrastruktur/

8 Krav på anläggningar med förhöjd säkerhet och funktion

8.1 Översikt

Anläggningar med krav på förhöjd säkerhet ska uppfylla en grundläggande säkerhet och funktion i enlighet med anvisningarna för Robust fiber samt, beroende av identifierat krav på förhöjd säkerhet, nedanstående bilagor:

- Bilaga 1 Robust Site för samhällsviktig digital infrastruktur
  - Bilaga 1.1 Checklista Robust site för samhällsviktig digital infrastruktur
- Bilaga 2 Passiv säker fysisk förbindelse
  - Bilaga 2.1 Checklista Passiv säker fysisk förbindelse
- Bilaga 3 Metod för anläggningsanalys

Bilden nedan utgör en konceptuell bild av relationerna mellan de olika anvisningarna för anläggningar med utökad säkerhet.

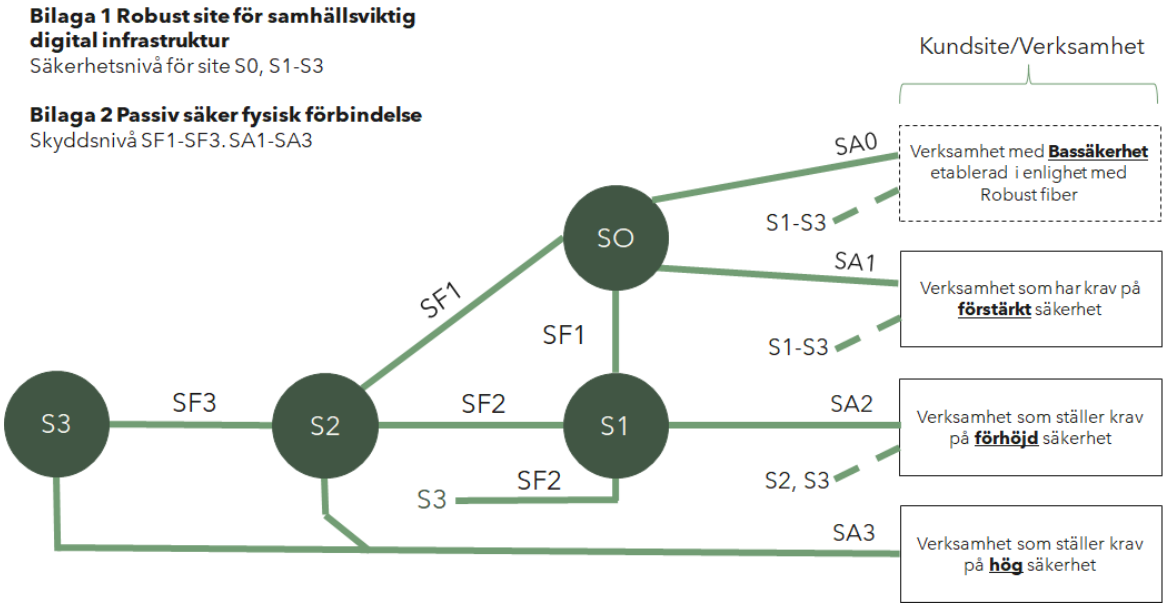


Bild. Översikt kravbilagor för anläggningar med förhöjd säkerhet

För att identifiera om en anläggning ska anläggas med en förhöjd säkerhet används en metod för anläggningsanalys, se *kapitel 9 Metod för anläggningsanalys*.

8.2 Bilaga 1: Robust Site för samhällsviktig digital infrastruktur

8.2.1 Inledning

Denna bilaga riktar sig till nätägare av fiberbaserad infrastruktur och utgör en komplettering av anvisningarna för Robust fiber Bilaga 4 Robust site och nod. Anvisningen 0mfattar alternativa åtgärder för hur skyddet av en Site kan kompletteras för att motstå allvarliga störningar vid krav på förhöjd eller hög säkerhet för Siten.

Bilagan omfattar krav vid nybyggnation samt krav vid ombyggnad av befintlig anläggning.

Bilagan innehåller även rekommendationer samt exempel på lösningar.

8.2.2 Bilagan och dess innehåll

Bilagan tar bland annat upp:

- Hot mot siters fysiska säkerhet.
- Säkerhetsnivåer för site.
- Beskrivning av skyddsåtgärder.
- Skyddsåtgärder för respektive säkerhetsnivå.
- RSA.

8.2.3 Säkerhetsnivåer

Säkerhetsnivåerna för site omfattar fyra säkerhetsnivåer enligt nedan.

S0. Liten lokal betydelse
Siten hanterar noder för ett lokalt område med ett begränsat antal anslutningar med verksamhet som inte har krav på förhöjd eller hög säkerhet. Siten kan hantera inplacering av system och utrustning genom montage i elektronikrack.

S1. Stor lokal betydelse
Siten hanterar noder för ett lokalt område som har en eller flera anslutningar med verksamhet som ställer krav på förhöjd säkerhet. Siten kan hantera insynsskyddad inplacering av system och utrustning i begränsad omfattning.

S2. Stor betydelse
Siten hanterar en central strategisk nod inom ett geografiskt område. Siten hanterar in och utgående trafik för ett geografiskt område till exempel en kommun. Kan hantera inplacering av system och utrustning för anslutningar med verksamhet som ställer krav på hög säkerhet genom inplacering av elektronikrack i, för verksamheten egen sektion, med inbrottslarm och passagesystem.

S3. Avgörande betydelse
Siten hanterar trafik som ingår i den regionala- eller nationella elektroniska infrastrukturen. Siten kan hantera inplacering av system och utrustning för anslutningar med verksamhet som ställer krav på hög säkerhet genom inplacering av elektronikrack i, för verksamheten eget, insynsskyddat utrymme med mekaniskt skydd, sabotageskydd, inbrottslarm och passagesystem.

8.2.4 Skyddsåtgärder

Bilagan innehåller beskrivningar av olika skyddsåtgärder för att öka säkerheten för siter. Skyddsåtgärderna åsätts de olika siterna beroende den på säkerhetsnivå som siten har. Skyddsåtgärderna är uppdelade på siteområde och sitebyggnad.

8.3 Bilaga 2: Passiv säker fysisk förbindelse

8.3.1 Inledning

Denna bilaga riktar sig till nätägare av fiberbaserad infrastruktur och utgör en komplettering av anvisningarna för Robust fiber Bilaga 2 Robusta nät. Anvisningen omfattar alternativa åtgärder för hur skyddet för fysiska förbindelser kan kompletteras för att motstå allvarliga störningar vid krav på förhöjd eller hög säkerhet mellan siter i nätet eller mellan en site i nätet och en kundsite.

Bilagan omfattar åtgärder vid nybyggnation samt vid ombyggnad av befintlig anläggning. Bilagan innehåller även rekommendationer samt exempel på lösningar.

8.3.2 Bilagan och dess innehåll

Bilagan tar bland annat upp:

- Hot mot fysiska förbindelser.
- Skyddsnivåer för fysiska förbindelser.
- Beskrivning av skyddsåtgärder.
- Skyddsåtgärder för respektive skyddsnivå.
- RSA.

8.3.3 Skyddsnivåer för förbindelser mellan siter

Skyddsnivå SF0
Fysiska förbindelser med krav på bassäkerhet i enlighet med Robust fiber.

Skyddsnivå SF1
Fysiska förbindelser med krav på förstärkt säkerhet och redundans mellan noder i siter med skyddsnivå S0 och S1 eller S2.

Skyddsnivå SF2
Fysiska förbindelser med förhöjd säkerhet för skydd av elektronisk kommunikation mellan noder i siter med skyddsnivå S1 och S2 eller S3.

Skyddsnivå SF3
Fysiska förbindelser med hög säkerhet för skydd av elektronisk kommunikation mellan noder i siter med säkerhetsnivå S2 eller S3.

8.3.4 Skyddsnivåer för anslutning

Skyddsnivå SA0
Fysiska förbindelser med krav på bassäkerhet i enlighet med Robust fiber.

Skyddsnivå SA1
Fysiska förbindelser för anslutning av en kundsite med användare som bedriver en verksamhet med krav på förstärkt säkerhet med redundans.

Skyddsnivå SA2
Fysiska förbindelser för anslutning av en kundsite med användare som bedriver verksamhet med krav på förhöjd säkerhet och redundans. Kan anslutas till Site S1 eller högre.

Skyddsnivå SA3
Fysiska förbindelser för anslutning av en kundsite med användare som bedriver verksamhet med krav på hög säkerhet och redundans. Kan anslutas till Site S2 eller högre.

8.3.5 Skyddsåtgärder

Bilagan innehåller beskrivningar av olika skyddsåtgärder för att öka säkerheten för fysiska förbindelser. Skyddsåtgärderna åsätts framföringsvägar och förbindelser beroende den på skyddsnivå förbindelsen har.

9 Anläggnings- och kundanalys

9.1 Metodöversikt

Nätägaren ska inom ramen för *Post-och telestyrelsens föreskrifter och allmänna råd om nät och tjänster* ha genomfört risk- och sårbarhetsanalyser på anläggningstillgångar och förbindelser.

För en nätägare är det viktigt att klargöra nedanstående frågor:

- Vilken/vilka säkerhets- och skyddsnivå(er) kan min anläggning erbjuda?
- Vilken/vilka säkerhets- och skyddsnivå(er) ska min anläggning kunna erbjuda?
- Vilka säkerhets- och skyddsåtgärder behöver jag komplettera anläggningen med?

För att analysera lämpliga skydds- respektive säkerhetsnivåer används en process för anläggningsanalys enligt nedan.

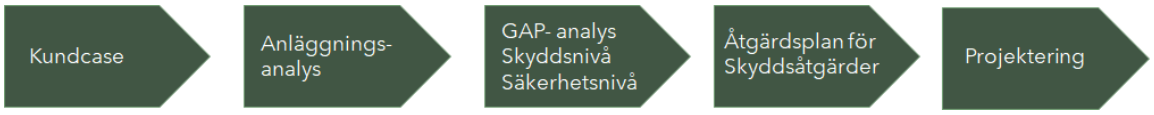


Bild. Anläggningsanalys

För detaljerad information se *Bilaga 3 Metod för anläggningsanalys*.

10 Hotkatalog, risk- och sårbarhetsanalys (RSA)

Hotkataloger samt verktyg och instruktioner för genomförandet av risk-och sårbarhetsanalyser finns samlat under en gemensam plats Bashot Telekom med adressen:

https://stadsnatsforeningen.se/branschstod/robust-digital-infrastruktur/

För genomförandet av risk-och sårbarhetsanalyser avseende verksamhet, siter, fysiska förbindelser och informationsbehandlingstillgångar används nedanstående dokument baserade på *Verktyget Hotkatalog, risk och sårbarhetsanalys*:

- RSA Site och nod.
- RSA Passiv säker förbindelse.
- RSA Informationsbehandlingstillgångar.
- RSA Verksamhet nätdrift.
- Instruktion för RSA inom Bashot Telekom.

11 Utbildning och certifiering

Utbildning och certifiering avseende anläggningar med krav på förhöjd säkerhet bedrivs under namnet **Personcertifikat Säker anläggning**.

Bild. Utbildning

Kursen riktar sig till ledningspersonal och tekniker som arbetar med planering, utveckling och förstärkning av den av den fysiska säkerheten i teleanläggningar.

Efter genomförd kurs och godkänt prov ska deltagaren kunna svara för klassificering av skyddsnivåer, projektering, besiktning och RSA för anläggningar med förhöjd säkerhet.

12 Referenslista

Europaparlamentets och rådets förordning (EU) 2015/2120 av den 25 november 2015 om åtgärder rörande en öppen internetanslutning och slutkundsavgifter för reglerad kommunikation inom EU och om ändring av direktiv 2002/22/EG och förordning (EU) nr 531/2012,

Lag 2022:482 om elektronisk kommunikation (LEK)

Förordning SFS 2022:511 om elektronisk kommunikation

Post-och telestyrelsens föreskrifter och allmänna råd om säkerhet i nät och tjänster PTSFS 2022:11

Offentlighets- och sekretesslagen (OSL) 2009:400

Lag (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap

Lag (1992:1403) om totalförsvar och höjd beredskap

Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS)

Säkerhetsskyddslagen (2018:585)

Säkerhetsförordning (2021:955)

Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2022:1)

Post- och telestyrelsens föreskrifter om säkerhetsskydd (PTSFS 2021:2)

MSB2032 Vägledning - säkerhetsåtgärder i informationssystem (MSB2032)

MSB932 Systematiskt arbete med skydd av samhällsviktig verksamhet: stöd för arbete med riskhantering, kontinuitetshantering och att hantera händelser