Rapportnummer
PTS-ER-2018:23

Datum
2018-10-24

Rapport:

Risk- och sårbarhetsanalys för PTS och dess ansvarsområden 2018

Risk- och sårbarhetsanalys för PTS och dess ansvarsområden 2018

Rapportnummer
PTS-ER-2018:23

Diarienummer
18-8163

ISSN
1650-9862

Författare
Jachym Ctvrtek, Åsa Gustafsson, Björn Scharin, Björn Hesthamar, Anders Bendz, Ulf Johansson, Lars Lundgren, Anna Wibom, Håkan Swedenborg, Peter Wallström, Christina Hedlund (projektledare)

Post- och telestyrelsen
Box 5398
102 49 Stockholm

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

Förord

Digitaliseringen av samhället och det förändrade säkerhetspolitiska läget har stor inverkan på Post- och telestyrelsen (PTS) uppdrag och verksamhet. Elektroniska kommunikationer är en grundläggande funktion för att dagens samhälle ska fungera och har stor betydelse för alla slags verksamheter. Detta gäller inte enbart för privatpersoner och företag. Allt fler samhällsfunktioner måste kunna utbyta information elektroniskt mellan individer, organisationer och tekniska system. Möjligheten att kommunicera och utbyta information är särskilt viktig vid olyckor, kriser samt vid andra allvarliga händelser som på olika sätt prövar vårt samhälle.

PTS verkar för robusta elektroniska kommunikationer som minskar risken för störningar och avbrott. Myndigheten vidtar åtgärder i samverkan mellan privat och offentlig sektor för att stärka infrastrukturen och berörda aktörers krishanteringsförmåga. Åtgärderna ska möta samhällets behov av elektronisk kommunikation och minska konsekvenserna av svåra påfrestningar på samhället i fred och öka beredskapen inför höjd beredskap eller krig. Detta arbete blir allt viktigare i takt med att beroendet av elektronisk kommunikation ökar samtidigt som förväntningarna på att det alltid ska fungera ökar.

PTS har även en viktig roll för att Sverige ska ha en tillförlitlig posttjänst för alla användare. Övergången från traditionella posttjänster till digitala lösningar ska ske på ett hållbart sätt. Olika användargruppers behov måste tillgodoses så att användarna har tillgång till grundläggande posttjänster till rimliga priser.

Samhällets beroende av elektroniska kommunikationer är större än någonsin. Beroendet av post är fortsatt stort och blir än större om elektroniska kommunikationerna fallerar. En förutsättning för digitalisering av samhället är att det i hela landet finns en väl utbyggd infrastruktur för elektronisk kommunikation, med tillräcklig kapacitet, kvalitet, säkerhet och robusthet.

Dan Sjöblom
Generaldirektör

Innehåll

Sammanfattning

Syftet med risk- och sårbarhetsanalysen är att bidra till en riskbild för samhället, ge underlag för bedömningar för beslutsfattare och verksamhetsansvariga, ge ett underlag för information om samhällets risker till allmänheten samt ge underlag för samhällsplanering.

Risk- och sårbarhetsanalys för PTS interna verksamhet

PTS har analyserat risker och sårbarheter i myndighetens interna verksamheter och funktioner som bedömts som samhällsviktiga. Dessa är:

- verksamheterna tillståndsgivning för radiosändare och radiotillsyn,
- verksamheter som under extraordinära händelser ska ta fram en samlad lägesbild för sektorerna elektronisk kommunikation respektive post, och
- verksamheter som under extraordinära händelser ska stödja sektorerna elektronisk kommunikation respektive post, t.ex. i samband med prioritering av resurser.

I analysen har oönskade händelser som kan resultera i skadekonsekvenser för verksamheter som PTS identifierat som samhällsviktiga riskbedömts. Med hänsyn tagen till att PTS vidtagit vissa åtgärder för att motverka de oönskade händelserna, har kvarstående systematiska sårbarheter kopplade till händelser som bedömts ha störst riskvärde identifierats. Dessa sårbarheter avser tekniska fel som kan leda till bortfall av internetförbindelser och it-angrepp med skadlig kod. För att motverka identifierade sårbarheter genomför PTS bl.a. åtgärder kopplade till myndighetens it-infrastruktur och åtgärder för att utveckla krishanteringsförmågan.

Risk- och sårbarhetsanalys för postsektorn.

Analysen för postsektorn är den fjärde som genomförts och har i likhet med de tidigare avgränsats, nu till Postnord Sverige AB

Samhällsviktiga verksamheters beroenden av den samhällsomfattande post-tjänsten är i dagsläget inte klarlagda. Analysen för postsektorn har därför gjorts utifrån en på förhand fastställd bedömningsgrund som bygger på de krav och förväntningar på postsektorn som kan utläsas ur de lagar och regler som styr den samhällsomfattande posttjänsten. Den här rapporten omfattar processerna ”Producera Brevtjänst” och ”Producera Paket” vilka avser hantering av brev (adresserade försändelser upp till 2 kg) respektive paket (adresserade försändelser upp till 20 kg).

Sammanfattningsvis bedöms Postnord Sverige AB ha en god generell förmåga att motstå och hantera de största och mest sannolika risker som identifierats och värderats i analysen.

Risk- och sårbarhetsanalys för sektorn elektronisk kommunikation

Elektronisk kommunikation är en mycket viktig del av dagens samhälle, för privatpersoner, företag och olika typer av organisationer. Nätsäkerhetshändelser som påverkar överförda och genererade informationstillgångars tillgänglighet, konfidentialitet och riktighet kan därmed påverka ett eller flera samhälleliga skyddsvärden negativt.

I risk- och sårbarhetsanalysen för elektronisk kommunikation identifieras och värderas de hot som kan få nationella konsekvenser. Här 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 riskerna för dessa bedöms vara låga.

PTS har genomfört och planerar flera åtgärder som på olika sätt kan minska risker i elektronisk kommunikation och som kompletterar operatörernas nätsäkerhetsarbete.

Risk– och sårbarhetsanalys för sektorerna elektronisk kommunikation och post för höjd beredskap

Redovisning av myndighetens risk- och sårbarhetsanalys för sektorerna elektronisk kommunikation och post för höjd beredskap sker i en bilaga som omfattas av sekretess enligt 15 kap 2 § lagen om offentlighet- och sekretess (2009:400).

1 Inledning och rapportens upplägg

Av 8 § tredje stycket i förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap ska varje myndighet i syfte att stärka sin egen och samhällets krisberedskap analysera om det finns sådan sårbarhet eller sådana hot och risker inom myndighetens ansvarsområde som synnerligen allvarligt kan försämra förmågan till verksamhet inom området. Enligt samma paragraf ska de myndigheter som har ett särskilt ansvar för krisberedskapen enligt 10 § krisberedskapsförordningen och de myndigheter som Myndigheten för samhällsskydd och beredskap (MSB) beslutar i enskilda fall, lämna senast vid utgången av oktober månad varje jämnt år en sammanfattande redovisning baserad på analysen till Regeringskansliet och MSB. Redovisningen ska innefatta vilka åtgärder som planeras och en bedömning av behovet av ytterligare åtgärder.

I risk- och sårbarhetsanalysen för Post- och telestyrelsen (PTS) och dess ansvarsområden 2018 genomförs risk- och förmågebedömningar utgående från ett samhällsperspektiv, MSBFS 2016:7 (Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters risk- och sårbarhetsanalyser). Analysen begränsas till de fall då förekomsten av avbrott och brister i informationssäkerhet kan innebära en stor risk eller fara för befolkningens liv och hälsa, störningar i samhällets funktionalitet eller negativ påverkan på samhällets grundläggande värden.

Denna sammanställning, som följer innehållsindelning från 4 § föreskriften MSBFS 2016:7, innehåller redovisningar av risk- och sårbarhetsanalyser avseende PTS interna verksamhet samt myndighetens båda sektorer post och elektronisk kommunikation. Enligt 3 § föreskriften MSBFS 2016:7 ska myndigheten i arbetet med risk- och sårbarhetsanalyser beakta både krissituationer i fredstid och situationer med höjd beredskap.

Rapportens disposition

Rapporten inleds i kapitel 2 med en beskrivning av myndigheten och dess ansvarsområden. Därefter redovisas risk- och sårbarhetsanalyser för PTS och dess ansvarsområden i följande 3 separata kapitel.

- Kapitel 3 Risk- och sårbarhetsanalys för PTS interna verksamhet
- Kapitel 4 Risk- och sårbarhetsanalys för postsektorn
- Kapitel 5 Risk- och sårbarhetsanalys för sektorn för elektronisk kommunikation

Upplägget för kapitel 3-5 följer innehållsindelning från 4 § föreskriften MSBFS 2016:7. Vilket medför att för PTS och dess ansvarsområden beskrivs:

- arbetsprocess och metod
- identifierade samhällsviktiga verksamheter inom ansvarsområdet som är av nationell/regional betydelse
- identifierade kritiska beroenden för identifierad samhällsviktig verksamhet
- identifierade och analyserade hot och risker
- beskrivning av identifierade sårbarheter och brister i krisberedskap
- genomförda, pågående och planerade åtgärder sedan föregående rapportering

Kapitel 3 som behandlar PTS interna verksamhet innehåller även en bedömning av PTS generella krisberedskap enligt indikatorer som framgår av bilaga i föreskriften MSBFS 2016:7.

2 Beskrivning av myndigheten och dess ansvarsområden

PTS är förvaltningsmyndighet med ett samlat ansvar inom postområdet och området för elektronisk kommunikation. PTS är en myndighet under Näringsdepartementet. Riksdag och regering styr PTS genom lagar, förordningar, regleringsbrev och samt genom särskilda regeringsuppdrag.

PTS övergripande mål:[1]

1. Fasta och mobila nät är utbyggda så att alla användare kan få tillgång till de tjänster som normalt efterfrågas.
2. Alla användare har tillgång till tillförlitliga post- och grundläggande betaltjänster.
3. Alla användare har tillgång till tillförlitliga och säkra elektroniska kommunikationsnät och -tjänster.
4. Radiospektrum och nummer förvaltas så att samhällsnyttan maximeras över tid.
5. Marknaderna för elektroniska kommunikationer och post kännetecknas av väl fungerande konkurrens med effektiva priser och valmöjlighet för konsumenter.
6. Konsumenter kan känna sig trygga med att deras rättigheter är väl tillgodosedda, och att de kan göra aktiva och välinformerade val.
7. PTS är en välskött myndighet som är nytänkande och en av Sveriges bästa arbetsplatser.

PTS har inom myndighetens ansvarsområde vissa uppgifter enligt krisberedskapsförordningen[2]. Myndigheten ska i enlighet med förordningen bland annat planera och vidta åtgärder för att skapa förmåga att hantera en kris och för att förebygga sårbarheter och motstå hot och risker.

Risk- och sårbarhetsanalysen består av risk- och förmågebedömningar som beskriver på vilket sätt postsektorn och sektorn för elektronisk kommunikation och samhället kan påverkas negativt av olika typer av händelser som t.ex. avbrott i nät och tjänster och brister i informationssäkerheten. Denna analys är begränsad till de fall då denna påverkan kan innebära en stor risk eller fara för befolkningens liv och hälsa, samhällets funktionalitet eller samhällets grundläggande värden.

[1] PTS Verksamhetsplan 2018, PTS-VR-2018:1.
[2] Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap

3 Risk- och sårbarhetsanalys för PTS interna verksamhet

3.1 Beskrivning av arbetsprocess och metod för PTS interna verksamhet

3.1.1 Arbetsprocess - PTS interna verksamhet

Risk- och sårbarhetsanalysen för PTS interna verksamhet är framtagen med stöd av MSB:s analysvägledning[3].

Analysen har avgränsats till de verksamhetsområden och funktioner inom PTS som bedömts kunna ha påverkan på myndighetens arbete reglerat av krisberedskapsförordningen och de identifierade risker som på detta sätt kan ha väsentlig samhällelig påverkan.

3.1.2 Metod - PTS interna verksamhet

PTS risk- och sårbarhetsanalys från 2016[4] innehåller en utförlig beskrivning av tillvägagångssättet för framtagande av myndighetens analys. I den föreliggande analysen har fokus varit på att aktualisera de bedömningar av risker som identifierades i 2016 års analys. Detta arbete har gjorts med utgångspunkt i de riskreducerande åtgärder som PTS vidtagit sedan 2016 och med hänsyn tagen till hotförändringar. Vidare har en förnyad analys av skyddsvärda verksamhetsområden och deras beroenden gjorts för att bedöma om några områden tillkommit eller om tidigare identifierade områden minskat i betydelse.

3.2 Identifierad samhällsviktig verksamhet inom PTS interna verksamhets ansvarsområde som är av nationell/regional betydelse

Analysen av PTS interna verksamhet har avgränsats till de verksamhets-områden och funktioner som bedömts kunna ha påverkan på myndighetens arbete reglerat av krisberedskapsförordningen och de identifierade risker som på detta sätt kan ha väsentlig samhällelig påverkan. Enligt samma förordning har PTS under extraordinära händelser i huvudsak följande två verksamhetsprocesser att upprätthålla:

1. Tillsammans med sina sektorer elektronisk kommunikation respektive post kontinuerligt ta fram en samlad lägesbild för sektorerna,

[3] Vägledning för risk- och sårbarhetsanalyser, MSB, publikationsnummer MSB245.
[4] Dnr. 16-4837

lokalt/regionalt och nationellt och förmedla denna till Näringsdepartementet samt MSB.
2. Stödja och samarbeta med regionala områdesansvariga gentemot sektorerna elektronisk kommunikation respektive post, t.ex. under en återställningsfas i samband med prioritering av resurser.

Ovanstående processer hanteras av PTS krisledningsverksamhet under extraordinära händelser och av funktionen tjänsteman i beredskap (TiB) under mindre störningar. Som stödjande funktioner till nämnda två verksamhetsprocesser finns i viss omfattning myndighetens signalskyddsverksamhet, it-verksamhet respektive verksamhet inom områdena fastighet och dokumentation.

Verksamheterna tillståndsgivning för radiosändare och radiotillsyn är grundstenarna för att åstadkomma och upprätthålla en väl fungerande radiomiljö som tillgodoser samhällets behov av radiokommunikation och därför bedöms dessa verksamheter som samhällsviktiga.

Sammanfattningsvis bedömer PTS att vissa delar av följande interna verksamheter och funktioner är samhällsviktiga:

- PTS krisledningsverksamhet
- PTS funktion för tjänsteman i beredskap
- PTS signalskyddsverksamhet
- PTS verksamhet inom tillståndsgivning för radiosändare och radiotillsyn
- PTS interna stödverksamhet inom it, fastighet och dokumentation

3.3 Identifierade kritiska beroenden för den identifierade samhällsviktiga verksamheten – PTS interna verksamhet

I avsnitt 2.2 beskrivs interna verksamhetsdelar som genom sitt bidrag i de processer som PTS måste upprätthålla under extraordinära händelser bedöms vara samhällsviktiga. Analysen av externa beroenden fokuserar därför på dessa verksamhetsdelar:

De identifierade verksamheterna och funktionerna är beroende av att kunna kommunicera med omvärlden – särskilt med operatörerna då dessa har den information som är nödvändig för att PTS ska kunna skapa och förmedla relevanta och aktuella lägesbilder. Kommunikationen med operatörer inom sektorn för elektronisk kommunikation och andra samverkande parter sker via olika internetbaserade samverkansportaler (t.ex. SOS Alarms webbtjänst

SOS.nu och NTSG-portalen) och med vissa parter kan bilateral kommunikation upprätthållas med hjälp av de tjänster som signalskyddsverksamheten tillhandahåller. Inom postsektorn och för PTS verksamhet inom tillståndsgivning för radiosändare och radiotillsyn sker kommunikationen med operatörerna och tillståndshavarna främst via telefon och e-post. Kommunikationen är alltså externt beroende av kommunikationstjänster (data- och telefonitjänster) samt av fungerande teknisk infrastruktur.

3.4 Identifierade och analyserade hot och risker för PTS interna verksamhet

Nedan beskrivs de oönskade händelser som har identifierats och bedömts som mest relevanta att analysera för PTS interna verksamhet. Urvalet har gjorts dels med ledning av de slutsatser som dragits av inträffade incidenter och dels utifrån de potentiella skadekonsekvenser händelserna har på den interna verksamhet som bedömts som samhällsviktig. Händelser som analyserats är följande:

1. Internetförbindelser ur funktion
2. Elavbrott
3. Informationssäkerhetsförlust

3.4.1 Internetförbindelser ur funktion

De för analysen relevanta direkta skadekonsekvenserna av att PTS internetförbindelser inte är i funktion är att e-post slutar fungera samt att externa tjänster som PTS TiB och krisledning använder inte går att nå från PTS huvudkontor samt att det inte går att fjärruppkoppla från annan ort/placering mot PTS. Under extraordinära händelser kommer därför den samlade nationella lägesbilden att temporärt brista avseende information från sektorerna elektronisk kommunikation och post. De system som är viktiga för att samverka med externa aktörer tillhandahålls dock av andra än PTS och är därför åtkomliga från ställen utanför PTS. Denna omständighet gör att de samhälleliga skadekonsekvenserna av att PTS internetförbindelser inte fungerar bedöms som låga.

PTS har vidtagit rimliga åtgärder för att oönskade händelser som kan sätta PTS internetförbindelser ur funktion motverkas. Dessa åtgärder är inte heltäckande varför vissa risker kvarstår. I huvudsak har följande orsaker till att internetförbindelserna skulle kunna sluta fungera analyserats:

- Kablar blir avgrävda.
- Kablar förstörs genom brand.
- Tekniska fel hos PTS eller hos tjänsteleverantör.

Med hänsyn tagen till vidtagna åtgärder för att motverka oönskade händelser bedömer PTS att sannolikheten för att en avgrävning[5] skulle resultera i att internetförbindelserna slås ut som låg. Givet att även de potentiella skadekonsekvenserna av förlorade internetförbindelser bedöms som låga, blir det sammanvägda riskvärdet lågt.

En (begränsad) brand som förstör kablar[6] bedöms ha låg sannolikhet att resultera i utslagna internetförbindelser givet vidtagna åtgärder för att motverka oönskade händelser. Då de potentiella skadekonsekvenserna av förlorade internetförbindelser bedöms som låga, blir även i detta fall det sammanvägda riskvärdet lågt.

Tekniska fel hos PTS eller hos tjänsteleverantörer kan ha många olika orsaker och är historiskt inte ovanliga och bedöms därför ha hög sannolikhet. De potentiella skadekonsekvenserna av förlorade internetförbindelser bedöms enligt tidigare resonemang som låga och därför blir det resulterande riskvärdet medelhögt.

3.4.2 Elavbrott

I en situation där PTS huvudkontor blir helt utan elförsörjning skulle myndighetens förmåga att kommunicera till och från huvudkontoret med vissa undantag upphöra. Men som i föregående avsnitt redan konstaterats är de system som är viktiga för att samverka med externa parter åtkomliga från ställen utanför PTS. Dessutom har PTS vidtagit åtgärder som gör att myndigheten under begränsad tid kan elförsörja vissa prioriterade system och funktioner även om man drabbas av avbrott i den ordinarie elförsörjningen. Alltså bedöms de samhälleliga skadekonsekvenserna av att PTS tappar elförsörjningen som mycket låga. De oönskade händelser som skulle kunna störa elförsörjningen som har identifierats i analysen avseende PTS interna verksamhet är följande:

- Elförsörjningskablar blir oavsiktligt avgrävda.
- Elförsörjningen saboteras.

Att det pågår olika typer av markarbeten i kvarteren kring PTS huvudkontor är inte ovanligt. Därmed kan elförsörjningskablar skadas eller kapas av misstag. Det har förvisso under de åtta åren som PTS funnits på nuvarande adress inte förekommit skador på elförsörjningskablar p.g.a. markarbeten, men sannolikheten för att elkablar oavsiktligt kan skadas bedöms som medel. Då skadekonsekvenserna av avbrott i den primära elförsörjningen är mycket låga blir den sammanvägda riskbedömningen låg.

[5] Avgrävda kablar är dock i sig inte en ovanlig företeelse.
[6] Bränder i t.ex. försörjningstunnlar är en mer sällan förekommande företeelse än avgrävning.

Att sabotera PTS primära elförsörjning skulle potentiellt kunna resultera i mer svåråterställda skador på elförsörjningen jämfört med en oavsiktlig skada. Det är dock svårt att hitta stöd för att sådana angrepp mot verksamheter av PTS typ förekommit i Sverige, varför sannolikheten för sabotage bedöms vara mycket låg[7]. De samhälleliga skadekonsekvenserna av avbrott i PTS primära elförsörjning är också mycket låga och därför blir den sammanvägda riskbedömningen mycket låg.

3.4.3 Informationssäkerhetsförlust

För att PTS ska kunna upprätthålla förmågan till samhällsviktig verksamhet som krisledning, funktionen PTS TiB samt tillståndsgivning för radiosändare och radiotillsyn, är det viktigt att vissa informationstillgångar[8] är tillgängliga och fungerar som avsett. Informationssäkerhetsförluster, dvs. att informationens konfidentialitet, riktighet eller tillgänglighet inte kan upprätthållas, kan skada PTS krisledningsförmåga, TiB-funktionen och PTS verksamhet inom radiotillstånd och radiotillsyn.

Följande övergripande typer av oönskade händelser som kan resultera i informationssäkerhetsförluster har varit föremål för analys:

- Stöld av it-utrustning
- It-angrepp

För att ta sig in i PTS lokaler i syfte att stjäla it-utrustning kan relativt många olika angreppsmetoder användas. T.ex. kan en angripare försöka göra inbrott, manipulera eller vilseleda PTS-personal samt smita in lokalerna tillsammans med andra inpasserande. PTS bedömer att sammantaget är sannolikheten för stöld av utrustning medel. Om en stöld resulterar i att viss specifik utrustning försvinner (alt. blir förstörd) kan den omedelbara skadekonsekvensen bli att PTS informationshanterings- och kommunikationsförmåga försämras. Denna påverkan bedöms bli kortvarig med hänsyn tagen till PTS åtgärder för att motverka skadekonsekvenser av oönskade händelser[9]. Som tidigare beskrivits är de system som behövs för att samverka med viktiga aktörer tillhandahållna av externa parter och åtkomliga från ställen utanför PTS. Skadekonsekvenserna av utrustningsstöld bedöms därför som mycket låga och därmed blir den sammanvägda riskbedömningen låg.

[7] Denna bedömning gäller sabotage direkt riktat mot PTS verksamhet. Händelser där en verksamhet som finns på samma inkommande elmatning är det primära målet och där sidokonsekvensen blir att även PTS drabbas bedöms inte då detta skulle bli spekulativt.
[8] T.ex. information, informationssystem och datakommunikationssystem.
[9] T.ex. går mycket av utrustningen relativt lätt att ersätta.

It-angrepp ska här tolkas som ett samlingsbegrepp för logiska angrepp mot PTS it-system som kan resultera i informationssäkerhetsförluster, dvs. att informationens konfidentialitet, riktighet eller tillgänglighet inte kan upprätthållas. It-angrepp är ett komplext område som kan karaktäriseras med hjälp av olika egenskaper[10] hos angreppen och angriparna. Att bedöma sannolikheten för att specifika angreppsscenarier ska inträffa riskerar att bli spekulativt. Därför har i den föreliggande riskbedömningen istället graden av potentiella skadekonsekvenser[11] getts ett stort utrymme. Med utgångspunkt i PTS erfarenhet av inträffade it-incidenter och den allmänna utvecklingstrenden avseende it-angrepp har överbelastningsattacker och angrepp med hjälp av skadlig kod valts ut för vidare analys.

De primära skadekonsekvenserna av överbelastningsattacker kan bli att PTS internetförbindelsers funktionalitet tillfälligt försämras eller till och med helt slås ut. Detta skulle i sin tur resultera i att externa tjänster som PTS TiB och krisledning använder inte går att nå från PTS huvudkontor samt att det inte går att fjärruppkoppla från annan ort/placering mot PTS. Med beaktande av de åtgärder PTS vidtagit för att motverka skadekonsekvenser av oönskade händelser och att de system som behövs för att samverka med viktiga aktörer är åtkomliga från ställen utanför PTS, bedöms det samlade riskvärdet som lågt. Det finns många och delvis svårupptäckta sätt att införa skadlig kod i en distribuerad och internetkopplad it-miljö. Skadlig kod kan med rätt kunskap fås att verka dolt under lång tid och kan vara mycket resurs- och tidskrävande att upptäcka, isolera och avlägsna. Det gör att angrepp med hjälp av skadlig kod skulle under relativt lång tid negativt kunna påverka funktionaliteten i stora delar av PTS it-miljö och därmed även möjligheten att nå viktiga samverkanssystem för PTS krisledning och TiB-funktion samt även kunna negativt påverka PTS verksamhet inom tillståndsgivning för radiosändare och radiotillsyn. En ytterligare potentiell skadekonsekvens är att angrepp med skadlig kod skulle kunna resultera i exfiltration av uppgifter som skulle underlätta planläggning av ett angrepp på viktiga samverkans- och verksamhetssystem. Sammantaget bedöms riskvärdet för angrepp med skadlig kod som medelhögt.

[10] Några exempel på egenskaper är om angreppen är riktade eller allmänna, om allmänt kända eller okända sårbarheter används och om angriparen har små eller omfattande angreppsresurser.
[11] Skadekonsekvenser på den interna verksamhet som bedömts som samhällsviktig.

3.5 Bedömning av myndigheten PTS generella krisberedskap

Här bedöms endast PTS egna verksamhets förutsättningar enligt indikatorer som framgår av bilaga i föreskriften MSBFS 2016:7 ”Indikatorer för bedömning av statliga myndigheters generella krisberedskapsförmåga”.

3.5.1 Ledning

Riskhantering

1. Ledningen har fattat beslut om hur arbetet med risk- och sårbarhetsanalys ska bedrivas.
    - **Ja.**
2. Samtliga delar av myndighetens verksamhet beaktas och vid behov involveras i arbetet med risk- och sårbarhetsanalysen.
    - **Ja.**
3. Redovisningen av risk- och sårbarhetsanalysen fastställs av myndighetens ledning.
    - **Ja.**
4. Risk- och sårbarhetsanalysen används som underlag vid planering och beslut om åtgärder för att stärka myndighetens krisberedskap.
    - **Ja.**
5. Relevanta delar av redovisningen från risk- och sårbarhetsanalysen görs tillgänglig för beslutsfattare och anställda inom myndigheten och berörda aktörer inom ansvarsområdet.
    - **Ja**.
6. Det finns en övad och utbildad Tjänsteman i Beredskap (TiB) som har beredskap dygnet runt alla dagar på året.
    - **Ja**.
7. Myndigheten bedriver omvärldsbevakning i syfte att tidigt kunna identifiera och varna för kriser.
    - **Ja**.

Planering

8. Myndigheten har en fastställd plan för hur de ska hantera kriser som beskriver hur myndigheten ska organisera sig under en kris (krishanteringsorganisation), hur myndighetens krishanterings-organisation leder, samordnar, samverkar samt säkerställer samband för att hantera en kris samt vilka lokaler för ledning och samverkan som disponeras vid en kris.
    - **Ja**.

9. Myndighetens planering för att förebygga risker och sårbarheter samt plan för att hantera kriser är framtagen i samverkan med andra aktörer, såväl offentliga som privata.
    - **Ja.**
10. Det finns dokumenterade rutiner för att aktivera krishanteringsorganisationen.
    - **Ja.**
11. Det finns en beslutsordning och mandat för krishanteringsorganisationen.
    - **Ja.**
12. Inom krishanteringsorganisationen finns möjlighet att bedriva: operativ ledning, samverkan, omvärldsbevakning, framtagande av lägesbild, kriskommunikation, analys av händelseutvecklingen av en händelse på kort och lång sikt.
    - **Ja.**
13. Det finns rutiner och planer för att upprätthålla samhällsviktiga verksamheter som myndigheten bedriver eller ansvarar för. *Exempelvis kontinuitetsplaner. De samhällsviktiga verksamheter som myndigheten bedriver eller ansvarar för ska vara beskrivna inom risk och sårbarhetsanalysen.*
    - **Ja.**
14. Planen för hantering av kriser och planerna för att upprätthålla samhällsviktig verksamhet kontrolleras minst en gång per år och revideras vid behov?
    - **Ja, delvis. Vissa planer är äldre än ett år och behöver kontrolleras.**

3.5.2 Samverkan

15. Myndigheten har tagit initiativ till att aktörer inom ansvarsområdet samverkar och uppnår samordning i planerings- och förberedelsearbetet inför hanteringen av kriser.
    - **Ja, för sektorn elektronisk kommunikation.**

16. Myndigheten har fastställda rutiner för att upprätta och förmedla en samlad lägesbild inom myndighetens ansvarsområde avseende kriser.
    - **Ja, för sektorn elektronisk kommunikation.**
17. Myndigheten har fastställda rutiner för deltagande i samverkanskonferenser
    - **Ja.**
18. Myndigheten har fastställda rutiner för att information till allmänheten vid en kris samordnas.

- **Ja**.

3.5.3 Kommunikation

19. Det finns informationskanaler för att ta emot och dela information vid kriser (internt inom myndigheten, till andra krisberedskapsaktörer, och till allmänheten)
    - **Ja.**
20. Det finns alternativa lösningar för att upprätthålla myndighetens prioriterade kommunikation (inom myndigheten, gentemot andra krisberedskapsaktörer, till allmänheten vid inträffad händelse)
    - **Ja.**

3.5.4 Informationssäkerhet

21. Myndigheten hanterar information säkert. Systematiskt säkerhetsarbete bedrivs i enlighet med MSB:s föreskrifter (MSBFS 2009:10) om statliga myndigheters informationssäkerhet.
    - **Ja, systematiken brister dock i vissa delar.**
22. Myndigheten har rutiner för att identifiera och hantera kritiska beroenden till system och tjänster för informationshantering som är av central betydelse för myndighetens verksamhet.
    - **Ja, för samhällsviktiga delar.**
23. Myndigheten ställer krav på informationssäkerhet när informationshantering upphandlas av en extern leverantör.
    - **Ja, där behov av sådana krav finns.**

3.5.5 Kompetens

Utbildning

24. Personalen i krishanteringsorganisationen har utbildning och kännedom om sin och myndighetens roll och ansvar vid en kris.
    - **Ja.**
25. Personalen i krishanteringsorganisation har kännedom om andra relevanta aktörers roller och ansvar vid kriser.
    - **Ja.**

Övning

26. Det finns en utbildnings- och övningsplan för mandatperioden som efterföljs
    - **Ja.**
27. Har myndighetens ledning övats under det gångna året?
    - **Ja.**
28. Har krishanteringsorganisationen övats under det gångna året?

- **Ja.**

29. Har myndigheten under det gångna året deltagit i planering, genomförande eller utvärdering av samverkansövning på lokal, regional och/eller nationell nivå?
    - **Ja.**
30. Har myndigheten utvärderat de övningar som genomförts under det gångna året?
    - **Ja.**
31. Myndigheten har rutiner för att ta till vara erfarenheter från inträffade händelser och övningar
    - **Ja.**

3.5.6 Resurser

32. Myndigheten har en behovsanalys av vilka materiella och personella resurser som krävs för att hantera kriser
    - **Nej, en samlad behovsanalys pågår.**
33. Myndigheten har uppdaterad/aktuell dokumentation rörande vilka interna materiella och personella resurser som finns att tillgå vid en kris
    - **Ja, till viss del.**
34. Det finns rutiner för att genomföra underhåll och kontrollera funktionalitet på de materiella resurserna som endast används vid kriser
    - **Ja, för identifierade resurser. Komplettering kan behövas efter avslutad behovsanalys.**
35. Det finns avtal och/eller överenskommelser med externa aktörer om förstärkningsresurser vid kriser.
    - **Ja, för identifierade behov.**
36. Det finns rutiner för att begära och ta emot förstärkningsresurser (materiella och personella) från externa aktörer (lokala/regionala/nationella/internationella) i samband med kriser.
    - **Ja.**
37. Lokalerna till krishanteringsorganisationen är utrustade och testade avseende åtminstone: a) elförsörjning, med möjlighet till reservkraft-försörjning, till lokaler, arbetsplatser och tekniska system med en uthållighet om minst en vecka; b) it-försörjning; c) tekniska system för kommunikation och samlad lägesbild (t.ex. Rakel och WIS); d) tillgång till vatten för hantering av mat, dryck och hygien som medger uthållighet om minst en vecka.
    - **Ja, i huvudsak (brister finns avseende d).**
38. Det finns utpekad alternativ lokalisering för krishanterings-organisationen.

- **Nej, arbetet med en alternativ lokalisering pågår.**

3.6 Beskrivning av identifierade sårbarheter och brister i krisberedskap inom PTS interna verksamhet

I kapitel 2.4 identifierades ett antal oönskade händelser som om de inträffar skulle kunna resultera i skadekonsekvenser för verksamhetsdelar som PTS bedömt som samhällsviktiga. Riskbedömningarna för de oönskade händelserna har gjorts i ljuset av att PTS vidtagit vissa åtgärder för att motverka att de oönskade händelserna uppstår och för att motverka deras eventuella skadekonsekvenser. I detta kapitel beskrivs kvarvarande systematiska sårbarheter kopplade till händelser som bedömts ha störst riskvärde – dvs. tekniska fel som kan leda till bortfall av internetförbindelser och it-angrepp med skadlig kod.

De system som är nödvändiga för att upprätthålla kontinuitet i PTS internetkommunikation är relativt tekniskt komplexa och ställer höga krav på korrekt handhavande för att avsedd funktionalitet ska uppnås. PTS är beroendet av extern expertis för att detta ska uppnås och därmed bedöms PTS egen förmåga vara begränsad.

Som tidigare beskrivits finns det många sätt att införa skadlig kod på i en distribuerad och internetkopplad it-miljö. De åtgärder PTS vidtagit för att skydda olika komponenter i it-miljön mot angrepp med skadlig kod bedöms ge ett välanpassat skydd, men det finns vissa it-arkitekturrelaterade sårbarheter som gör att förmågan att begränsa spridningen av skadlig kod vid ett eventuellt angrepp bedöms som otillräcklig.

3.7 Genomförda, pågående och planerade åtgärder sedan föregående rapportering PTS interna verksamhet

PTS arbetar kontinuerligt med att utvärdera och förbättra myndighetens samhällsviktiga verksamheter och därtill hörande stödverksamheter. PTS genomför bland annat följande åtgärder som bedöms bidra till att minska sårbarheter i PTS samhällsviktiga verksamhetsdelar:

- Utredning av PTS krishanteringsarbete i samband med skogsbränderna sommaren 2018
- Översyn av PTS krisplan
- Planering och genomförande av interna krisövningar
- Planering för inrättande av alternativ ledningsplats

- Förstudie inför förnyande av PTS it-infrastruktur
- Förbättring av PTS fysiska skydd
- Utökning av PTS signalskyddsorganisation
- Ökad informationssäkerhet för vissa verksamhetssystem

4 Risk- och sårbarhetsanalys för postsektorn

Gällande postsektorn har PTS följande uppgifter enligt 2 § förordning (2007:951) med instruktion för Post- och telestyrelsen:

1. *främja att en väl fungerande samhällsomfattande posttjänst av god kvalitet finns tillgänglig för alla användare enligt de mål som anges i postlagen (2010:1045),*
2. *fortlöpande följa utvecklingen och bevaka att posttjänsterna svarar mot samhällets behov,*
3. *främja en effektiv konkurrens,*
4. *övervaka prisutvecklingen,*
5. *pröva frågor om tillstånd och utöva tillsyn enligt postlagen, och*
6. *meddela föreskrifter enligt postförordningen (2010:1049).*

Med samhällsomfattande posttjänst i första punkten avses:

en posttjänst som ska finnas i hela landet, som är av god kvalitet och som innebär att alla användare kan ta emot postförsändelser och till rimliga priser för befordran kan avlämna sådana försändelser.[12]

För att se till att en sådan posttjänst finns, har PTS ålagt PostNord Group AB att tillhandahålla den samhällsomfattande posttjänsten. Bolaget har i sin tur överlåtit åt dotterbolaget PostNord Sverige AB att tillhandahålla kommunikationstjänster för företags- och privatmarknaderna i Sverige. I rapporten är PostNord Sverige AB ofta refererad till som postoperatören.

4.1 Beskrivning av arbetsprocess och metod för postsektorn

4.1.1 Arbetsprocess - Postsektorn

Arbetet med risk-och sårbarhetsanalysen för postsektorn har följt en process som tar sin utgångspunkt i standarden ISO 22 301 (Kontinuitetshantering), anpassat till de krav som följer av Myndigheten för samhällsskydd och beredskaps (MSB) föreskrifter om RSA. Den redovisade analysen för postsektorn bygger till del på ett omfattande internt arbete avseende kontinuitetshantering som genomförts av Postnord under de senaste åren.

Det är genom den samhällsomfattande posttjänsten som landets behov av posttjänster ska tillgodoses. Risk- och sårbarhetsanalysen för postsektorn avgränsas därför till den postoperatör som är ålagd att tillhandahålla den samhällsomfattande posttjänsten, Postnord. Inga andra operatörer har därför analyserats. Därutöver har analysen också avgränsats till den verksamhet som enligt postlagen omfattas av den samhällsomfattande posttjänsten, ytterligare

[12] Postlag (2010:1045)

beskriven i tidigare kapitel 1. Operatören tillhandahåller ett stort antal övriga tjänster som inte omfattas av den samhällsomfattande posttjänsten och därmed inte heller tas upp i denna risk- och sårbarhetsanalys, (t ex pakettjänster för försändelser över 20 kg)

Operatören har initierat och under 2018 delvis slutfört ett omfattande arbete kopplat till kontinuitetshantering för de viktigaste processerna. Arbetet kopplat till ”Producera Tjänst (Brev)” och ”Producera Tjänst (Paket)” är slutfört och resultatet av detta arbete har nyttjats i denna analys.

Operatörens verksamhet för att tillhandahålla den samhällsomfattande post-tjänsten har kartlagts utifrån dennes kritiska processer, kritiska aktiviteter, kritiska resurser och externa beroenden. I den här rapporten ligger fokus på dessa processer och dess ingående huvudaktiviteter – i det följande benämnt ”den samhällsomfattande posttjänsten”. Hot och risker har analyserats per kritisk resurs utifrån sannolikhet och hur allvarliga konsekvenserna skulle bli enligt bedömningsgrunder beskrivna i kapitel 3.3. Av uppenbara skäl har alla detaljer i den av operatören gjorda analysen inte fullt ut redovisats utan har i flera fall aggregerats till en högre nivå. Detta har dock inte påverkat de i rapporten redovisade huvudslutsatserna.

Vissa hot, risker och konsekvenser har generaliserats i texten då dessa inte ska komma till allmän kännedom. Analysen har dock genomförts utan hänsyn till generaliseringen och de övergripande slutsatserna har inte påverkats därav.

4.1.2 Metod - Postsektorn

Data har samlats in genom en kombination av dokumentstudier, intervjuer och workshops. I det arbetet har relevant kompetens främst från operatören men även från PTS involverats. Insamlat material har därefter analyserats och vid behov kompletterats med ytterligare datainsamling. Resultatet har slutligen verifierats av operatören.

4.2 Identifierad samhällsviktig verksamhet inom myndighetens ansvarsområde som är av nationell/regional betydelse för postsektorn

Sedan år 1636 har en rikstäckande posttjänst funnits inom Sverige, ursprungligen genom Postverket och sedan avregleringen 1993 genom flera konkurrerande postoperatörer. Idag bedrivs postverksamhet av ett trettiotal aktörer inom olika geografiska områden. Av aktörerna är det endast Postnord som i tillståndsvillkoren har ålagts att tillhandahålla den samhällsomfattande posttjänsten enligt 3 kap. 1 och 2 §§ postlagen. Tillståndsvillkor med skyldighet

att svara för den samhällsomfattande posttjänsten utfärdas av PTS för två år i taget.

PTS är bevakningsansvarig myndighet för såväl postsektorn som sektorn elektronisk kommunikation enligt förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap[13]. Däremot framgår det inte om den samhällsomfattande posttjänsten utgör samhällsviktig verksamhet.

I den nationella strategin för skydd av samhällsviktig verksamhet, *Ett fungerande samhälle i en föränderlig värld*, definieras samhällsviktig verksamhet som:

en samhällsfunktion av sådan betydelse att ett bortfall av eller en svår störning i funktionen skulle innebära stor risk eller fara för befolkningens liv och hälsa, samhällets funktionalitet eller samhällets grundläggande värden. [14]

Det råder en oklarhet i hur stor grad samhällets funktionalitet påverkas av en allvarlig störning i förmedlingen av postförsändelser. PTS kan konstatera att ett flertal andra samhällsviktiga verksamheter såsom finansiella tjänster, handel, hälso- och sjukvård, omsorg, offentlig förvaltning samt socialförsäkringar dagligen använder sig av de tjänster som den samhällsomfattande posttjänsten förmedlar. Men vilka effekter en allvarlig störning skulle få på dessa verksamheter är i dagsläget fortfarande inte klarlagt.

Analysen har tagit sin utgångspunkt i de krav som ställs på den samhällsomfattande posttjänstens omfattning. Allvarliga eller mycket allvarliga störningar i dessa har antagits vara sådana som skulle kunna resultera i störningar hos annan samhällsviktig verksamhet. Kraven på omfattning beskrivs nedan, samt den bedömningsgrund som tagits fram utifrån dessa krav.

Den samhällsomfattande posttjänsten definieras i kapitel 1 i postlagen. I 3 kap 1 § postlagen ställs också ett antal krav gällande dess omfattning. Kraven som ska uppfyllas är att:

1. det varje arbetsdag och minst fem dagar i veckan, utom under omständigheter eller geografiska förhållanden som tillståndsmyndigheten bedömer utgör skäl för undantag, ska göras minst en insamling och minst en utdelning av postförsändelser,
2. expeditions- och inlämningsställena ska ligga så tätt att användarnas behov beaktas,

[13] Se även Förordning (2007:951) med instruktion för Post- och telestyrelsen
[14] Ett fungerande samhälle i en föränderlig värld: Nationell strategi för skydd av samhällsviktig verksamhet. Publ.nr: MSB266 – december 2011. ISBN: 978-91-7383-137-6

3. de bestämmelser om befordringstider efterlevs, som meddelats av regeringen eller den myndighet som regeringen bestämmer,
4. det ska vara möjligt att försäkra postförsändelser och att få kvitto från mottagaren på att en postförsändelse har tagits emot,
5. enstaka postförsändelser ska befordras till enhetliga priser, och
6. villkoren för tjänsten ska vara allmänt tillgängliga.

Med postförsändelser avses:

en adresserad försändelse som väger högst 20 kg och som överlämnas i den slutliga form i vilken den ska transporteras av en tillhandahållare av posttjänster[15]

Med brev avses:

en adresserad försändelse som är innesluten i kuvert eller annat omslag och som väger högst 2 kg samt vykort, brevkort och liknande försändelser[16]

Paket definieras inte i postlagen utan anses i denna analys vara postförsändelser med en vikt mellan 2 och 20 kg. Det som kännetecknar paket är att de är spårbara och därmed kan följas av mottagaren eller avsändaren under distributionen[17].

För gällande leveranstider och övernattbefordran trädde förändringar i postförordningen i kraft 1 april 2018 som för inrikes brev innebär att:

Den samhällsomfattande posttjänstens befordringskrav för brev med normalporto ändras från övernattbefordran till tvådagarsbefordran. Minst 95 procent av de inrikes brev som lämnas in för tvådagarsbefordran ska ha delats ut inom två arbetsdagar, oavsett var i landet breven har lämnats in.

Utöver kraven i postlagen och postförordningen ställs i tillståndsvillkoren[18] för Postnord ett antal specifika krav knutna till punkterna ovan samtidigt som ytterligare aspekter om integritet och säkerhet tas upp. Dessa krav har legat till grund till utformningen av den bedömningsgrund som använts i analysen.

Bedömningsgrund

I avsaknad av kunskap om andra samhällsviktiga verksamheters beroenden av den samhällsomfattande posttjänsten har all analys i denna rapport genomförts utifrån följande fyra kriterier:

1. behov av in- och utlämning av försändelser tillgodoses,

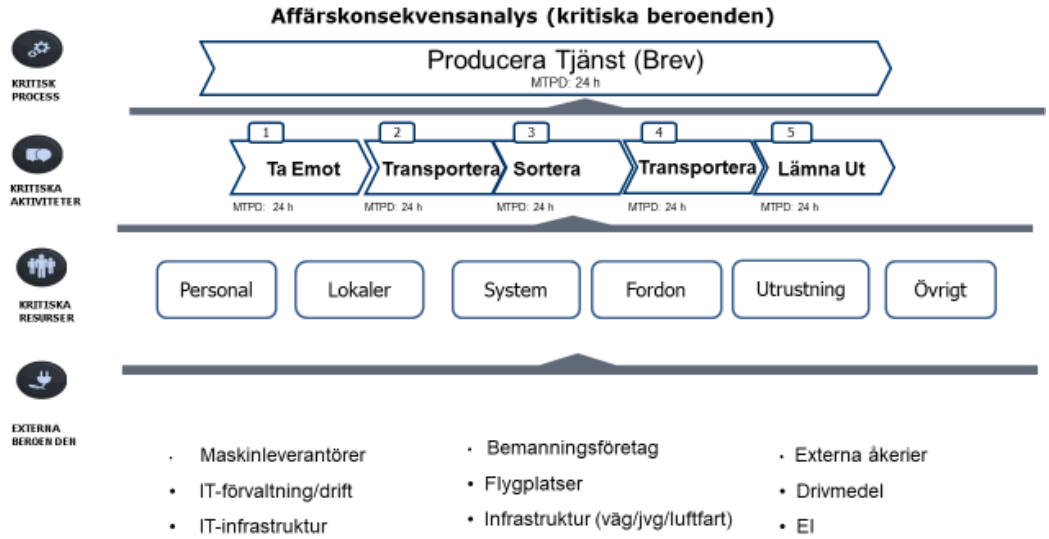
[15] Postlagen (2010:1045)
[16] Postlagen (2010:1045)
[17] Prop. 2017/18:41
[18] Beslut om tillståndsvillkor för Postnord Group AB, Dnr 17-3548

2. försändelser befordras inom erforderlig tid,
3. försändelser kommer fram utan skador, och
4. försändelser exponeras ej för obehöriga.

Bedömningsgrunden bygger på de krav och förväntningar på postsektorn som PTS anser rimliga utifrån postlagen och postförordningen. Hänsyn har dock även tagits till operatörens affärsmässiga åtaganden samt organisationens förmåga att hantera effekterna av avbrott överstigande 24 timmar (internt krav Postnord). Identifiering av kritiska beroenden och värdering av hot, risker och sårbarheter har gjorts utifrån hur allvarliga konsekvenserna bedöms bli för varje kriterium.

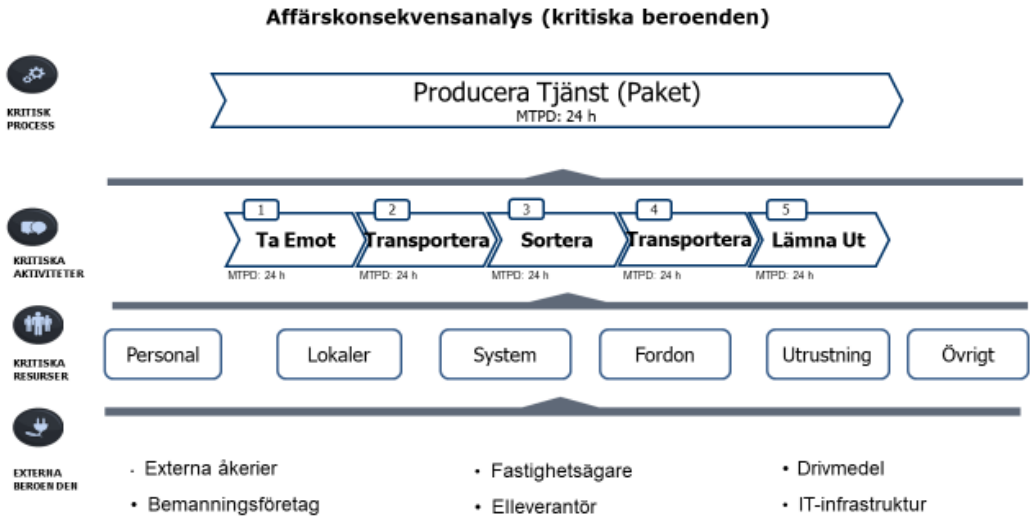
4.3 Identifierade kritiska beroenden för den identifierade samhällsviktiga verksamheten inom Postsektorn

Operatörens verksamhet för att tillhandahålla den samhällsomfattande post-tjänsten har kartlagts utifrån en modell uppdelad i fyra nivåer; kritisk process, kritiska aktiviteter, kritiska resurser som krävs för att utföra aktiviteterna samt externa beroenden som aktiviteter och/eller resurser är beroende av. Figur 1 beskriver utifrån dessa fyra nivåer de grundläggande förutsättningarna för att den samhällsomfattande posttjänsten för att ta emot och skicka brev – i bilden benämnd ”Producera Tjänst (Brev)” ska fungera.



Figur 1 Kritiska processer, aktiviteter, resurser och beroenden för den samhällsomfattande tjänsten för brev

Figur 2 beskriver utifrån dessa fyra nivåer de grundläggande förutsättningarna för att den samhällsomfattande posttjänsten för att ta emot och skicka försändelser upp till 20 kilo – i bilden benämnd ”Producera Tjänst (Paket)” ska fungera. Aktiviteterna och resurskategorierna beskrivs övergripande i tabell 1 och tabell 2.



Figur 2 Kritiska processer, aktiviteter, resurser och beroenden för den samhällsomfattande tjänsten för paket

Tabell 1 Kritiska aktiviteter, förklaring

Kritisk aktivitet	Beskrivning
Ta emot (1)	Aktiviteten består av de delaktiviteter som behövs för att samla in alla postförsändelser. Detta sker via brevlådor, företagscenter och postombud men kan även ske direkt på ett brevbärarkontor eller genom att försändelser hämtas direkt ute hos kunden.
Transportera (2)	Denna aktivitet innefattar uppsamlingstransporten mellan att postförsändelsen tagits emot till att den når en terminal för vidare sortering. Posten ankommer till spridande brevterminal med transporter via flyg, tåg eller lastbil.
Sortera (3)	Aktiviteten omfattar uppsamlingssortering och spridningssortering. Uppsamlingssortering innefattar en grovsortering av alla postförsändelser från ett geografiskt

	område för att dessa ska kunna transporteras vidare till rätt geografiska område för utdelning. Sker på uppsamlande brevterminal. Spridningssorteringen sorterar alla postförsändelser per mottagare varefter försändelserna transporteras till respektive brevbärarkontor för utdelning. I aktiviteten spridningssortering görs en finsortering av postförsändelser inom ett geografiskt område.
Transportera (4)	Denna aktivitet består av rikstransport, som är en del av sorteringen, och spridningstransport.
Lämna ut (5)	Aktiviteten inkluderar utdelningen av alla postförsändelser från ett brevbärarkontor till ett postombud, företagscenter, brevlåda eller direkt till privata postlådor eller företag.

Tabell 2 Kritiska resurskategorier, förklaring

Kritiska resurskategorier	Beskrivning
Personal	Resurskategorin inkluderar samtlig personal på terminaler, på brevbärarkontor, vid transport eller hos postombud.
Lokaler	Lokaler utgörs av fasta lokaler och terminaler för mottagning, sortering och utdelning av postförsändelser, t.ex. brev- och paketterminaler, brevbärarkontor, företagscenter (FC) och brevlådor samt övriga postombud som tillhandahåller in- eller utlämning men som inte ingår i Postnord Sverige AB.
System	De mjukvarusystem som används för hantering, sortering, etc. av postförsändelser. Inkluderar både postoperatörens system samt de system som tredje parts postombud använder och som tillhandahålls av postoperatören.
Fordon	Samtliga fordon för transport av postförsändelser, både vid inhämtning, transport mellan terminaler samt vid utdelning. Både operatörens egna fordon samt fordon tillhörande entreprenörer ingår i denna kategori.
Utrustning	Resurskategorin inkluderar maskiner för exempelvis sortering av postförsändelser och vägning samt av reservaggregat och andra utrustningsresurser.
Övrigt	Kategorin ”Övrigt” innefattar exempelvis nycklar, printar, brevlådor och lastbärare.

4.4 Identifierade och analyserade hot och risker för postsektorn

Det finns flertalet hot som kan påverka den samhällsomfattande posttjänstens funktion genom dess beroende av kritiska resurser.

4.4.1 Sårbarhet per aktivitet

Aktiviteterna ”Ta emot” (1) och ”Lämna ut” (5) utgörs av den verksamhet som krävs för att samla in eller dela ut postförsändelser till och från olika inhämtnings- och utdelningsställen såsom postombud, brevlådor, postlådor, företagscenter och kunder. Båda aktiviteterna är till stor del beroende av samma resurser även om ingående delaktiviteter skiljer sig åt. Navet är vanligtvis det lokala brevbärarkontoret, varifrån post antingen anländer från eller skickas vidare till en terminal. Sårbarheterna i dessa två aktiviteter hanteras tillsammans.

Uppsamlings- och spridningssortering, under aktiviteten ”Sortera” (3), sker på olika brevterminaler runt om i Sverige. Båda aktiviteterna är till stor del beroende av samma resurser även om ingående delaktiviteter skiljer sig åt. Uppsamlingssortering syftar till att i ett första steg göra en grovsortering; att sortera brev från ett geografiskt område till ett annat, och vid spridningssortering en finfördelning; sortera försändelserna till respektive brevbärarkontor/mottagare. Sortering sker vanligtvis maskinellt och är starkt beroende av tillgång till terminalerna och deras maskiner. Sårbarheterna i dessa två aktiviteter hanteras tillsammans.

Aktiviteterna ”Transportera” (2 och 4) sker mellan inlämningsställe och terminal, mellan terminaler och mellan terminal och utlämningsställe. Aktiviteterna är beroende av till stor del samma resurser och sårbarheterna hanteras således tillsammans.

”Ta emot” och ”Lämna ut”

”Ta emot” och ”Lämna ut” är två decentraliserade aktiviteter och därmed inte särskilt sårbara för händelser. Anledningen är det stora antal in- och utlämningsställen som finns vilket skapar en redundans genom att det finns alternativa platser att lämna in och hämta postförsändelser. Vissa händelser kan naturligtvis påverka redan inlämnade försändelser och/eller ej uthämtade försändelser men detta ger endast en liten konsekvens för samhället.

Det krävs att ett större område drabbas för att störningar i ”Ta emot” och ”Lämna ut” ska få stora konsekvenser för samhället. Om störningen begränsas till ett mindre område kan antingen operatören eller operatören tillsammans

med kunden ändå sköta kritiska ärenden medan mindre kritiska ärenden får vänta utan att allvarliga konsekvenser uppstår.

Utöver att störningen drabbar ett större område krävs även att den är tämligen utsträckt i tid för att konsekvenserna ska bli allvarliga. Det finns stora möjligheter att ta igen förlorad tid genom övertid hos ordinarie personal, extrainkallad personal och genom att vid behov nedprioritera mindre brådskande leveranser.

En stor del av in- och utlämning av postförsändelser innefattar att försändelser registreras i mjukvara vars drift sköts av operatörens underleverantörer vilket medför att en störning i denna mjukvara, elförsörjningen eller i den elektroniska kommunikationen i sin tur skulle kunna medföra störningar på regional eller nationell nivå. Även om det finns manuella rutiner för de fall då mjukvaran inte fungerar som den ska, skulle det innebära leveransförseningar, ökad arbetsbelastning och delvis inskränkta möjligheter till in- och utlämning. För att minska sårbarheten på detta område finns virusprogram, brandväggar etc. på plats samtidigt som driften av kritisk mjukvara är redundant uppsatt bl.a. genom dubblerade system på geografiskt separerade platser. Anpassade servicenivåer (Service Level Agreements – ”SLA”) finns för samtliga system och även med leverantören av elektronisk kommunikation. Hittills har ingen störning av allvarlig omfattning inträffat på detta område varför risken bedöms som liten även om konsekvenserna skulle kunna bli omfattande.

Ett strömavbrott i en större del av landet skulle leda till allvarliga konsekvenser och här finns det för postombud, företagscenter och brevbärarkontor ofta ingen redundans i form av reservkraft. Baserat på tidigare inträffade ström-avbrott i Sverige bedöms dock risken för ett sådant omfattande strömavbrott, i utbredning och tid, som låg. Dessutom finns beredskapen att hantera, hämta in och dela ut postförsändelser genom manuell hantering, både på operatörens egna anläggningar och hos postombuden.

Att omfattande personalbrist samtidigt skulle uppstå på ett så stort antal post-ombud, företagscenter eller brevbärarkontor att omfördelning av personal eller inkallning av extrapersonal inte skulle räcka för att hantera situationen har aldrig inträffat. En pandemi eller strejk skulle dock kunna medföra sådana konsekvenser. Trots att risken är låg finns det hos operatören beredskapsplaner, innefattande bland annat redundans via bemanningsföretag, framtagna och möjligheten finns att prioritera vilka anläggningar som ska användas.

Slutligen, skulle en nationell brist på drivmedel uppstå skulle det för operatören också kunna innebära en allvarlig störning i inhämtning och utdelning av postförsändelser. Ingen direkt redundans eller beredskap finns för sådana omständigheter men sannolikheten för att det ska inträffa bedöms vara låg. Om en nationell drivmedelsbrist ändå uppstår kommer troligen ransonerings- och prioriteringsåtgärder från statens sida inrättas varvid posttjänsten förhoppningsvis inkluderas i denna prioritering.

Sammanfattningsvis bedöms aktiviteterna ”Ta emot” och ”Lämna ut” vara robusta och ha en låg sårbarhet. Detta framförallt då riskerna för att tillräckligt stora störningar ska inträffa är små samtidigt som möjligheterna att trots störningar hantera försändelser är goda.

”Sortera”

Uppsamlings- och spridningssortering genomförs vid 15 stycken terminaler varav nio är för brev och sex är för paket. Trots att sortering utförs vid ett flertal platser är sorteringsprocesserna mer sårbara än aktiviteterna för inhämtning och utdelning som utgår ifrån en betydligt större mängd brevbärarkontor, företagscenter, postombud m.m. Eftersom stora mängder postförsändelser hanteras på terminalerna kan störningar för en enskild terminal innebära stora konsekvenser framförallt på kort sikt innan omdirigering till annan terminal kan genomföras.

De olika terminalerna skiljer sig åt främst beroende både på var de är belägna och vilken sorts försändelser de hanterar. Vissa terminaler som betjänar storstadsområdena eller ligger strategiskt utifrån transportnätets uppbyggnad hanterar mycket större kvantiteter än andra. Generellt kan sägas att om en störning drabbar en enskild terminal finns det dels manuella rutiner för att snabbt fortsätta med pågående hantering och sortering, dels åtgärder i form av att andra terminaler kan överta postförsändelser. Vid behov kan post-försändelser från en drabbad terminal spridas till flera andra terminaler som istället hanterar och sorterar försändelserna. Sådan omfördelning kan fortfarande innebära förseningar i befordran men bör inte innebära några andra konsekvenser.

Gällande specifika risker är de som kan resultera i elavbrott eller störningar i elektronisk kommunikation också de som får de mest omfattande konsekvenserna. Sannolikheten att sådana risker inträffar är förhållandevis hög vilket innebär att förmågan att hantera uppkomna störningar är avgörande för vilka konsekvenserna blir. Samtliga brevterminaler är därför utrustade med avbrottsfri kraft genom ”uninterruptible power supply” (UPS) och reservkraftaggregat vilka försörjer de produktionskritiska systemen och därmed

minimerar sårbarheten för elavbrott betydligt. Däremot finns inte samma robusthet vad gäller reservkraft på paketterminalerna. Därmed är dessa terminaler mer sårbara för störningar i elförsörjningen.

Avbrott i elektronisk kommunikation samt fel i mjukvara och hårdvara kan bero på risker som slår på ett lokalt, regionalt eller nationellt plan. Konsekvenserna vid dessa typer av avbrott kan i vissa fall bli allvarliga då flera terminaler riskerar att drabbas. Av denna anledning finns det en god redundans för dessa typer av händelser. Exempelvis finns de mest kritiska systemen för brevsortering lokalt på respektive terminal och mycket av sorteringen kan ske även utan tillgång till uppdaterad data. Varje terminal har också redundanta kommunikationssystem i form av flera tekniska lösningar för elektronisk kommunikation så att en lösning ska fungera även om den andra går ner. Dock tillhandahålls all kommunikation av samma leverantör vilket innebär en något sårbar leverantörssituation. Vid ett omfattande avbrott sker en omfördelning till andra terminaler.

Brand skulle kunna leda till att stora mängder försändelser skadas eller förstörs men det bedöms att operatören har ett bra brandskydd på terminalerna. Risken för att en brand ska uppstå och allvarligt sprida sig ses som liten. Större risk finns för att en brand orsakar skada på sorteringsmaskinerna vilket därmed innebär avbrott i sorteringen. En sådan störning finns det dock möjlighet att hantera genom de alternativa rutinerna som beskrivs ovan.

Risken för inbrott bedöms i huvudsak bero på hur värdefulla eller känsliga försändelserna är som skickas via terminalen. Postrån är idag ovanliga och senast det inträffade var 2008 då ett större rån mot brevterminalen i Göteborg genomfördes. Operatören har vidtagit flera åtgärder för att minska risken för inbrott och rån dock kan detta ändå ske. Konsekvenser på grund av inbrott som innebär att stora kvantiteter försändelser skadas eller exponeras för obehöriga kan därför inte uteslutas.

I avsnittets inledning konstaterades att sorteringsprocesserna är mycket beroende av terminalernas maskiner. Förutom de risker som beskrivits ovan vilka bland annat kan drabba maskiner finns ett antal risker som mer ensidigt drabbar maskiner. Där inberäknas givetvis rena fel på maskiner men även fel på den mjukvara maskinerna använder och de elektroniska kommunikationer som används för att skicka korrekt information till och från maskinerna.

Att maskinfel uppstår på terminalerna kan knappast undvikas men däremot bör dess omfattning och konsekvenser begränsas. Operatören har därför också vidtagit riskreducerande åtgärder i form av att teknisk kompetens finns på plats

och ytterligare kompetens kan även avropas, att reservdelar finns att tillgå och att sorteringen till viss grad kan anpassas efter uppkomna fel. Sannolikheten för att ett maskinfel ska leda till en allvarlig störning är därför låg men existerande. En maskinutbytesplan inleddes 2013 och ska avslutas under 2018. Delar av maskinparken är utbytt men inte i den omfattning som planerades 2013. Åtgärden bör minska risken för olika former av driftstörningar kopplade till maskinparken.

Då störningar vid en *enskild* anläggning kan få allvarliga konsekvenser för sorteringsaktiviteterna hos operatören är dessa även något mer sårbara för personalrelaterade risker. Risken för att en stor del av personalen eller specifik nyckelpersonal vid en enskild terminal blir sjuk är större då det rör sig om en avgränsad personalstyrka, som lättare kan drabbas av till exempel dricksvatten-störningar eller oväder som hindrar personalen att ta sig till arbetsplatsen. Med färre terminaler minskas möjligheten till, och beredskapen för, omfördelning av både personal och försändelser.

Sammanfattningsvis bedöms aktiviteterna för uppsamlings- och spridningssortering vara robusta trots vissa sårbarheter. Framförallt är det nätet av terminaler som skapar en god redundans med god förmåga att hantera händelser utan stora konsekvenser för samhället.

”Transportera”

Den omfattande transporten mellan uppsamlande och spridande brevterminaler sker via lastbil, tåg eller flyg. Transporten är, förutom ett signifikant mjukvaruberoende, även starkt beroende av kritisk infrastruktur samt beroende av underleverantörer som utför en stor del av de fysiska transporterna.

Transporten är viktig för att all post ska kunna sorteras och skickas till rätt geografisk terminal över hela Sverige, varför den är kritisk och en störning i denna skulle snabbt kunna få stora konsekvenser. Störningar – speciellt relaterat till tåg och flygtransporter - på regional nivå kan snabbt få nationella konsekvenser eftersom en regional störning kan medföra att tidtabeller inte hålls vilket i sin tur ger följdeffekter. Eftersom just transporten mellan terminaler bedöms som extra kritisk ges detta område extra utrymme i denna risk- och sårbarhetsanalys.

Väderstörningar kan påverka både ett mindre geografiskt område eller ett större om en storm eller kraftigt snöoväder drar in över landet. Även om ett mindre geografiskt område är drabbat av oväder, eller skador på infra-strukturen som påverkar transporterna till och från en terminal, medför det att

ett stort antal försändelser inte kan transporteras vidare till sortering och därför inte kan befordras inom rätt tid. Ifall väderstörningen enbart drabbar ett specifikt trafikslag, som exempelvis ett askmoln som drabbar flyget, finns goda möjligheter att omfördela försändelserna till andra transportslag. Om det drabbar en enskild region finns ofta möjlighet att skicka försändelser till andra terminaler. Om en störning eller försening inträffar under natten har operatören en uppbyggd robusthet genom att transportledningen har mandat och kunskap att hantera alla händelser initialt. Under kontorstid finns givetvis ytterligare personal som kan arbeta med att mildra konsekvenserna av uppkomna störningar.

Förutom väderlek är även transporterna starkt beroende av den kritiska infrastrukturen i Sverige. Redundans för att hantera störningar på järnvägen eller på flygplatser säkerställs genom att använda alternativa transportmedel eller genom att transportera försändelserna till alternativa terminaler. För störningar som uppkommer under exempelvis pågående tågtransport är dock möjligheterna till kontinuitetslösningar mer begränsade.

För att skydda mot inbrott, stöld och dylikt finns skalskydd på samtliga transportfordon samt rutiner och särskild behörighet för att transportera eller köra vissa försändelser. Säkerhetsrutiner, beredskapsplaner och omvärlds-bevakning hanterar eventuella specifika hot mot operatören, dess personal och dess försändelser.

Då transporterna styrs via mjukvarusystem vars drift sköts av operatörens underleverantörer, skulle en störning i denna mjukvara, eller i den elektroniska kommunikationen också kunna innebära störningar på både regional och nationell nivå. Även om det finns manuella rutiner för att hantera att mjukvara inte fungerar skulle det kunna innebära förseningar eller fel-transporter vilket skulle få konsekvenser för vidare sortering eller transport då tidtabeller inte hålls. Sårbarheten minskas dock av de riskreducerande åtgärder gällande mjukvara och elektronisk kommunikation som redan nämnts under aktiviteterna ”Ta emot” och ”Lämna ut”.

Flygtransporter kan drabbas av internationella händelser och beslut såsom flygförbud för speciella flygplanstyper. En liten men reell risk existerar samtidigt som det finns viss redundans genom att flera olika flygplanstyper används samtidigt som omdirigering av försändelser till andra transportsätt kan ske.

Brister i drivmedelsförsörjningen regionalt eller nationellt skulle också innebära ett problem men skulle först och främst hanteras genom att omdirigera försändelser till tågtransport. Som tidigare nämnts bedöms dock sannolikheten för att detta skulle inträffa som liten, och i den händelse att det ändå inträffar och i den omfattningen att det skulle få stora konsekvenser för den samhällsomfattande posttjänsten, så är det troligt att staten skulle besluta om konsekvenslindrande ransonerings- och/eller prioriteringsåtgärder.

En pandemi eller en strejk skulle kunna medföra att transporter drabbas av personalbrist vilket i sin tur kan leda till förseningar i leveranser. Beroende på vilka som omfattas av en strejk finns möjligheten att använda andra transportmedel. Då beroendet av nyckelpersonal inom t ex transportledningen är stort är riskerna för personalbrist stor i den här delen av verksamheten jämfört med andra delar. Enskilda regioner kan dock själva hantera mindre problem och vid större eller långvariga störningar kan nationell krisledning kallas in.

Under senare tid kan det konstateras att det finns risk för en nationell brist på chaufförer då behovet av denna kompetens ständigt ökar. Operatören följer denna utveckling och analys pågår avseende konsekvenser och möjliga lösningar.

Transporterna är sammanfattningsvis robusta då det finns en stor redundans i form av möjligheten att kunna använda alternativa transportmedel samt möjlighet att omdirigera försändelser till andra, icke-drabbade terminaler och områden. Sannolikheterna för riskerna inom transporter bedöms dock högre än för de andra aktiviteterna, varför aktiviteten ”Transporter” kan ses som den mest sårbara. Operatören bedömer att initialt kommer den operativa förmågan att sänkas speciellt under den första dagen av störningen. Därefter räknar man med att kunna komma åter till normal operativ nivå.

4.5 Beskrivning av identifierade sårbarheter och brister i krisberedskap för postsektorn

Operatören bedöms ha god förmåga att hantera störningar på lokal och regional nivå. De sårbarheter som har identifierats omfattar framförallt nationella störningar inom elektronisk kommunikation, elförsörjning och drivmedelsförsörjning. Dessa typer av störningar är framförallt kopplade mot höjd beredskap och men bör även stödjas av normala krisberedskapsåtgärder hos operatören.

Det kan konstateras att:

- operatörens förmåga att upprätthålla den samhällsomfattande posttjänsten vid en *nationell* störning i elektroniska kommunikationer med stor sannolikhet skulle påverkas. Detta beror främst på att verksamheten vid enskild terminal påverkas samtidigt som möjligheten att omfördela postförsändelser till andra terminaler försvinner helt eller delvis. Verksamheten vid terminalerna kan dock till del upprätthållas men i begränsad omfattning.
- operatörens förmåga att upprätthålla den samhällsomfattande posttjänsten vid en *nationell* störning i elförsörjningen med stor sannolikhet skulle påverkas. Detta beror främst på att verksamheten vid enskild terminal påverkas samtidigt som möjligheten att omfördela postförsändelser till andra terminaler försvinner. Brevförsändelser påverkas mindre än övriga postförsändelser då dessa terminaler har fast installerad reservkraft.
- operatörens förmåga att upprätthålla den samhällsomfattande posttjänsten vid en *nationell* drivmedelsbrist kan påverkas. Detta beror främst på att operatören är beroende av fordon för att upprätthålla sin verksamhet. Konsekvenserna av en nationell drivmedelsbrist är dock mindre i jämförelse med nationella störningar i elektronisk kommunikation och elförsörjning då det dels finns möjlighet till omfördelning till andra trafikslag, dels är det troligt att staten inför ransonerings- och/eller prioriteringsåtgärder där operatören förhoppningsvis blir prioriterad.

4.6 Genomförda, pågående och planerade åtgärder sedan föregående rapportering för postsektorn

Utifrån av operatören genomförd kontinuitetsplanering har ett antal åtgärdsförslag identifierats vilka skulle förbättra och/eller säkerställa den samhällsomfattande posttjänstens förmåga att hantera kriser och störningar. Några av åtgärdsförslagen har PTS eller operatören redan planerat att vidta medan övriga föreligger för dialog både internt och externt med operatören och eventuella övriga parter.

Genomförda åtgärder

Ett tidigare identifierat åtgärdsförslag är genomfört av operatören:

- Uppstart av en intern kartläggning av beroenden hos operatören och att kontinuitetsplanera verksamheten därefter. Åtgärden syftar till att öka operatörens förståelse för olika interna och externa beroenden.

Kunskapen används för att ställa välgrundade krav på kontinuitet och återhämtningstider i operatörens olika processer.

- Operatören har fullföljt den interna kartläggningen av beroenden kopplade till ”Producera Tjänst (Brev)” och Producera Tjänst (Paket)”, ställt krav på kontinuitet och återhämtningstider till dessa processer samt utvecklat kontinuitetslösningar vid behov.

Planerade åtgärder

En planerad åtgärd är identifierad:

Utveckla samverkan mellan operatören och de myndigheter som den samhällsomfattande posttjänsten kan vara beroende av vid kriser och störningar, exempelvis PTS, räddningstjänst, polisen, trafikverket med flera. I förlängningen bör även samverkansövningar kunna genomföras för att kontrollera att organisationer och rutiner fungerar som tänkt.

4.7 Behov av ytterligare åtgärder med anledning av risk- och sårbarhetsanalysens resultat för postsektorn

1. Se över möjligheterna att genomföra en kartläggning av samhällsviktiga verksamheters beroende till den samhällsomfattande posttjänsten
   - Förslaget syftar till att utreda om och i så fall i vilken omfattning den samhällsomfattande posttjänsten är samhällsviktig. Resultatet skulle vara ett väsentligt underlag för att orientera nästa RSA mot just de delar där andra samhällskritiska verksamheters beroenden av den samhällsomfattande posttjänsten är som störst.
2. Utred om det finns ett behov av och möjlighet att prioritera tillgången till viss kritisk infrastruktur (såsom elförsörjning, elektronisk kommunikation, järnvägstransport och drivmedel) för den samhällsomfattande posttjänsten.
   - Förslaget bygger på att en kartläggning av andra samhällsviktiga verksamheters beroende av den samhällsomfattande posttjänsten genomförs. Resultatet kan visa om det finns ett behov av att prioritera posttjänstens tillgång till kritisk infrastruktur.
3. Utred om PTS bör ställa utökade krav på, alternativt fördjupa tillsynen av, den samhällsomfattande posttjänsten rörande förmågan att hantera kriser och störningar.
   - Förslaget syftar till att förbättra PTS möjlighet att genomföra sitt uppdrag att bevaka att posttjänsterna svarar mot samhällets behov.

5 Risk– och sårbarhetsanalys sektorn för elektronisk kommunikation

5.1 Sektorn för elektronisk kommunikation

Marknaden för elektronisk kommunikation kännetecknas av komplexa nät och många olika aktörer som är ömsesidigt beroende av varandra. I januari 2018 fanns cirka 640 operatörer anmälda hos PTS.

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.

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. Dessa regler har tydliggjort i PTS föreskrifter (2015:2) om Driftsäkerhet. I föreskrifterna finns krav på långsiktigt, systematiskt och kontinuerligt driftsäkerhetsarbete genom bl.a. riskanalyser, kontinuitetsplanering, övervakning, tester och handlingsplaner.

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, t.ex. genom att köpa redundanta förbindelser med geografisk diversitet. .

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. De åtgärder som genomförs berör såväl fasta som mobila nät, men PTS genomför även utbildningar och övningar. Myndigheten finansierar även åtgärder som exempelvis Ledningskollen, för att motverka avgrävningar, och Robust fiber, ett branschkoncept för att skapa robust fiberanläggning.

5.2 Beskrivning av arbetsprocess och metod

Risk- och sårbarhetsanalysen består av risk- och förmågebedömningar som beskriver på vilket sätt postsektorn och sektorn för elektronisk kommunikation och samhället kan påverkas negativt av olika typer av händelser som avbrott i nät och tjänster. Denna analys är begränsad till de fall då denna påverkan kan innebära en stor risk eller fara för befolkningens liv och hälsa, samhällets funktionalitet eller samhällets grundläggande värden.

PTS risk- och sårbarhetsanalys syftar till att:

- bidra till en riskbild för samhället,
- ge underlag för bedömningar för beslutsfattare och verksamhetsansvariga,
- ge ett underlag för information om samhällets risker till allmänheten, samt
- ge underlag för samhällsplanering.

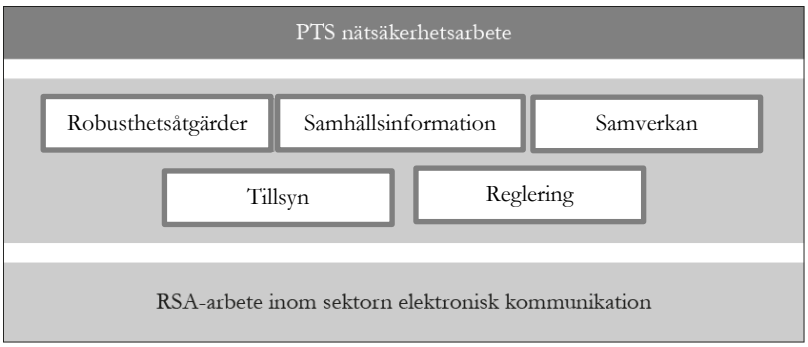
5.2.1 Arbetsprocess - Sektorn för elektronisk kommunikation

PTS arbete med risk- och sårbarhetsanalyser för sektorn elektronisk kommunikation följer i huvudsak[19] den process som beskrivs i SS-ISO 31000. Informationsspridning inom myndigheten sker som del i det ordinarie nätsäkerhetsarbetet. Dialoger med operatörer och samhällsaktörer som är beroende av elektronisk kommunikation integreras på samma sätt i befintliga samarbetsfora.

PTS mål för arbetet med risk- och sårbarhetsanalyser är att skapa en stabil grund för myndighetens arbete för mer robusta och driftsäkra elektroniska kommunikationsnät och –tjänster.

[19] Vissa skillnader förekommer för att avspegla förhållanden inom sektorn elektronisk kommunikation. Ett sådant exempel är att huvuddelen av operatörer med möjlig nationell påverkan är privata företag som verkar på en konkurrensutsatt marknad.

Figur 3 PTS RSA-arbete utgör grunden för myndighetens samlade arbete inom nätsäkerhetsområdet.



De huvudsakliga informationskällor som ligger till grund för riskidentifiering och riskanalys är följande:

- nationella och internationella händelser med betydande påverkan på elektroniska kommunikationsnät och kommunikationstjänster,
- övningar som syftar till att stärka sektorns förmåga att genom samverkan mellan operatörer hantera allvarliga och omfattande nätsäkerhetshändelser,
- PTS föreskrifts- och tillsynsverksamhet som utgår från LEK,
- samverkan och dialoger med operatörer och andra aktörer inom och utanför sektorn, och
- internationella kontakter med myndigheter och organisationer.

5.2.2 Metod - Sektorn för elektronisk kommunikation

Den metod som PTS använder för riskbedömningar har anpassats efter de riktlinjer som utarbetats av NIST.[20] Riskbedömningarna relaterar till möjliga orsaker och händelser som kan påverka den samhällsviktiga verksamheten inom sektorn för elektronisk kommunikation och därmed samhället negativt.

Riskidentifieringen och riskanalysen utgår från en allmän beskrivning av riskkällor som kan orsaka nätsäkerhetshändelser. Sådana händelser leder till negativa samhälleliga konsekvenser med en viss sammanvägd sannolikhet.

[20] Guide for Conducting Risk Assessments, NIST Special Publication 800-30, Revision 1, Initial Public Draft.

Händelser beskrivs på en aggregerad nivå utan att i detalj specificera samtliga förhållanden som kan orsaka negativa konsekvenser.

Konsekvenserna av en händelse bedöms i två steg. I det första steget värderas händelsens negativa påverkan på elektronisk kommunikation. I det andra steget värderas hur denna negativa påverkan på elektronisk kommunikation kan drabba:

- befolkningens liv och hälsa,
- samhällets funktionalitet, och
- grundläggande värden som rättssäkerhet och demokrati, samt
- leda till skador på egendom och miljö.

Även konsekvensbedömningar redovisas på en aggregerad nivå. En enskild bedömning av de tekniska och samhälleliga konsekvenserna ska därmed betraktas som ett representativt utfall. Variationer mellan liknande händelser hanteras som del i en känslighetsanalys. Riskbedömningar sker för sådana hot som kan ge upphov till mer allvarliga nationella konsekvenser[21].

5.3 Identifierad samhällsviktig verksamhet inom sektorn för elektronisk kommunikation som är av nationell/regional betydelse

Elektroniska kommunikationsnät och tjänster spelar en allt viktigare roll i vårt samhälle, i vardagen såväl som vid extraordinära händelser. Varje dag bidrar elektronisk kommunikation till olika former av finansiella tjänster, hälso- och sjukvård, arbete för samhällets skydd och säkerhet, transporter, energiförsörjning och flera andra samhällssektorer.

Andra delar av samhället är också beroende av elektronisk kommunikation, från enskilda medborgare till företag och andra organisationer. I vissa fall kan medborgares liv och hälsa direkt påverkas av störningar och avbrott i elektronisk kommunikation.

[21] I enlighet med 4 § 3 pkt. MSBFS 2016:7 ska centrala myndigheters samhällsviktiga verksamheter begränsas tills sådana verksamheter som kan leda till allvarliga nationella och internationella konsekvenser..

PTS tolkning[22] är att den samhällsviktiga verksamheten inom sektorn elektronisk kommunikation som är av nationell betydelse ska uppfylla minst ett av två kriterier:

- Ett bortfall av, eller svår störning i, verksamheten kan ensamt eller tillsammans med motsvarande händelser i andra verksamheter på kort tid leda till att en allvarlig *nationell* kris inträffar i samhället.
- Verksamheten är nödvändig, eller mycket väsentlig, för att en redan inträffad *nationell* kris i samhället ska kunna hanteras så att skadeverkningarna blir så små som möjligt.

Utgående från denna tolkning redovisas i tabell PTS bedömning av samhällsviktiga verksamheter av nationell betydelse inom sektorn elektronisk kommunikation.

[22] De allmänna råden i MSBFS 2016:7 anger dels att samhällsviktig verksamhet omfattar ”verksamheter, noder, infrastrukturer och tjänster […] som är av avgörande betydelse för upprätthållandet av viktiga samhällsfunktioner”, dels att nationellt samhällsviktig verksamhet ”är verksamhet som vid ett bortfall eller störning […] kan leda till allvarliga nationella eller internationella konsekvenser”. Kommunikationstjänster ges som exempel på viktiga samhällsfunktioner. PTS ser inte att definitionerna i föreskrifterna och de allmänna råden som helt konsistenta.

Tabell 3 Sammanställning av samhällsviktiga verksamheter av nationell betydelse inom sektorn elektronisk kommunikation.

Benämning	Beskrivning
Nätövervakning	Arbete med att kontinuerligt övervaka kommunikations-tjänster och aktiva delar av kommunikationsnät samt att upprätthålla beredskap för att ta emot larm och initiera relevanta åtgärder.
Särskilda tillgångar och förbindelser	Tillgångar och förbindelser som påverkar elektronisk kommunikation på nationell eller internationell nivå. I begreppet ingår också sådan information som är nödvändig för att upprätthålla elektronisk kommunikation samt de logiska skydd som används för att skydda informationen och tillgångarna. Exempel är användarregister, routrar och förbindelser som förmedlar trafik på nationell och internationell nivå, och internationella trafikutbytespunkter.
Viss incidenthantering och felavhjälpning	Incidenthantering och felavhjälpning dels för särskilda tillgångar och förbindelser, dels för samhällsviktiga verksamheter som är beroende av elektronisk kommunikation i hanteringen av en redan inträffad nationell kris.
Visst informations-utbyte med och stöd till samhället	För att möjliggöra felavhjälpning krävs att samhällsviktiga verksamheter har en möjlighet att anmäla fel i nät och tjänster som påverkar verksamheten negativt. För att en pågående nationell kris ska kunna hanteras på ett sätt som minimerar skadeverkningar krävs också att operatörerna kan upprätthålla en grundläggande förmåga att rapportera lägesinformation om pågående störningar, avbrott och integritetsincidenter inom och utanför sektorn elektronisk kommunikation för att minimera skadeverkningarna av en inträffad nationell kris. En del av den information som de brottsbekämpande myndigheterna har tillgång till enligt bestämmelserna i LEK, biståndet vid brottsutredningar och verkställighet av hemliga tvångsmedel kan vara viktiga för att hantera allvarliga kriser på ett sätt som gör att förtroendet för samhället inte urholkas.

5.4 Identifierade kritiska beroenden för den identifierade samhällsviktiga verksamheten inom sektorn för elektronisk kommunikation

Den samhällsviktiga verksamheten[23] av nationell betydelse är kritiskt beroende av processer, resurser och aktörer inom och utanför sektorn elektronisk kommunikation. Inom sektorn finns tre huvudsakliga kritiska beroenden:

- *personal*: som bidrar i samhällsviktig verksamhet och ledningsfunktioner som kan fatta beslut och göra avvägningar mellan olika intressen,
- *anläggningar*: platser som innehåller särskilt viktiga tillgångar och personal som bedriver samhällsviktig verksamhet, och
- *stödsystem*: som används för nätövervakning, vid incidenthantering och felavhjälpning samt för förmedling av lägesinformation.

Den samhällsviktiga verksamheten av nationell betydelse har också beroenden utanför sektorn elektronisk kommunikation. Ett centralt beroende är elförsörjning. Långvariga nationella elavbrott kommer i stor utsträckning att leda till långvariga avbrott i elektronisk kommunikation. Vid långvariga elavbrott kan personal, transportresurser och drivmedel säkra fortsatt samhällsviktig verksamhet med hjälp av bränsledrivna reservkraftsystem. Dock kommer det inte att vara möjligt att upprätthålla tillgängligheten till elektronisk kommunikation då även andra tillgångar, förutom de särskilt viktiga tillgångarna, måste försörjas med reservkraft.

Kommunikationsnät och kommunikationstjänster är beroende av tid- och frekvensrelaterad information för sin funktion.[24] Operatörerna är också beroende av utrustning i form av tekniska system men också olika former av externa tjänster. Ett flertal operatörer anlitar exempelvis en extern part för fältserviceverksamhet. Andra operatörer överlåter nätövervakning och andra samhällsviktiga verksamheter till en annan part.

Tiden från det att en påfrestning drabbar ett eller flera av de kritiska beroendena, till det att den samhällsviktiga verksamheten inom sektorn påverkas varierar. Långvariga elavbrott kan redan efter några timmar leda till avbrott i elektronisk kommunikation medan personalbrist hos leverantörer inte ens på kort eller medellång sikt behöver ge några egentliga negativa konsekvenser. De sammanlagda kritiska beroendena för den samhällsviktiga

[23] Enligt definitionen i MSBFS 2016:7.
[24] Denna information benämns här synkroniseringsinformation. Upprätthållande av en lämplig tid- och frekvensrelaterad information benämns här nätsynkronisering.

verksamheten inom sektorn för elektronisk kommunikation redovisas i tabell nedan.

Tabell 4 Översikt av kritiska beroenden för sektorn elektronisk kommunikation

Beroende	Beskrivning av beroende
Elförsörjning	Samtliga samhällsviktiga verksamheter inom sektorn är kritiskt beroende av en fungerande elförsörjning. Särskilt viktiga tillgångar kan förväntas ha tillgång till reservkraftsystem med 24 timmars reservkraft och möjlighet att upprätthålla funktion under lång tid givet att transportresurser och drivmedel finns tillgängliga i rimlig utsträckning. Vid en elbristsituation kan vissa tillgångar inom elektronisk kommunikation prioriteras.
Transporter och drivmedel	Vid långvariga elavbrott behöver drivmedel tillföras reservkraftsystem inom sektorn. Det finns här ingen prioriteringsordning som gör det möjligt att säkra tillgången till transportresurser och drivmedel i en bristsituation.
Synkroniserings-information	Tid- och frekvensinformation som är nödvändig för att upprätthålla elektronisk kommunikation. På nationell nivå, finns från mitten av 2013 centrala källor till synkroniseringsinformation på utvalda platser i landet som är oberoende av satellitnavigeringssystem.
Leverantörer av utrustning och tjänster	Behov av ersättningsutrustning efter bortfall av särskilt viktiga tillgångar och också felavhjälpnings- och felrättningsinsatser vid allvarliga nätsäkerhetshändelser.
Fältservice personal	Flertalet operatörer har service, reparationer och underhåll på entreprenad. Dessa företag har utöver operatörerna, tillhandahållare i andra sektorer som kunder. Det innebär att det kan bli resursbrist och konkurrens om resurserna i samband med störningar och avbrott som drabbar flera operatörer och eventuellt sektorer.

5.5 Bedömning av sektorn elektronisk kommunikations generella krisberedskap

Nätsäkerhetshändelser i elektronisk kommunikation kan på olika sätt påverka samhället. PTS identifierar hot och bedömer sådana händelser som kan få mer allvarliga samhälleliga konsekvenser på nationell nivå. I vissa fall genomförs enbart konsekvensbedömningar.

5.5.1 Förekomsten av betydande nätsäkerhetshändelser i elektronisk kommunikation

Årligen inträffar mellan ett trettiotal och ett femtiotal händelser med betydande[25] störningar och avbrott i elektronisk kommunikation som följd. Av dessa har endast en mindre del nationell påverkan och påverkan på internationell kommunikation är ovanlig. Antalet kända nätsäkerhetshändelser som påverkar konfidentialitet och riktighet är lägre.[26]

Tabell 5 Antalet nätsäkerhetshändelser med betydande störningar och avbrott i elektronisk kommunikation.

År	2012	2013	2014	2015	2016	2017	2018[27]
Antal händelser	26	35	44	39	33	37	18
Antal händelser med nationell påverkan	11	5	17	6	4	6	3
Antal händelser med internationell påverkan	1	–	–	1	1	-	1

Under åren från 2012 till och med det första halvåret 2018 har sammanlagt 52 händelser inträffat med nationella störningar och avbrott. Av dessa har mer än hälften (33 stycken) orsakats av konfigurations- och andra handhavandefel[28], ofta i kombination med andra fel eller brister. Den näst största felkategorin (12 stycken) är fel i hård- och mjukvara. Resterande nationella störningar och

[25] Operatörer är skyldiga att rapportera störningar och avbrott av betydande omfattning till PTS enligt PTSFS 2015:2. En händelse baseras på en eller flera sådana rapporter. Flera rapporter sammanförs till en händelse om de delar grundorsak. Exempelvis ses en storm som en händelse. I de fall där upprepade störningar och avbrott drabbat en och samma operatör under en kort tid och av samma orsak räknas dessa som en händelse.

[26] Sedan den 1 juli 2011 är operatörer skyldiga att rapportera inträffade integritetsincidenter till PTS och till berörda abonnenter. En integritetsincident är en händelse som leder till oavsiktlig eller otillåten utplåning, förlust eller ändring, eller otillåtet avslöjande av eller otillåten åtkomst till uppgifter som behandlas i samband med tillhandahållandet av allmänt tillgängliga elektroniska kommunikationstjänster.

[27] Första halvåret. Den internationella störningen är en tillhandahållare av IP-telefoni vars verksamhet i Sverige, Danmark och Norge påverkades.

[28] Inom den drabbade operatörens organisation men också hos en annan operatör där konfigurations- eller handhavandefelet påverkat en annan operatör.

avbrott (7 stycken) orsakas av överbelastningsattacker. En närmare analys visar också följande:

- Huvuddelen av alla störningar och avbrott pågår en kortare tid, från några timmar upp till 8 timmar. Cirka 25 procent överstiger 12 timmar och ingen störning eller avbrott varade längre än 21 timmar.
- De störningar och avbrott som orsakas av tillgänglighetsattacker pågår vanligtvis mellan 1 timme och 2 timmar. I ett fall pågick störningarna och avbrotten i över 10 timmar.

Tabell 6 Antalet nätsäkerhetshändelser med betydande störningar och avbrott påverkan på fasta och mobila tjänster

År	2015	2016	2017	2018[29]
Antal händelser	39	33	37	18
Påverkan mobila tjänster	9	6	10	7
Påverkan fasta tjänster	23	24	23	9
Påverkan fasta och mobila tjänster	7	3	4	1

Fler händelser har under perioden 2015 till första halvåret 2018 påverkat fasta tjänster än mobila tjänster. Dessa händelser har dock i regel haft mindre omfattande konsekvenser med färre antal drabbade abonnenter eller geografiskt område.

5.5.2 Särskilda händelser sedan rapporteringen 2016[30]

Antalet nätsäkerhetshändelser med nationell påverkan varierar år från år. Sedan den senaste rapporteringen år 2016, har en händelse inträffat som på olika sätt har påverkat samhället:

- Kapacitetsproblem i ett mobilnät till följd av terrorattentatet den 7 april 2017[31]

I samband med attentatet upplevde mobiloperatörerna en betydande ökning av mobilsamtal- och datakommunikation. Taltrafiken ökade kraftigt och var 2–10 gånger normaltrafik. Datatrafiken ökade och var cirka 2 gånger jämfört med

[29] Första halvåret.
[30] Händelser som inträffat efter det första halvåret 2016.
[31] Skrivelse PTS Dnr: 17-9965

normaltrafiken. Trafikökningarna inleddes i vissa fall så tidigt som någon minut efter den inträffade händelsen. Genomgående var belastningen som störst mellan kl. 15.00 och 16.00, även om vissa operatörer upplevde hög men gradvis minskande belastning fram till kl. 16.30 eller 17.00.

Den betydande ökningen av mobil samtals- och datakommunikation ledde till att mobilnäten drabbades av överbelastningar. Överbelastningarna innebar i huvudsak att användare hade svårt att ringa och ta emot samtal i området runt attentatsplatsen och i centrala delar av Stockholm. Lokalt och i Stockholms centrala delar kunde 10-60 procent av mobilsamtalen inte genomföras. Spannet på 10–60 procent beror främst på variationer mellan olika geografiska områden, olika tidsperioder och olika mobiloperatörer. Överbelastningarna hade störst påverkan i Stockholms centrala delar, men det förekom till viss del även regional påverkan, och i ett fall även viss nationell påverkan.

Sedan föregående rapportering 2016 har det, av operatörerna, inte inrapporterats några händelser som påverkat konfidentialitet och riktighet i elektronisk kommunikation med en mer betydande och bestående samhällspåverkan.

PTS har inte sett anledning att förändra riskbedömningarna från 2016 med anledning av de inträffade händelserna.

5.5.3 Utgångspunkter för genomförande av riskbedömningar

Ett mindre antal hot mot sektorn elektronisk kommunikation kan ge upphov till mer allvarlig påverkan på befolkningens liv och hälsa, samhällets funktionalitet och grundläggande värden eller ge upphov till betydande skador på egendom och miljö. Riskbedömningar sker för sådana hot som uppfyller minst ett av följande fyra villkor: [32]

1. Hotet ska kunna leda till *långvarigt* avbrott i flera kommunikations-tjänster[33] som drabbar en *övervägande* del av landets befolkning.
2. Hotet ska kunna leda till *upprepade* och *långvariga* avbrott som drabbar en *övervägande* del av landets befolkning.
3. Hotet ska kunna leda till *långvarigt* avbrott som påverkar en eller flera samhällsviktiga verksamheter av nationell betydelse samtidigt.

[32] I villkoren förekommer (i kursiv stil) flera kvalitativa bestämningsord utan att de preciseras närmare. I bilaga 1redogörs för tolkningen av bestämningsorden.
[33] Markbaserade radio- och TV-utsändningar ingår här som del i begreppet kommunikationstjänst.

4. Hotet ska kunna påverka informationstillgångar av *betydande* demokratiskt, ekonomiskt, miljömässigt eller på annat sätt samhälleligt värde negativt.

Denna avgränsning gör att riskbedömningar inte genomförs för händelser med lokala och regionala avbrott eller där ett mindre antal abonnenters personliga integritet påverkas negativt. Om antalet eller omfattningen av händelser av denna karaktär skulle öka från dagens nivåer, kan det uppstå negativ påverkan på nationell nivå.[34]

5.5.4 Risknivån för flera hot bedöms vara obetydlig

Av de inträffade och rapporterade händelserna gör PTS bedömningen att ingen uppfyller något av villkoren 1 och 2. PTS har ingen information som gör det möjligt att avgöra i vilken utsträckning som inträffade störningar och avbrott påverkade flera samhällsviktiga verksamheter samtidigt (villkor 3). På samma sätt bedöms att ingen annan nätsäkerhetshändelse som rapporterats till PTS uppfyller villkor 4.

En viktig anledning till att huvuddelen av de hot som kan påverka elektronisk kommunikation normalt inte leder till allvarliga samhälleliga störningar är de sätt som moderna kommunikationsnät etableras och underhålls. Här bidrar både den tekniska utvecklingen, kommersiella hänsyn och regulatoriska krav till detta förhållande. Tabellen nedan ger exempel på sådana typer av hot som bedöms utgöra samhälleliga risker.

[34] PTS avser följa utvecklingen i detta avseende enligt beskrivningen i avsnitt 5.5.7.

Tabell 7 Exempel på hot som bedöms utgöra samhälleliga risker på nationell nivå.

Typ av hot	Hotbeskrivning
Fysiska hot	Bränder[35], vattenskador, dammbrott och olika typer av radiologiska eller kemiska föroreningar förväntas inte leda till nationella avbrott. På samma sätt bedöms inte skadegörelse, dammbrott, korrosion, förfrysning och enskilda avgrävningar av förbindelser få några samhälleliga konsekvenser av stor dignitet.
Naturligt förekommande hot	Klimatologiska fenomen som torka, global uppvärmning och översvämningar bedöms inte kunna leda till nationella avbrott. På samma sätt kan det förväntas att rimligen förekommande seismiska och vulkaniska fenomen, stormar, snöstormar och värmeböljor inte leder till mer allvarliga samhälleliga konsekvenser på nationell nivå.
Elektromagnetiska eller termiska hot	Avsiktliga elektromagnetiska störningar, åska, geomagnetiska stormar, andra oavsiktliga eller naturligt förekommande elektromagnetiska störningar samt termisk strålning bedöms inte kunna få allvarliga nationella konsekvenser.
Brist på kritiska resurser	PTS gör bedömningen att händelser där personalbrist kan orsaka nätsäkerhetshändelser i elektronisk kommunikation med betydande samhällelig påverkan är mycket osannolika. På samma sätt ser PTS hot som riktas mot tillgången till synkroniseringsinformation (*Tid och Takt*) som obetydliga risker. Lokala och regionala elavbrott samt korta och medellånga nationella elavbrott bedöms inte leda till några mer allvarliga samhälleliga konsekvenser på nationell nivå.

[35] Brand i försörjningstunnlar är undantaget.

5.5.5 Risk- och konsekvensbedömningar för händelser som kan leda till allvarliga samhälleliga konsekvenser

Flera olika typer av hot kan orsaka nätsäkerhetshändelser som leder till mer allvarliga samhälleliga konsekvenser. Utgående från de villkor som angivits i avsnitt 5.5.3 identifierar PTS sex typer av händelser[36] som på olika sätt kan ge en mer betydande negativ påverkan på liv och hälsa, ekonomisk värden eller andra samhälleliga skyddsvärden:

- nationella elavbrott,
- avbrott som orsakas av fel och brister i:
    - hantering, handhavandefel,
    - programvara respektive
    - hårdvara,
- avbrott i särskilda tillgångar och förbindelser,
- tillgänglighetsattacker.

Konsekvensbedömningar redovisas för attacker som riktas mot informationstillgångars konfidentialitet, riktighet och spårbarhet. De fullständiga riskbedömningarna för de sex händelsetyperna sammanfattas i avsnitt 5.5.6.

Långvariga nationella elavbrott bedöms vara en medelhög risk

Varje år inträffar ett stort antal elavbrott. Den absoluta majoriteten av dessa elavbrott drabbar ett mindre antal (elektriska) nätanslutningspunkter. I de fall där ett långvarigt nationellt elavbrott inträffar som påverkar huvuddelen av samtliga nätanslutningspunkter uppstår nationella avbrott i elektronisk kommunikation. Befintliga stationära reservkraftsystem har begränsad uthållighet och antalet transportabla reservkraftsystem är begränsat.[37] För medellånga nationella elavbrott begränsar reservkraftsystemen de negativa konsekvenserna.

Det finns inga utvecklade rutiner för att prioritera återställningen av elförsörjning till tillgångar inom sektorn för elektronisk kommunikation som påverkar samhällsviktig verksamhet och på så sätt mildra konsekvenserna.

[36] Inom varje typ av hot ryms flera olika händelser som kan påverka elektronisk kommunikation på olika sätt. Varje enskilt hot som kan orsaka händelsen behandlas inte enskilt.
[37] Tillgångar av särskild betydelse kan förväntas fortsätta fungera 24 timmar efter det att ett elavbrott inträffat och genom kontinuerlig tillförsel av drivmedel ges fortsatt funktion. Tillgångar som påverkar ett mindre antal abonnenter har inte samma möjlighet till kontinuerlig drift.

Händelse	
A	Ett långvarigt nationellt elavbrott inträffar som påverkar huvuddelen av landets (elektriska) nätanslutningspunkter
B	Upprepade medellånga elavbrott inträffar som påverkar huvuddelen av landets (elektriska) nätanslutningspunkter

Sannolikhetsbedömning			
	Inträffar	*Negativ påverkan*	*Sammanvägt*
A	Mycket låg	Mycket hög	Låg
B	Mycket låg	Mycket hög	Låg

Konsekvenser för elektronisk kommunikation			
	Operatörer	*Tjänster*	*Längd*
A	Flertal	Flertal	Långvariga
B	Flertal	Flertal	Kortvariga

Samhällskonsekvenser					
	Liv och hälsa	*Funktionalitet*	*Värden*	*Egendom*	*Nivå*
A	Ja	Ja	–	–	Medel
B	Ja	Ja	–	–	Låg

Samhällelig risknivå		
A	Långvarigt nationellt elavbrott	Medelhög risk
B	Upprepade medellånga elavbrott	Låg risk

Känslighetsanalys
Bedömningen av sannolikheterna för nationella elavbrott innehåller osäkerhet. PTS gör bedömningen att båda händelserna är mycket sällsynta. På samma sätt är det svårt att uppskatta de samhälleliga konsekvenserna av de avbrott som uppstår i elektronisk kommunikation då en rad omständigheter inom och utanför sektorn påverkar konsekvenserna.

Avbrott som orsakas av fel och brister i hantering, programvara eller hårdvara bedöms alla vara låga risker[38]

Elektronisk kommunikation bygger på komplexa tekniska system där mänsklig hantering, programvara och hårdvara samverkar. Allmänt gäller att operatörer tillämpar rutiner för genomförande av ändringar av tekniska system, genomför tester och använder redundans för att mildra eller eliminera effekterna av enskilda hårdvarufel. Trots sådana rutiner och åtgärder kan fel och brister orsaka omfattande avbrott.

Händelse	
A	Ett eller flera samverkande fel inträffar och påverkar flera särskilda tillgångar hos en operatör med en betydande marknadsandel
B	Ett eller flera samverkande fel inträffar och påverkar flera särskilda tillgångar hos flera operatörer med betydande sammanlagd marknadsandel

Sannolikhetsbedömning			
	Inträffar	*Negativ påverkan*	*Sammanvägt*
A	Hög	Medel	Hög
B	Låg	Låg	Låg

Konsekvenser för elektronisk kommunikation			
	Operatörer	*Tjänster*	*Längd*
A	En	Fåtal	Medellång
B	Flertal	Fåtal	Medellång

Samhällskonsekvenser					
	Liv och hälsa	*Funktionalitet*	*Värden*	*Egendom*	*Nivå*
A	Ja	Ja	–	–	Mycket låg
B	Ja	Ja	–	–	Låg

Samhällelig risknivå		
A	Ett eller flera samverkande fel påverkar en operatör	Låg risk
B	Ett eller flera samverkande fel påverkar flera operatörer	Låg risk

Känslighetsanalys

[38] Även om förekomsten av avbrott som orsakas av fel och brister i hantering, programvara och hårdvara varierar, gör PTS bedömningen att risknivåerna för de särskilt allvarliga händelserna är likvärdiga varför riskbedömningarna genomförs samlat.

De samhälleliga konsekvenserna kan i stor utsträckning förväntas variera. Om avbrottet påverkar samhällsviktiga funktioner eller om avbrottet inträffar samtidigt som en allvarlig händelse kan de samhälleliga konsekvenserna bli allvarligare. På samma sätt kan de samhälleliga konsekvenserna ofta vara lägre.

Avbrott i tillgångar och förbindelser bedöms vara en låg risk

Det finns flera olika händelser som kan leda till att tillgångar eller förbindelser förlorar förmåga att överföra information. Ett sätt är avgrävning i olika delar av kommunikationsnät som följd av någon form av anläggningsarbete. En annan är hårdvarufel i kommunikationsutrustning där en tillgång eller förbindelse bortfaller utan annan samtidig skada.

I vissa tätbebyggda områden används tunnlar för att framföra olika typer av försörjningssystem. I anslutning till tunnlarna kan det även finnas utrymmen som innehåller flera tillgångar (noder). Kommunikationsförbindelser blir på detta sätt mindre sårbara. I gengäld så innehåller flera försörjningstunnlar en särskild hög koncentration av förbindelser som påverkar ett flertal olika kommunikationsnät och kommunikationstjänster.

En omfattande brand i en försörjningstunnel kan resultera i avbrott i flera eller samtliga förbindelser med begränsade möjligheter till reparationer annat än efter lång tid. Samtidigt arbetar operatörer aktivt för att minska påverkan på abonnenter genom olika typer av alternativa lösningar. De resulterande avbrotten kan förväntas ha mer bestående lokal snarare än regional eller nationell påverkan och i vissa fall[39] påverka samhällsviktig verksamhet eller på annat sätt leda till mer betydande samhälleliga konsekvenser.

För särskilda tillgångar och förbindelser är användningen av redundans som skydd mot nationella avbrott väl etablerad. Det innebär att det normalt krävs två eller flera samtidiga avbrott i förbindelser för att nå egentlig negativ påverkan på nationell nivå. Reparationsinsatser begränsar normalt avbrottens längd.

Händelse
A Flera samverkande avbrott i särskilda förbindelser inträffar och påverkar en större operatör

[39] Inte alla försörjningstunnlar innehåller förbindelser som direkt påverkar viktiga samhällsfunktioner, särskilt inte om dessa verksamheter har avtalat om redundans i förbindelser.

B Flera samverkande avbrott i särskilda förbindelser inträffar och påverkar ett flertal operatörer med en betydande sammanlagd marknadsandel

Sannolikhetsbedömning

	Inträffar	*Negativ påverkan*	*Sammanvägt*
A	Medel	Medel	Medel
B	Låg	Mycket låg	Mycket låg

Konsekvenser för elektronisk kommunikation

	Operatörer	*Tjänster*	*Längd*
A	En	Fåtal eller flertal	Medellång
B	Flertal	Fåtal eller flertal	Medellång

Samhällskonsekvenser

	Liv och hälsa	*Funktionalitet*	*Värden*	*Egendom*	*Nivå*
A	Ja	Ja	–	–	Mycket låg
B	Ja	Ja	–	–	Låg

Samhällelig risknivå

A	Flera samverkande avbrott i särskilda förbindelser hos en operatör	Låg
B	Flera samverkande avbrott i särskilda förbindelser hos flera operatörer	Mycket låg

Känslighetsanalys

Det är i första hand konsekvenserna för elektronisk kommunikation samt de samhälleliga konsekvenserna som kan variera. På vissa platser kan geografiska, marknadsmässiga eller andra förhållanden leda till avvikelser från de allmänna nätbyggnadsprinciper som operatörerna tillämpar. I andra fall kan ett större antal samhällsviktiga funktioner inom samma geografiska område drabbas av avbrotten. I förekommande fall kan därmed både de tekniska och samhälleliga konsekvenserna vara både högre och lägre än de angivna nivåerna.

Det är fler händelser än brand som kan påverka förbindelser i försörjnings-tunnlar, exempelvis sabotage. Den angivna sannolikheten är i första hand kopplad till en brand. I många andra försörjningstunnlar, med en mindre koncentration av särskilt viktiga förbindelser, kan det förväntas att de samhälleliga konsekvenserna blir mer begränsade. De samhälleliga

konsekvenserna beror också av samhällsviktiga verksamheters val av kommunikationslösningar och också av möjligheten att reducera avbrottens längd genom alternativa lösningar. I de fall där avbrotten skulle pågå under lång tid och påverka en bredare skara samhällsviktiga verksamheter kan risknivån vara högre.

Tillgänglighetsattacker av en sofistikerad angripare bedöms vara en låg risk

Tillgänglighetsattacker på nivåer som kräver åtgärder är i dag relativt vanligt förekommande. Hos de nationella operatörerna bedöms förmågan att skydda informationstillgångar och tekniska system vara god. De har etablerade säkerhetsorganisationer som aktivt arbetar för att skydda information och tillgångar samt hantera incidenter när de väl inträffar. Sofistikerade angripare med särskild kunskap och med stora eller avsevärda resurser kan dock vara svåra att skydda sig mot.

Händelse					
A	Upprepade tillgänglighetsattacker som riktas mot en enskild operatör och påverkar en betydande del av befolkningen eller viktiga samhällsfunktioner av nationell betydelse				
B	Upprepade tillgänglighetsattacker som riktas mot flera operatörer samtidigt och påverkar en betydande del av befolkningen eller viktiga samhällsfunktioner av nationell betydelse				
Sannolikhetsbedömning					
	Inträffar		*Negativ påverkan*		*Sammanvägt*
A	Mycket hög		Medel		Hög
B	Medel		Medel		Medel
Konsekvenser för elektronisk kommunikation					
	Operatörer		*Tjänster*		*Längd*
A	En		Fåtal		Medellång
B	Flertal		Fåtal		Medellång
Samhällskonsekvenser					
	Liv och hälsa	*Funktionalitet*	*Värden*	*Egendom*	*Nivå*
A	Ja	Ja	–	–	Mycket låg
B	Ja	Ja	–	–	Låg
Samhällelig risknivå					

A	Upprepade tillgänglighetsattacker mot en enskild operatör	Låg
B	Upprepade tillgänglighetsattacker mot flera operatörer samtidigt	Medel

Känslighetsanalys

Sannolikheter för att händelserna inträffar och att de leder till negativa konsekvenser baseras på uppskattningar av en angripares intresse och förmåga att rikta och genomföra mer bestående logiska attacker mot en eller flera operatörer. På samma sätt är det svårt att uppskatta de samhälleliga konsekvenserna av tillgänglighetsattackerna. Flertalet attacker som genomförs kan förväntas få ringa påverkan på samhället i kraft av de skyddsåtgärder som tillämpas.

Attacker som riktas mot informationstillgångars konfidentialitet kan få stora konsekvenser[40]

Attacker mot informationstillgångar, som antingen förmedlas med eller genereras vid användning av elektronisk kommunikation, kan utföras både av en intern och extern angripare och också för olika syften. Förekomsten av fel och brister i protokoll, rutiner, hårdvara och programvara påverkar både antalet händelser med negativ samhällelig påverkan och omfattningen av denna negativa påverkan.

I konsekvensbedömningar för logiska attacker som riktas mot informationstillgångars konfidentialitet beaktas dels en insider, dels en sofistikerad extern angripare med betydande resurser och särskild kompetens. I båda fallen bedömer PTS att det i första hand är samhällets grundläggande funktionalitet, samhälleliga värden samt egendom som kan påverkas negativt.

Attacker som riktas mot riktigheten i informationstillgångar bedöms normalt ge upphov till mer begränsade samhälleliga konsekvenser. Spårbarhet för informationstillgångar bedöms på samma sätt påverka samhälleliga skyddsvärden i mindre utsträckning.[41] Av dessa skäl redovisas ingen konsekvensbedömning för dessa typer av attacker.

Händelse	
A	Insiderattacker som riktas mot informationstillgångars konfidentialitet hos en operatör

[40] För denna typ av attacker saknar PTS underlag och information för att uppskatta sannolikheter. Av detta skäl redovisas enbart konsekvensbedömningar.
[41] Spårbarhetens betydelse för rättsvårdande myndigheters och andra samhälleliga verksamheters behov ingår inte som del i bedömningen.

B	Sofistikerade (externa) attacker som riktas mot informationstillgångars konfidentialitet och påverkar flera operatörer

Konsekvenser för elektronisk kommunikation			
	Operatörer	*Omfattning*	*Längd*
A	En	Omfattande	Långvarig
B	Flertal	Omfattande	Långvarig

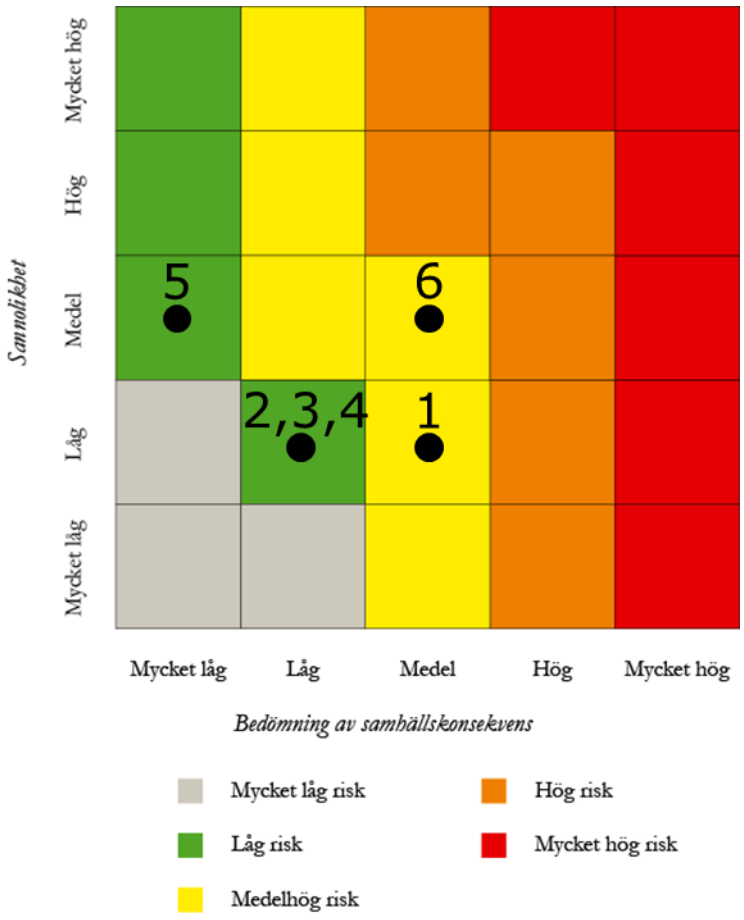
Samhällskonsekvenser					
	Liv och hälsa	*Funktionalitet*	*Värden*	*Egendom*	*Nivå*
A	–	-	Ja	Ja	Låg
B	–	-	Ja	Ja	Medel

5.5.6 Sammanfattning av riskbilden för elektronisk kommunikation

De riskbedömningar som redovisats i avsnitt 4.5.5 utgår från händelser som på olika sätt kan leda till mer allvarlig nationell påverkan. Händelser som påverkar ett mindre geografiskt område eller leder till mer kortvariga avbrott i elektronisk kommunikation utelämnas. På samma sätt redovisas enbart konsekvensbedömningar för vissa händelser.

I figur 4 redovisas riskbedömningarna för de olika typer av hot som PTS har identifierat som relevanta. Varje typ av händelse representeras av händelsen med högst risknivå.

Figur 4 Riskmatris för hot med möjlig nationell påverkan på elektronisk kommunikation.



Hottyper med möjlig nationell påverkan

1. Nationella elavbrott
2. Fel och brister i hantering, handhavandefel
3. Fel och brister i hårdvara
4. Fel och brister i programvara
5. Avbrott i tillgångar och förbindelser
6. Logiska tillgänglighetsattacker

5.5.7 Flera allmänna hot och förändringar kan långsiktigt påverka riskbilden

I de föregående avsnitten redovisas riskbedömningar för ett antal hot som direkt eller på kort sikt påverkar samhället negativt. Förutom dessa hot, finns det flera andra hot och andra förändringar som på längre sikt riskerar att förskjuta riskbilden.[42]

[42] Med en påverkan på riskbilden menas en utveckling där sårbarheter eller allmänna förhållanden ändras över tiden på ett sätt som inte är förutsägbart eller kan kvantifieras. Genom en sådan förskjutning påverkas sannolikheten för att ett eller flera hot ger upphov till negativa konsekvenser eller att de samhälleliga konsekvenserna förvärras utan att ett eller flera specifika hot ändras.

Om samhällsviktiga verksamheter i ökad utsträckning inte värderar säkerhetsaspekter på ett lämpligt sätt vid anskaffning kan flera risknivåer öka. En verksamhet som är kritiskt beroende av fasta datakommunikationstjänster blir exempelvis mer sårbar mot avbrott i förbindelser om anskaffningen inte säkerställer redundans. Operatörernas marknadsmässiga incitament att prioritera nätsäkerhetsåtgärder, utöver den lagstadgade nivån, kan med en sådan utveckling förväntas minska.

Samverkan, mellan operatörer, områdesansvariga myndigheter och organisationer, är centrala för samhällets samlade förmåga att på ett effektivt sätt hantera konsekvenserna av en extraordinär händelse. PTS gör i dag bedömningen att sektorns större operatörer har en god förmåga att leda, samverka och informera. En försämrad förmåga kan dock leda till längre återställningstider och därmed större samhälleliga påfrestningar efter olika typer av extraordinära händelser, särskilt då resursbehoven är så stora att de nationella resurserna inte är tillräckliga.

I PTS föreskrifter och allmänna råd som förtydligar regulatoriska krav i LEK anges att operatörer bör bedriva ett kontinuerligt och systematiskt säkerhetsarbete. En utveckling där detta säkerhetsarbete ges mindre resurser, exempelvis genom ökat fokus på effektiviseringar, kan påverka riskbilden. Andra utvecklingsmöjligheter, som en minskning av antalet oberoende nätinfrastrukturer genom konsolidering och följderna av klimatförändringar, kan öka flera risknivåer.

Under det senaste året har en rad sårbarheter i olika typer av kundplacerad eller kundägd utrustning som används för elektronisk kommunikation konstaterats men också i protokoll och andra former av tillgångar. Med nya användningsområden, från e-hälsa till fjärrövervakning och kontroll av tekniska system, kan sårbarheter få allt större negativ påverkan, både för den enskilde individen som samhället i stort. Om samhällsviktiga användare i framtiden kommer att utnyttja mobila kommunikationsnät för verksamhetskritisk kommunikation[43] kommer också riskbilden att påverkas.

5.6 Beskrivning av identifierade sårbarheter och brister i krisberedskap inom sektorn för elektronisk kommunikation

De huvudsakliga sårbarheter och allmänna brister i krisberedskap som kan identifieras för sektorn för elektronisk kommunikation påverkar i första hand

[43] På det sätt som beskrivs i PTS rapport Säker och tillgänglig mobil, ip-baserad kommunikation, PTS-ER-2016:12.

förekomsten av olika typer av störningar och avbrott på lokal och regional nivå.

PTS gör bedömningen att enbart ett mindre antal sårbarheter och brister i krisberedskap kan leda till nationella avbrott och nätsäkerhetshändelser med mer betydande samhällelig påverkan:[44] I huvudsak härrör dessa brister och sårbarheter från förhållanden som går utöver grundläggande regulatoriska krav och rimliga kommersiella hänsyn.

Tabell 8 Sammanställning av sårbarheter och brister i krisberedskap utgående från den eller de aktörer som kan mildra eller avhjälpa sårbarheten.

Berörda aktörer	Sårbarhet eller brist i krisberedskap
Samhället	Brister i samhällsviktiga verksamheters värdering av de egna behoven av driftsäkerhet, exempelvis för att tillförsäkra sig bibehållen elektronisk kommunikation även vid långvariga elavbrott
	Avsaknad av en prioritetsordning som vid nationella elavbrott ger sektorn för elektronisk kommunikation prioritet vid återställningsarbetet inom elsektorn samt till transport- och drivmedelsresurser
PTS	Brister i detaljerad kunskap om samhällets beroenden, sett utifrån alla sektorer som är beroende av elektronisk kommunikation som underlag för konsekvensbedömningar
Sektorns aktörer inräknat PTS	Brister i erfarenhet och resurser för att hantera betydande nationella avbrott som kräver långvariga och geografiskt spridda insatser
	Brister i önskvärd förmåga att motstå, upptäcka och hantera sofistikerade logiska attacker
	Brister i operatörers hantering och ändringar av elektroniska kommunikationsnät
Leverantörer	Brister i leverantörers tester av tillgångar för att säkerställa att de inte innehåller fel eller brister
Fältservice	Brister i resurser att samtidigt reparera och underhålla tillgångar och förbindelser för flera operatörer samtidigt på flera olika geografiska platser.

[44] Detta utgår från de avgränsningar som tidigare redovisats. Sårbarheterna och bristerna i krisberedskap undantar därmed sådana sårbarheter och brister med huvudsaklig koppling till säkerhetsskydd, höjd beredskap och väpnat angrepp mot landet.

5.7 Genomförda, pågående och planerade åtgärder sedan föregående rapportering inom sektorn för elektronisk kommunikation

Utvecklingen inom sektorn för elektronisk kommunikation gör att operatörer kontinuerligt genomför åtgärder som på olika sätt kan påverka förekomsten av mer omfattande nätsäkerhetshändelser[45]. Varje år genomförs också ett antal åtgärder där PTS bidrar med medel för att finansiera olika samhälleliga intressen. I de följande avsnitten redovisas enbart sådana åtgärder som antingen bedöms påverka riskbedömningarna eller som genomförts för att skapa alternativt bibehålla en lämplig förmåga att motstå och hantera nätsäkerhetshändelser med nationell påverkan.

5.7.1 Genomförda åtgärder

PTS har under perioden följt upp inrapporterade incidenter, och bedrivit tillsyn utgående från LEK och gällande föreskrifter inom nätsäkerhetsområdet.[46]

Två system (GLU och DIO) som förmedlar av information om planerade och pågående driftstörningar och avbrott mellan operatörer och till samhället i övrigt har vidareutvecklats och sammanförts i ett system, Navet. Ett system för spridning av lägesinformation mellan operatörer och elnätsägare för att underlätta återställningsarbetet efter mer långvariga elavbrott har vidareutvecklats. PTS har även stöttat stadsnäten vid framtagning av motsvarande krishanteringssystem för dem.

En utbildnings- och övningsstrategi för krisberedskap 2017-2021, sektorn elektronisk kommunikation[47] har tagits fram. PTS har fortsatt införandet av RAKEL och FTN hos aktörerna inom Nationella telesamverkansgruppen (NTSG). PTS har finansierat åtgärder för att minska sannolikheten för avbrott i särskilda förbindelser, exempelvis genom förläggning under vattendrag. PTS har även finansierat konceptet Robust Fiber för att generellt öka kvaliteten på framtida förbindelser.

[45] Det föreligger ingen rapporteringsskyldighet där operatörerna har att förmedla information till PTS om de åtgärder som genomförs och deras påverkan på riskbilden. I beskrivningarna av genomförda, pågående och planerade åtgärder ingår inte de åtgärder som sektorns aktörer genomför av kommersiella skäl.

[46] PTSFS 2014:1 och 2015:2.

[47] Utbildnings och övningsstrategi, https://pts.se/globalassets/startpage/dokument/icke-legala-dokument/rapporter/2017/internet/rapport_utbildnings--och-ovningsstrategi-2017-2021_pts-er-2017-02.pdf

5.7.2 Pågående åtgärder

PTS har låtit genomföra en studie för att öka kunskapen om brandförlopp och hur bränder i försörjningstunnlar kan släckas snabbare, nu genomförs ett arbete som finansieras av PTS för att minska risken för brand i särskilda försörjningstunnlar. För att öka medvetenheten hos samhällsviktiga abonnenter att värdera de egna behoven av nätsäkerhet pågår arbetet med att uppdatera myndighetens vägledning för anskaffning av elektronisk kommunikation.

PTS har även låtit påbörja ett pilotprojekt för distribution av webbaserat innehåll så att samhällsviktig information skulle kunna vara tillgänglig även vid överbelastningsattacker. Åtgärder för att skydda särskilda förbindelser pågår kontinuerligt.

5.7.3 Planerade åtgärder

PTS planerar flera ytterligare åtgärder som kan påverka förmågan att motstå eller hantera mer omfattande nätsäkerhetshändelser, exempelvis:

- deltagande i och arrangerande av krisövningar[48] enligt PTS utbildnings och övningsstrategi,
- ökad redundans av hårdvara och förbindelser,
- fler och uppgraderade transportabla mobilbasstationer,
- fortsatt finansiering av mer robust fiberförläggning vid vattendrag för att minska konsekvenserna för förbindelserna, exempelvis vid dammbrott,
- förstärkning av reservkraft utöver föreskrivna krav där det är motiverat, och
- tillsyn för att granska efterlevnaden av PTS föreskrifter (PTSFS 2015:2 om driftsäkerhet och PTSFS 2014:1 om skydd av behandlade uppgifter)

5.8 Behov av ytterligare åtgärder med anledning av risk- och sårbarhetsanalysens resultat inom sektorn för elektronisk kommunikation

PTS har identifierat behov av åtgärder som kan förväntas skapa en ökad förmåga att motstå och hantera lokala och regionala nätsäkerhetshändelser och som därför inte heller ingår i redovisningen.

[48] T.ex. FMÖ 2020.

1 Bilagor

1.1 PTS metod för riskanalys för sektorn elektronisk kommunikation

I risk- och sårbarhetsanalysen sammanvägs sannolikheten för händelser som kan till leda mer allvarliga samhälleliga konsekvenser med bedömningar av graden av negativ samhällelig påverkan. Bilagan innehåller kompletterande beskrivningar av den metod och de kriterier som används för de riskbedömningar som redovisas i avsnitt 4.5.5.

1.1.1 Riskbedömningar följer en stegvis process

Riskbedömningen följer en stegvis process. I det första steget definieras hot, en kombination av en eller flera riskkällor och händelser som tillsammans kan påverka sektorn negativt. Varje sådan händelse tilldelas en sannolikhet som anger i vilken utsträckning som händelsen kan förväntas inträffa under en viss tidsperiod.

Som ett andra steg görs en bedömning av sannolikheten för att en inträffad händelse leder till negativa konsekvenser i beaktande av den resulterade sårbarheten. I det tredje steget sammanvägs sannolikheten att en händelse inträffar och att den leder till negativa konsekvenser. Denna sammanvägda sannolikhet ingår som del i riskbedömningen.

I det fjärde steget karaktäriseras de tekniska konsekvenserna som en händelse bedöms medföra. Det femte steget innehåller en bedömning av de samhälleliga konsekvenserna av nätsäkerhetshändelsen. I det sjätte steget sammanförs sannolikhet och samhällelig konsekvensbedömning till en risk med känslighetsanalys. De bedömningsgrunder som används i varje enskilt steg redovisas i de följande avsnitten.

1.1.2 Utgångspunkter för genomförande av riskbedömningar

Längden på den tidsperiod som används för riskbedömningen har satts till tio år. Längden är medvetet vald så att också långsiktiga risker, representerande händelser som i dagsläget bedöms som osannolika men som bedöms öka över tiden, kan inkluderas som del i risk- och sårbarhetsanalysen. De hot och sårbarheter som beskrivs bedöms vara giltiga under en femårsperiod eller längre.

Riskbedömningen genomförs för sådana händelser som kan leda till mer betydande samhällelig påverkan på nationell nivå. Tabell 1 ger en kvalitativ definition av orden.

Tabell 1 Definition av bestämningsord för värdering av händelser

Bestämningsord	Beskrivning
Långvarig	En händelse där samhällets anpassningsförmåga utsätts för påfrestningar och där de samhälleliga konsekvenserna inte kan förväntas vara av obetydlig och övergående natur.
Övervägande	En övervägande del av befolkningen drabbas av händelsen om en klar majoritet av befolkningen påverkas, direkt eller indirekt.
Upprepade	En serie händelser av samma grundorsak där samhällets anpassningsförmåga utsätts för påfrestningar och där de sammanlagda samhälleliga konsekvenserna inte kan förväntas vara av obetydlig och övergående natur.
Betydande	Informationstillgångar av betydande demokratiskt, ekonomiskt eller på annat sätt samhälleligt värde är sådana tillgångar där brister i tillgänglighet, konfidentialitet och riktighet påverkar ett eller flera nationella skyddsvärden negativt.

Bedömningen av de samhälleliga konsekvenserna utgår från den negativa påverkan som nätsäkerhetshändelsen orsakar. Det innebär exempelvis att konsekvensbedömningen för elavbrott omfattar den påverkan som de följande avbrotten i elektronisk kommunikation orsakar men inte den direkta negativa påverkan som elavbrotten i övrigt föranleder.

1.1.3 Steg 1: Kvalitativ bedömning av sannolikheten för att en händelse inträffar

Sannolikheten för en händelse är ett mått på i vilken utsträckning som den givna händelsen kan förväntas inträffa under den närmaste tioårsperioden. En kvalitativ bedömning sker i enlighet med kriterierna som redovisas i tabellen nedan.

Tabell 2 Definition av kriterier för kvalitativ bedömning av sannolikheten för att en händelse inträffar under det närmaste decenniet.

Nivå	Beskrivning
Mycket hög	Händelsen kommer nästan säkert att inträffa
Hög	Händelsen kommer med stor sannolikhet att inträffa
Medel	Händelsen kan inträffa

Låg	Händelsen förväntas inte inträffa
Mycket låg	Händelsen är mycket osannolik

1.1.4 Steg 2: Kvalitativ bedömning av sannolikheten för negativa konsekvenser

En händelse behöver inte nödvändigtvis leda till negativa konsekvenser. Exempelvis kan elavbrott pågå under så kort tid att sannolikheten för att det uppstår negativa konsekvenser inom sektorn är mycket liten. I riskbedömningen ingår både sannolikheten för att en händelse inträffar (steg 1) och sannolikheten för att händelsen leder till någon form av beaktansvärda negativa konsekvenser för elektronisk kommunikation, givet att händelsen inträffar (steg 2). Denna betingade sannolikhet bedöms enligt kriterierna i tabellen nedan.

Tabell 3 Definition av kriterier för kvalitativ bedömning av sannolikheten för negativa konsekvenser.

Nivå	Beskrivning
Mycket hög	Om händelsen inträffar är det närmast säkert att händelsen får negativa konsekvenser.
Hög	Om händelsen inträffar är det sannolikt att händelsen får negativa konsekvenser.
Medel	Om händelsen inträffar är det möjligt att händelsen får negativa konsekvenser.
Låg	Om händelsen inträffar är det osannolikt att händelsen får negativa konsekvenser.
Mycket låg	Om händelsen inträffar är det mycket osannolikt att händelsen får negativa konsekvenser.

1.1.5 Steg 3: Sammanvägning av sannolikheter

Den risk som ska associeras med en viss händelse ska dels avspegla sannolikheten för negativa konsekvenser, dels omfattningen av dessa samhälleliga konsekvenser. Sannolikheten för negativa konsekvenser beror av både sannolikheten att en händelse inträffar (steg 1) och sannolikheten att händelsen leder till negativa konsekvenser givet att den inträffar (steg 2). Tabell 4 visar hur de båda sannolikheterna tillsammans används för att tillskriva en sammanvägd sannolikhet i riskbedömningen.

Tabell 4 Sammanvägning av sannolikhet för att en händelse inträffar med sannolikheten för negativa konsekvenser.

		Sannolikhet för negativa konsekvenser				
		Mycket låg	Låg	Medel	Hög	Mycket hög
Sannolikhet för händelse	Mycket hög	Låg	Medel	Hög	Mycket hög	Mycket hög
	Hög	Låg	Medel	Hög	Hög	Mycket hög
	Medel	Mycket låg	Låg	Medel	Medel	Hög
	Låg	Mycket låg	Låg	Låg	Låg	Medel
	Mycket låg	Mycket låg	Mycket låg	Mycket låg	Låg	Låg

1.1.6 Steg 4: Karaktärisering av tekniska konsekvenser

En teknisk bedömning beskriver de konsekvenser för elektronisk kommunikation som en händelse medför. Händelser där informationstillgångars tillgänglighet värderas utgående från vissa nivåer och kriterier. Händelser där informationstillgångars konfidentialitet eller riktighet påverkas värderas utgående från andra bedömningsgrunder.

Kriterier och nivåer för händelser som påverkar tillgänglighet

I de fall en händelse leder till avbrott inom sektorn, bedöms konsekvenserna i tre dimensioner:

- *operatörer*: det antal operatörer med nationell påverkan som drabbas av avbrott,
- *tjänster*: det antal tjänster med möjlig samhällspåverkan som påverkas av avbrottet,
- *längd*: omfattningen i tid med en indelning efter korta, medellånga och långa avbrott utan direkta, kvantitativa kopplingar till faktisk tid.

I varje dimension används nivåer för att beteckna graden av påverkan. De nivåer som definierar antalet operatörer framgår av tabell 5.

Tabell 5 Nivåer och kriterier för antalet operatörer som drabbas av avbrott.

Operatörer	Beskrivning
Flertal	Avbrottet påverkar ett flertal operatörer med betydande marknadsinflytande och därmed huvuddelen av alla abonnenter och samhällsviktiga verksamheter i landet
Fåtal	Avbrottet påverkar ett mindre antal operatörer med betydande marknadsinflytande och därmed en ansenlig mängd abonnenter och samhällsviktiga verksamheter i landet.
En	Avbrottet påverkar endast en operatör med betydande marknadsinflytande eller med en betydande andel samhällsviktiga verksamheter som kunder.

Inte enbart antalet operatörer påverkar de samhälleliga konsekvenserna av avbrott. Även antalet tjänster är en påverkansfaktor.

Tabell 6 Nivåer och kriterier för antalet tjänster som påverkas av avbrott.

Tjänster	Beskrivning
Flertal	Avbrottet påverkar flertalet tjänster som används av privatpersoner, företag och organisationer och där ett avbrott påverkar något samhälleligt skyddsvärde negativt.
Fåtal	Avbrottet påverkar ett mindre antal tjänster som används av privatpersoner, företag och organisationer och där ett avbrott påverkar något samhälleligt skyddsvärde negativt.
En	Avbrottet påverkar endast en tjänst som används av privatpersoner, företag och organisationer och där ett avbrott påverkar något samhälleligt skyddsvärde negativt.

Motsvarande nivåer och kriterier för avbrottets förväntade längd framgår av tabell 7.

Tabell 7 Nivåer och kriterier för avbrottets förväntade längd.

Längd	Beskrivning
Långvarigt	Avbrottet kan förväntas pågå under längre tid Exempel: Avbrottet varar flera dygn
Medellångt	Avbrottet kan förväntas pågå en begränsad tid Exempel: Avbrottet varar en stor del av ett dygn
Kortvarigt	Avbrottet kan förväntas pågå under en kort tid Exempel: Avbrottet varar någon eller några timmar

Nivåer och kriterier för händelser som påverkar informationstillgångars konfidentialitet och riktighet

I de fall en händelse leder till att informationens konfidentialitet eller riktighet inte kan upprätthållas, bedöms konsekvenserna i dimensionerna:

- *operatörer*: det antal operatörer som påverkas av händelsen,
- *information*: omfattningen av de informationstillgångar vars konfidentialitet eller riktighet inte kan upprätthållas,
- *längd*: i tid med en indelning som konfidentialitet och riktighet inte kan upprätthållas.

Antalet operatörer som påverkas bedöms enligt samma kriterier som för händelser som påverkar tillgänglighet enligt Tabell . Omfattningen av en händelse ska avspegla den sammanlagda mängd skyddsvärd information som påverkas enligt nivåerna och kriterierna i tabell 8.

Tabell 8 Nivåer och kriterier för omfattningen av en händelse som påverkar konfidentialitet eller riktighet.

Omfattning	Beskrivning
Fullständig	Huvuddelen av informationstillgångars konfidentialitet eller riktighet kan inte upprätthållas. Exempel: Abonnentinformation, kommunikationsmönster och innehåll i elektronisk kommunikation kan inte skyddas.
Omfattande	Flera eller stora delar av informationstillgångars konfidentialitet eller riktighet kan inte upprätthållas.

	Exempel: Abonnentinformation och övergripande kommunikationsmönster kan inte skyddas.
Begränsad	Vissa, enskilda informationstillgångars konfidentialitet eller riktighet kan inte upprätthållas. Exempel: Konfidentialitet för vissa, övergripande abonnentinformation kan inte bevaras.

Motsvarande nivåer och kriterier för informationsincidentens förväntade längd framgår av tabell 9.

Tabell 9 Nivåer och kriterier för informationsincidentens förväntade längd.

Längd	Beskrivning
Långvarigt	Incidenten kan förväntas pågå under längre tid Exempel: Incidenten varar flera månader
Medellångt	Incidenten kan förväntas pågå en begränsad tid Exempel: Incidenten varar under ett fåtal dagar
Kortvarigt	Incidenten kan förväntas pågå under en kort tid Exempel: Incidenten varar under en del av en dag

1.1.7 Steg 5: Sammanvägning av tekniska konsekvenser till samhälleliga konsekvenser

Sammanvägningen av den tekniska konsekvensbedömningen till samhälleliga konsekvenserna sker genom resonerande bedömningar som utgår från den tekniska konsekvensbedömningen med kriterier enligt tabell 10.

Tabell 10 Nivåer för bedömning av samhälleliga konsekvenser.[49]

Nivå	Beskrivning
Mycket hög	Katastrofala direkta eller mycket stora indirekta hälsoeffekter, extrema störningar i samhällets funktionalitet, grundmurad misstro mot samhällsinstitutioner och allmän instabilitet, katastrofala skador på egendom och miljö.
Hög	Mycket stora direkta eller betydande indirekta hälsoeffekter, mycket allvarliga störningar i samhällets funktionalitet, bestående misstro mot flera samhällsinstitutioner och förändrat beteende, mycket allvarliga skador på egendom och miljö.

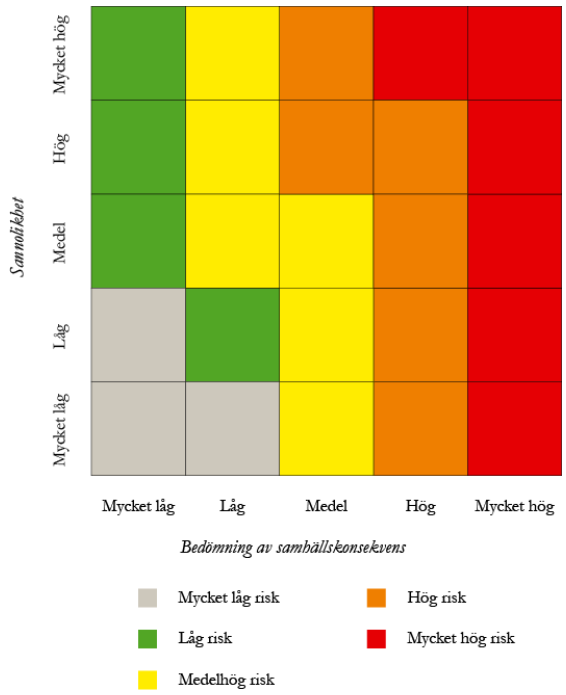
[49] Vägledning för Risk- och sårbarhetsanalyser, MSB, publikationsnummer MSB245.

Medel	Betydande direkta eller måttliga indirekta hälsoeffekter, allvarliga störningar i samhällets funktionalitet, bestående misstro mot flera samhällsinstitutioner eller förändrat beteende, allvarliga skador på egendom och miljö.
Låg	Måttliga direkta hälsoeffekter, begränsade störningar i samhällets funktionalitet, övergående misstro mot flera samhällsinstitutioner, begränsade skador på egendom och miljö.
Mycket låg	Små direkta hälsoeffekter, mycket begränsade störningar i samhällets funktionalitet, övergående misstro mot enskild samhällsinstitution, mycket begränsade skador på egendom och miljö.
Obetydliga	Mindre allvarliga effekter än de som anges för övriga nivåer.

1.1.8 Steg 6: Riskbedömning och känslighetsanalys

Riskbedömningen utgår från sammanvägningen av de samhälleliga konsekvenserna och sannolikheten på det sätt som framgår av figur 1.

Figur 1 Risknivåer och deras koppling till konsekvens- och sannolikhetsbedömningar.



De riskbedömningar som redovisas i risk- och sårbarhetsanalysen är alla förknippande med någon form av osäkerhet. På samma sätt kommer naturligt förekommande variationer, exempelvis längden på avbrott i elektronisk kommunikation som orsakas av en viss typ av händelse, påverka risk-bedömningar. Varje enskild riskbedömning följs av en känslighetsanalys som beskriver de variationer som därmed kan förväntas.