Från: [redacted]
Ärende: Remiss av förslag till nya föreskrifter och allmänna råd om säkerhet i nät och tjänster (PTS dnr: 20-3324)
Datum: den 2 mars 2022 09:54:38
Bilagor: Konsekvensutredning föreskrifter och allmänna råd om säkerhet i nät och tjänster.pdf
Förslag till föreskrifter och allmänna råd om säkerhet i nät och tjänster.pdf
Missiv Remiss av nya föreskrifter och allmänna råd om säkerhet i nät och tjänster_final.pdf
Sändlista_final.pdf

Hej!
Post- och telestyrelsen (PTS) ger er härmed tillfälle att yttra er över förslag till nya föreskrifter och allmänna råd om säkerhet i nät och tjänster. För förslag till nya föreskrifter, konsekvensutredning inklusive kostnadssammanställning, missiv och sändlista, se bifogade dokument.

Om ni vill yttra er över förslaget till föreskrifter om säkerhet i nät och tjänster och konsekvensutredningen ska ett skriftligt yttrande ha inkommit till PTS senast **den 1 april 2022**. PTS tar emot svar i elektronisk form till adressen pts@pts.se. Vänligen ange diarienummer 20-3324 och PTS säkerhetsföreskrifter i ärenderaden. Frågor rörande remissen skickas till pts@pt.se.

Please find attached The Swedish Post and Telecom Authority's (PTS) proposal on new secondary legislation regarding security in networks and services. The proposal, in Swedish only, is hereby the subject of public consultation, please send your comments to pts@pts.se **by April 1 2022** at the latest, and use 20-3324 and "secondary legislation security in networks and services" as reference in the subject line. It is not mandatory to comment.

Hälsningar,

Erika Hersaeus
Uppdragsledare säkerhetsföreskrifter fr.o.m. extern remiss

Post- och telestyrelsen (PTS)
Avdelningen för säker kommunikation

Telefon: 08-678 57 75
Mobil: 0736 44 57 75
erika.hersaeus@pts.se
https://www.pts.se

Vår referens: 20-3324, **Ert datum:** 2022-03-02

Sändlista med anledning av remiss av förslag till nya föreskrifter och allmänna råd om säkerhet i nät och tjänster

Remissen skickas till följande mottagare:

Tillhandahållare av elektroniska kommunikationsnät och -tjänster

Hallstahammars kommun

Vårgårda Stadsnät AB

Malungs Elnät AB

Obduro Network AB

STADSNÄT I ÅMÅL AB

VaraNet AB

Lycksele kommun

Överkalix kommun

Nordmalings kommun

Strömsunds kommun

Open Infra Operator AB

Sollefteå kommun

Sundbyberg Stadsnätsbolag AB

Mark Kraftvärme AB

Post- och telestyrelsen
Postadress: Box 6101, 102 32 Stockholm
Besöksadress: Hälsingegatan 38
Telefon: 08-678 55 00
E-post: pts@pts.se
www.pts.se

Ronneby Miljö & Teknik AB

C4 Elnät AB

AB STOKAB

AB strömstaNET

Fast Fiber Connection i Sverige AB

Telephonia Telecom AB

Vodafone Enterprise Sweden AB

Voice Integrate Nordic AB

Awiwo AB

ITTRE Sverige AB

Rockan Data Center AB

IT4U Sweden AB

PEMA kommunikationer AB

ITCONNECT Scandinavia AB

Add Logo Telecom AB

Tictic AB

Hammarö Kommun/Stadsnät

Wexnet AB

Orange Business Sweden AB

Gävle Energi AB

A3 Privat AB

Halmstads stadsnät AB

Skellefteå Kraft Fibernät AB

Arkaden Konsult AB

Winther Wireless AB

Lyssna & Njut AB

Primlight AB

Finspångs Stadsnät, Finet AB

Bredbandsson AB

Stockholms Stadsnät AB

Visolit Sweden AB

Eniro 118118 AB

Telavox AB

Canal Digital AB (Allente)

VCB Sweden AB (Allente)

Telia Company AB

Telenor Sverige AB

Tele2 Sverige AB

Hi3G Access AB

T-MOBILE HOTSPOT GMBH

GTT International B.V.

Soracom DK ApS

DIDWW Ireland Ltd

DNA Oyj

e-BO Enterprises NV

Inmarsat Ventures SE

Google Voice Ltd

Mobiweb Ltd

LINK Mobility A/S

euNetworks Fiber UK Limited

Infobip Limited UK

CITIC Telecom CPC Sweden AB

Talli AB

OrbiGo AB

Globetouch AB

AecorLink AB

Megaport (Sweden) AB

Mobile Network Scandinavia AB

Loxysoft AB

JT Technologies & Telecommunications AB

iTUX Communication AB

Kalix Tele24 AB

Sierra Wireless Sweden AB

Bosnet AB

Netnod Internet Exchange i Sverige AB

46elks AB

STORADIO AERO AB

Robertsfors kommun

Vallebygdens Energi Ekonomiska förening

Dala Energi Fibernät AB

Hjo Energi AB

InfraCom Managed Services AB

Quality of Service Networks Sweden AB

BoreNet AB

Köpings Kabel-TV AB

Balder Tech AB

WCOM AB

Aurora Innovation AB

Voice Provider Sweden AB

Teracom AB

Trafikverket

Starlink Internet Services Limited

Global Connect AB

Vattenfall AB

Facebook Sweden AB

Omnitor AB

T-Meeting (Europea i Malmö AB)

nWise AB

Google Sweden AB

Mötesplatsen (Schibstedt AB)

Match.com Nordic AB

Cisco Sverige AB

Cisco Systems Sverige AB

Microsoft Sweden AB

Myndigheter

Regelrådet

Polismyndigheten

Säkerhetspolisen

Integritetsskyddsmyndigheten

Myndigheten för samhällsskydd och beredskap

Statens energimyndighet

Finansinspektionen

Inspektionen för vård och omsorg

Livsmedelsverket

Försvarsmakten

Försvarets materielverk

Försvarets radioanstalt

Kommerskollegium

Konkurrensverket

Konsumentverket

Myndigheten för delaktighet

Myndigheten för press, radio och tv

Svenska kraftnät

Transportstyrelsen

Vinnova

Företag

Ericsson AB

Huawei Technologies Sweden AB

Intertek SEMKO AB

Branschorganisationer och andra organisationer

Elektronikbranschen

ITS Svenska Informations- och Telekommunikationsstandardiseringen

MTB MobilTeleBranschen

SOS Alarm

Sveriges kommuner och regioner

Svensk Handel

Svenska stadsnätsföreningen

Svenskt Näringsliv

Tech Sverige

Teknikföretagen

Telekområdgivarna

Enligt sändlista

Vår referens: 20-3324, **Ert datum:** 2020-03-02

Remiss av förslag till nya föreskrifter och allmänna råd om säkerhet i nät och tjänster

Post- och telestyrelsen (PTS) ger er härmed tillfälle att yttra er över förslag till nya föreskrifter och allmänna råd om säkerhet i nät och tjänster som upphäver och ersätter följande föreskrifter:

- Post- och telestyrelsens föreskrifter (PTSFS 1995:1) om fredstida planering för totalförsvarets behov av telekommunikation m.m.,
- Post- och telestyrelsens föreskrifter och allmänna råd (PTSFS 2012:2) om rapportering av störningar eller avbrott av betydande omfattning,
- Post- och telestyrelsens föreskrifter och allmänna råd (PTSFS 2012:4) om skyddsåtgärder i samband med lagring och annan behandling av uppgifter för brottsbekämpande ändamål,
- Post- och telestyrelsens föreskrifter och allmänna råd (PTSFS 2014:1) om skyddsåtgärder för behandlade uppgifter, samt
- Post- och telestyrelsens föreskrifter (PTSFS 2015:2) om krav på driftsäkerhet.

De nya föreskrifterna kompletterar skyldigheterna i 1 kap. 11 § samt 8 kap. 1, 3 – 6 och 9 §§ lagen (2022:XX) om elektronisk kommunikation (nya LEK).

Förslaget till nya säkerhetsföreskrifter och konsekvensutredning bifogas samt finns tillgängliga på PTS webbplats, www.pts.se .

Post- och telestyrelsen
Postadress: Box 6101, 102 32 Stockholm
Besöksadress: Hälsingegatan 38
Telefon: 08-678 55 00
E-post: pts@pts.se
www.pts.se

Bakgrund till förslaget

Regeringen har föreslagit en ny lag som ersätter den nuvarande lagen om elektronisk kommunikation (LEK). Den nya lagen genomför EU:s direktiv[1] om inrättande av en europeisk kodex för elektronisk kommunikation. Nya LEK föreslås träda i kraft den 1 augusti 2022. I samband med detta har PTS tagit fram förslag till nya föreskrifter. Dessa föreslås träda ikraft den 1 augusti 2022, samma dag som nya LEK träder ikraft.

De nya föreslagna föreskrifterna syftar till att säkerställa att bestämmelserna står i överensstämmelse med den överordnade regleringen samt att de motsvarar en säkerhetsnivå som är lämplig i förhållande till riskerna för incidenter och samhällets behov av säker elektronisk kommunikation, tydliggör vilka säkerhetsåtgärder som tillhandahållare ska vidta i sin verksamhet för att hantera risker för incidenter.

Förslagets innehåll

PTS nu föreslagna föreskrifter och allmänna råd innebär en hopslagning av flera gällande föreskrifter inom säkerhetsområdet till en regelsamling i syfte att underlätta för tillhandahållarna. Förslaget till föreskrifter specificerar och kompletterar skyldigheterna i nya LEK. I sak motsvarar förslaget till de nya föreskrifterna i stora delar de nuvarande föreskrifterna. Vissa krav förtydligas och vissa ändringar och tillägg görs.

Föreskrifterna innehåller bl.a. krav på det övergripande säkerhetsarbetet, riskanalys, åtgärder efter riskbedömning, åtgärder avseende åtkomst och behörighet, loggning, kryptering, redundans och reservkraft, åtgärder avseende övervakning och beredskap, fredstida planering för totalförsvarets behov av elektroniska kommunikationer, information till användare om konkret och betydande hot om en säkerhetsincident samt rapportering av säkerhetsincidenter till PTS.

Konsekvenserna som redogörs för i tillhörande konsekvensutredning uppkommer med anledning av de materiella ändringar och kompletteringar som genomförs i sak i förhållande till nu gällande föreskrifter.

Ert yttrande

Om ni vill yttra er över förslaget till föreskrifter och allmänna råd och konsekvensutredningen ska ett skriftligt yttrande ha inkommit till PTS **senast den 1 april 2022**. PTS tar emot svar i elektronisk form till adressen pts@pts.se. Vänligen ange diarienummer 20-3324 och PTS säkerhetsföreskrifter i ärenderaden. PTS föreskrifter är avsedda att träda i kraft den 1 augusti 2022.

[1] Europaparlamentets och rådets direktiv (EU) 2018/1972 om inrättande av en europeisk kodex för elektronisk kommunikation

Frågor rörande remissen skickas till pts@pts.se, ange diarienummer 20-3324 - PTS säkerhetsföreskrifter.

De handlingar som bifogas är:

1. Konsekvensutredning

2. Förslag till föreskrifter och allmänna råd om säkerhet i nät och tjänster

3. Missiv

4. Sändlista

Vår referens: Dnr 20-3324

Konsekvensutredning avseende föreskrifter och allmänna råd om säkerhet i nät och tjänster

Post- och telestyrelsen (PTS) föreslår nya föreskrifter och allmänna råd om säkerhet i nät och tjänster m.m. (de nya föreskrifterna) som upphäver och ersätter följande föreskrifter.

- Post- och telestyrelsens föreskrifter (PTSFS 1995:1) om fredstida planering för totalförsvarets behov av telekommunikation m.m.,
- Post- och telestyrelsens föreskrifter och allmänna råd (PTSFS 2012:2) om rapportering av störningar eller avbrott av betydande omfattning,
- Post- och telestyrelsens föreskrifter och allmänna råd (PTSFS 2012:4) om skyddsåtgärder i samband med lagring och annan behandling av uppgifter för brottsbekämpande ändamål,
- Post- och telestyrelsens föreskrifter och allmänna råd (PTSFS 2014:1) om skyddsåtgärder för behandlade uppgifter, samt
- Post- och telestyrelsens föreskrifter (PTSFS 2015:2) om krav på driftsäkerhet.

De nya föreskrifterna kompletterar skyldigheterna i 1 kap. 11 § samt 8 kap. 1, 3 – 6 och 9 §§ lagen (2022:XX) om elektronisk kommunikation (nya LEK).

I sak motsvarar de nya föreskrifterna i stora delar de nuvarande föreskrifterna.

Flera bestämmelser i de nuvarande föreskrifterna föreslås överföras till de nya föreskrifterna oförändrade eller med enbart språkliga eller redaktionella ändringar. Det görs dock även ändringar i sak i vissa fall som föranleds av ändringar i den överordnade regleringen och samhällets behov av säker elektronisk kommunikation. Föreskrifterna syftar till att säkerställa att elektroniska kommunikationsnät och -tjänster är säkra.

De nya föreskrifterna föreslås att träda i kraft den 1 augusti 2022 vilket är samma dag som nya LEK träder i kraft.

Post- och telestyrelsen
Postadress: Box 6101, 102 32 Stockholm
Besöksadress: Hälsingegatan 38, Stockholm
Telefon: 08-678 55 00
E-post: pts@pts.se
www.pts.se

Innehållsförteckning

1. Inledning

PTS är den myndighet som ansvarar för området för elektronisk kommunikation i Sverige.

PTS arbetar för att det ska finnas en fungerande marknad för elektronisk kommunikation i Sverige där aktörerna tillhandahåller en mångfald av kommunikationstjänster. Konkurrensen ska vara hållbar, resurser som frekvenser och nummer ska utnyttjas effektivt och kommunikationerna ska vara säkra. Då skapas en långsiktig nytta för konsumenterna och viktiga aktörer i samhället. PTS arbetar för att skapa goda förutsättningar för att marknaden ska fungera och griper in där det finns brister.

Elektroniska kommunikationsnät- och tjänster utgör en grundläggande funktion för att dagens samhälle ska fungera. Sverige är beroende av fungerande elektroniska kommunikationer i såväl normalläge som i kris, höjd beredskap och krig. Elektroniska kommunikationer används i allt från att ringa ett telefonsamtal och söka information till att genomföra finansiella transaktioner, styra och övervaka industriella processer samt för att nödkommunicera och leda insatser vid kriser och katastrofer.

Det är viktigt att kunna utnyttja möjligheterna med elektronisk kommunikation och samtidigt undvika de negativa konsekvenser som kan uppstå om nät och tjänster har bristande säkerhet. Det är således viktigt att säkerheten upprätthålls och att näten och tjänsterna inte drabbas av störningar och avbrott samt att uppgifter om personer och deras kommunikation behandlas på ett korrekt sätt och skyddas.

PTS verkar för att samhällets behov av robust och säker kommunikation ska tillgodoses i normalläge, men även i kris och vid höjd beredskap.

För att uppnå detta arbetar PTS bl.a. med att ta fram reglering och myndigheten har utfärdat ett flertal föreskrifter inom området.

PTS har identifierat ett behov av att se över och ändra bestämmelserna i ett antal av dessa föreskrifter. Behovet har uppstått till följd av att det införs ändringar i den överordnade regleringen och mot bakgrund av de förändringar i samhället som skett sedan de nuvarande föreskrifterna trädde i kraft.

Syftet med översynen och ändringarna är således att säkerställa att PTS föreskrifter står i överensstämmelse med den överordnade regleringen samt att de motsvarar en

säkerhetsnivå som är lämplig i förhållande till riskerna för incidenter och samhällets behov av säker elektronisk kommunikation.

Avsnitten 1.1 och 1.2 innehåller en beskrivning av de förändringar som ligger till grund för PTS förslag. Avsnitt 2 innehåller en beskrivning av problemen, vad PTS vill uppnå och alternativa lösningar. Avsnitt 3 innehåller en beskrivning av de rättsliga förutsättningarna.

De som berörs av förslagen är främst de som tillhandahåller elektroniska kommunikationsnät och elektroniska kommunikationstjänster samt de som använder sådana tjänster. I avsnitten 6–13 redovisas de konsekvenser av förslaget som bedöms vara av betydelse. Det inkluderar en redovisning av de föreslagna bestämmelserna innebär (avsnitt 6). Avsnitt 4 beskriver de tillhandahållare som berörs av förslaget. Avsnitt 5 redovisar de samråd PTS har genomfört under arbetets gång. Avsnitt 14 innehåller en beskrivning av vissa övriga frågor.

I denna konsekvensutredning används begreppen

- ”kommunikationsnät” och ”nät” synonymt med begreppet ”elektroniskt kommunikationsnät” så som det definieras i nya LEK,
- ”kommunikationstjänst” och ”tjänst” synonymt med begreppet ”elektronisk kommunikationstjänst” så som det definieras i nya LEK,
- ”åtgärder” och ”säkerhetsåtgärder” för de åtgärder som ska vidtas enligt 8 kap. 1, 5 och 6 §§ nya LEK jämte de föreslagna föreskrifterna,
- ”tillhandahållare”, ”aktör” eller ”företag” för den som tillhandahåller ett allmänt elektroniskt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst, samt
- ”behandlade uppgifter” för de uppgifter som behandlas i samband med tillhandahållande av kommunikationsnät eller kommunikationstjänster och som ska skyddas enligt 8 kap. 1, 5 och 6 §§ nya LEK.

1.1 Ett nytt direktiv och en ny lag

1.1.1 Nuvarande reglering

Lagen (2003:389) om elektronisk kommunikation (nuvarande LEK) syftar till att enskilda och myndigheter ska få tillgång till säkra och effektiva elektroniska kommunikationer och största möjliga utbyte när det gäller urvalet av elektroniska kommunikationstjänster samt deras pris och kvalitet (1 kap. 1 § nuvarande LEK).

Den EU-rättsliga regleringen på området för elektronisk kommunikation, som består av nedanstående direktiv, genomförs i huvudsak genom nuvarande LEK.

- Europaparlamentets och rådets direktiv 2002/21/EG om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektivet),
- Europaparlamentets och rådets direktiv 2002/19/EG om tillträde till och samtrafik mellan elektroniska kommunikationsnät och tillhörande faciliteter (tillträdesdirektivet),
- Europaparlamentets och rådets direktiv 2002/20/EG om auktorisation för elektroniska kommunikationsnät och kommunikationstjänster (auktorisationsdirektivet),
- Europaparlamentets och rådets direktiv 2002/22/EG om samhällsomfattande tjänster och användares rättigheter (USO-direktivet), och
- Europaparlamentets och rådets direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (e-dataskyddsdirektivet).

Nuvarande LEK reglerar ett flertal olika områden varav ett är säkerhet. Nuvarande LEK ålägger tillhandahållare bl.a. följande skyldigheter inom området.

- Enligt 1 kap. 8 § nuvarande LEK är tillhandahållare skyldiga att i fredstid planera för totalförsvarets behov av elektroniska kommunikationer i höjd beredskap och krig.
- Enligt 5 kap. 6 b § nuvarande LEK ska tillhandahållare vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att verksamheten uppfyller rimliga krav på driftsäkerhet.
- Enligt 5 kap. 6 c § nuvarande LEK ska tillhandahållare utan onödigt dröjsmål till tillsynsmyndigheten rapportera störningar eller avbrott av betydande omfattning.
- Enligt 6 kap. 3 § nuvarande LEK ska tillhandahållare vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att uppgifter som behandlas i samband med tillhandahållandet av tjänsten skyddas.
- Enligt 6 kap. 3 a § nuvarande LEK ska den som är skyldig att lagra uppgifter enligt 16 a § vidta de särskilda tekniska och organisatoriska åtgärder som behövs för att skydda de lagrade uppgifterna vid behandling.
- Enligt 6 kap. 4 b § nuvarande LEK ska tjänstetillhandahållare löpande föra en förteckning över integritetsincidenter.

Skyldigheterna utgör delvis det svenska genomförandet av bestämmelserna i ramdirektivet och e-dataskyddsdirektivet.

PTS har i anslutning till de ovan nämnda skyldigheterna i nuvarande LEK meddelat PTSFS 1995:1, PTSFS 2012:2, PTSFS 2012:4, PTSFS 2014:1 och PTSFS 2015:2.

PTSFS 1995:1 innehåller bestämmelser om den planering som tillhandahållare är skyldiga att genomföra i fredstid för de behov av elektronisk kommunikation som totalförsvaret kan ha i höjd beredskap och krig. PTSFS 2012:2 innehåller bestämmelser om när och hur rapportering av driftstörningar och avbrott ska ske till PTS. PTSFS 2012:4, PTSFS 2014:1 och PTSFS 2015:2 innehåller bestämmelser om de åtgärder tillhandahållare ska vidta för att hantera risker för olika typer av incidenter. PTSFS 2012:4 gäller specifikt skydd av uppgifter som lagras för brottsbekämpande ändamål. PTSFS 2014:1 gäller specifikt skydd av uppgifter som behandlas i samband med tillhandahållandet av tjänster. PTSFS 2015:2 gäller driftsäkerhet i nät och tjänster.

Bestämmelserna i nuvarande LEK och i PTS föreskrifter gäller samtliga tillhandahållare av nät och tjänster.[1] Reglerna utgör grundnivån avseende säkerhet som samtliga tillhandahållare måste säkerställa och bekosta. Det utgör också grundnivån för vad slutanvändare kan förvänta sig från sin tillhandahållare.

1.1.2 Kodexen och e-dataskyddsdirektivet

Den 11 december 2018 antogs Europaparlamentets och rådets direktiv (EU) 2018/1972 om inrättande av en europeisk kodex för elektronisk kommunikation (kodexen). Före antagandet av kodexen bestod det EU-rättsliga regelverket för elektronisk kommunikation av framför allt ramdirektivet, tillträdesdirektivet, auktorisationsdirektivet, USO-direktivet och e-dataskyddsdirektivet. Kodexen är en omarbetning av och ersätter samtliga dessa direktiv förutom e-dataskyddsdirektivet.

E-dataskyddsdirektivet är ett direktiv som preciserar och kompletterar Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (EU:s dataskyddsförordning). Målsättningen från EU:s sida är att även e-dataskyddsdirektivet ska upphävas och att det direktivet ska ersättas av en ny förordning. EU-kommissionen har tagit fram ett förslag till en förordning som ska upphäva och ersätta e-dataskyddsdirektivet men det förslaget förhandlas fortfarande och är inte antaget.[2]

Till dess att e-dataskyddsdirektivet upphävs och ersätts kommer således både det direktivet och kodexen att gälla. Båda direktiven innehåller bestämmelser om säkerhetsåtgärder och incidentrapportering. Gällande incidentrapporteringen som ska ske enligt e-dataskyddsdirektivet kompletteras den skyldigheten av

[1] Förutom PTSFS 2014:1 som endast gäller tjänstetillhandahållare

[2] Förslag till Europaparlamentets och rådets förordning om respekt för privatlivet och skydd av personuppgifter i samband med elektronisk kommunikation och om upphävande av direktiv 2002/58/EG (förordning om integritet och elektronisk kommunikation), COM/2017/010 final - 2017/03 (COD).

kommissionens förordning (EU) nr 611/2013 av den 24 juni 2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott enligt Europaparlamentets och rådets direktiv 2002/58/EG vad gäller personlig integritet och elektronisk kommunikation (förordning 611/2013).

Förhållandet mellan kodexen och e-dataskyddsdirektivet regleras i artikel 40.4 i kodexen där det framgår att bestämmelser om säkerhetsåtgärder och incident-rapportering i kodexen inte ska påverka tillämpningen av e-dataskyddsdirektivet.

1.1.3 Nya LEK

För att genomföra kodexen har regeringen föreslagit en ny lag, nya LEK.[3] Nya LEK föreslås träda i kraft den 1 juni 2022. Samtidigt föreslås nuvarande LEK och lagen (2003:390) om införande av lagen (2003:389) om elektronisk kommunikation att upphöra att gälla.

Bestämmelser om den fredstida planeringen för totalförsvarets behov av elektroniska kommunikationer, säkerhetsåtgärder samt rapportering av säkerhets- och integritetsincidenter finns i 1 kap. 11 § och 8 kap. nya LEK.

Bestämmelserna inom säkerhetsområdet i nya LEK motsvarar delvis nuvarande LEK, dock med de ändringar och tillägg som föranleds av kodexen. Det innebär att vissa delar av nuvarande LEK förs oförändrade över till nya LEK medan andra delar innehåller ett antal nyheter och tillägg. Följande nyheter och tillägg är av relevans för detta föreskriftsarbete.

Utökat tillämpningsområde

En övergripande förändring är utvidgningen av begreppet ”elektronisk kommunikationstjänst” och vilka tjänster som därmed omfattas av nya LEKs tillämpningsområde.

Utvidgningen innebär att även nummeroberoende interpersonella kommunikationstjänster (*Number-independent interpersonal communications service*, NI-ICS) omfattas av viss reglering, bl.a. regler inom säkerhetsområdet. Det gäller både regleringen som genomför kodexen och som genomför e-dataskyddsdirektivet.[4]

---

[3] Prop. 2021/22:136 *Genomförande av direktivet om inrättande av en europeisk kodex för elektronisk kommunikation.*

[4] Bestämmelser om säkerhetsåtgärder och incidentrapportering i e-dataskyddsdirektivet (artikel 4) ska tillämpas av tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster. Enligt artikel 2 i e-dataskyddsdirektivet ska definitionerna i ramdirektivet gälla. Ramdirektivet ska enligt kodexen upphöra att gälla med verkan från och med den 21 december 2020. Hänvisningar till det direktivet ska då, enligt

NI-ICS är interpersonella kommunikationstjänster som inte använder allmänt tilldelade nummerresurser och definieras i 1 kap. 7 § nya LEK.

Utgångspunkten för att inkludera även NI-ICS motiveras med att dessa tjänster är funktionellt likvärdiga med traditionell taltelefoni, sms och e-post. Definitionen av elektroniska kommunikationstjänster ändras därför så att den är funktionellt baserad snarare än baserad på enbart tekniska parametrar.[5]

Nytt säkerhetsbegrepp

Kodexen, som genomförs i nya LEK, innebär en ändring av säkerhetsregleringen i förhållande till ramdirektivet, som genomförs i nuvarande LEK, genom att det i artikel 2.21 införs en definition av begreppet ”säkerhet för nät och tjänster”[6]. Definitionen förtydligar att säkerhet omfattar fyra aspekter: tillgänglighet, autenticitet, riktighet och konfidentialitet.[7] Det införs även i artikel 2.42 i kodexen en ny definition av begreppet ”säkerhetsincident”[8].

Ramdirektivet och kodexen innehåller skyldigheter för medlemsstaterna att säkerställa att tillhandahållare av nät och tjänster vidtar ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att på ett lämpligt sätt hantera risker som hotar näts och tjänsters säkerhet samt att tillhandahållarna utan onödigt dröjsmål rapporterar om säkerhetsincidenter som har haft en betydande påverkan på driften av nät och tjänster.

Ramdirektivets bestämmelser har i svensk rätt genomförts i 5 kap. 6 b och 6 c §§ nuvarande LEK. Enligt 5 kap. 6 b § nuvarande LEK ska den som tillhandahåller allmänna nät och tjänster vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att verksamheten uppfyller rimliga krav på *driftsäkerhet*. Med driftsäkerhet avses förmågan att upprätthålla avsedd funktion och skydd mot oönskad påverkan eller förändring i ett nät eller system.[9] Enligt 5 kap. 6 c § nuvarande LEK ska den som

---

artikel 125 i kodexen, anses vara hänvisningar till kodexen (och läsas i enlighet med jämförelsetabellen bilaga XIII). Eftersom definitionen av en elektronisk kommunikationstjänst ändras i kodexen på så sätt att även NI-ICS omfattas ska således dessa tjänster även omfattas av e-dataskyddsdirektivet.

[5] Läs mer, bl.a. i ingresspunkt 15 och 95 i kodexen.

[6] Elektroniska kommunikationsnäts och kommunikationstjänsters förmåga att vid en viss tillförlitlighetsnivå motstå åtgärder som undergräver tillgängligheten, riktigheten, integriteten eller konfidentialiteten hos dessa nät och tjänster, hos lagrade eller överförda eller behandlade uppgifter eller hos de närliggande tjänster som erbjuds genom eller är tillgängliga via dessa elektroniska kommunikationsnät eller kommunikationstjänster.

[7] Se prop. 2021/22:136 *Genomförande av direktivet om inrättande av en europeisk kodex för elektronisk kommunikation*, s. 313-314.

[8] En händelse med en faktisk negativ inverkan på säkerheten i elektroniska kommunikationsnät eller kommunikationstjänster.

[9] Se prop. 2010/11:115 *Bättre regler för elektroniska kommunikationer*, s. 169.

tillhandahåller allmänna nät och tjänster utan onödigt dröjsmål till tillsynsmyndigheten rapportera störningar eller avbrott av betydande omfattning.

Den nya definitionen av säkerhet och säkerhetsincident i kodexen och nya LEK omfattar det vi i svensk rätt kallar ”driftsäkerhet” samt ”störningar och avbrott” men omfattar även ytterligare säkerhetsaspekter. Bestämmelserna i 5 kap. nuvarande LEK motsvarar således i och med den nya definitionen endast delvis artikel 40 i kodexen. Nya LEK genomför de ändringar som föranleds av kodexen.

Den ändrade definitionen i kodexen gör att regelverket numera omfattar områden som delvis även regleras i e-dataskyddsdirektivet. Bestämmelser om säkerhetsåtgärder och incidentrapportering finns idag både i ramdirektivet samt i e-dataskyddsdirektivet och i förordning 611/2013. Tillhandahållare måste, i förekommande fall, se till att vidtagna säkerhetsåtgärder och incidentrapporteringen uppfyller kraven som har sin grund i båda regelverken. Det är emellertid av vikt att uppmärksamma att regelverken skiljer sig något åt. Till exempel gäller e-dataskyddsdirektivet och bestämmelserna som genomför direktivet i svensk rätt all behandling av uppgifter som *har samband med tillhandahållandet* av en kommunikationstjänst, dvs. inte enbart konfidentialiteten i de uppgifter som överförs eller lagras genom dessa tjänster. Det är även av vikt att uppmärksamma huruvida en händelse utgör en säkerhetsincident eller en integritetsincident och att olika regler gäller vid rapportering av dessa incidenter.

Ny skyldighet om information till användare

I 8 kap. 4 § nya LEK införs en ny skyldighet som innebär att tillhandahållare, om det föreligger ett konkret och betydande hot om en säkerhetsincident, ska informera de användare som kan komma att påverkas av hotet om de eventuella skydds- eller motåtgärder användarna kan vidta och, om det är lämpligt, om själva hotet.

Skyldigheten gäller konkreta och betydande hot om säkerhetsincidenter som upptäcks. Att hotet ska vara konkret och betydande innebär att det ska finnas ett konkret hot som kan drabba användare på ett ingående sätt, t.ex. genom att användare kan drabbas av avbrott i tjänster eller att känsliga uppgifter om användare riskerar att spridas.

I sammanhanget kan nämnas att det inom integritetsområdet sedan tidigare finns en liknande reglering i 6 kap. 4 § nuvarande LEK som stadgar att om det vid tillhandahållande av en allmänt tillgänglig elektronisk kommunikationstjänst finns särskild risk för bristande skydd av behandlade uppgifter, ska den som tillhandahåller tjänsten informera abonnenten om risken. Om den som tillhandahåller tjänsten inte är skyldig att avhjälpa risken, ska abonnenten informeras om hur och till vilken ungefärlig kostnad risken kan avhjälpas.

1.2 Samhällets behov av säker elektronisk kommunikation

Teknisk utveckling och ökad användning

Sverige har historiskt sett varit ledande inom it- och telekomsektorn, och har även i modern tid legat i framkant vad gäller innovation och teknik. Utbyggnaden av den digitala infrastrukturen under 2000-talet antas vara en viktig bakomliggande orsak, och tillgången till snabba och robusta elektroniska kommunikationer har banat väg för nya innovationer på området.

Invånarna i Sverige har i stor utsträckning tillgång till fibernät och snabba bredbandsabonnemang. Under det senaste året har antalet snabba bredbandsabonnemang ökat i Sverige, vilket framförallt beror på fortsatt fiberutbyggnad. Utbyggnad av infrastruktur i form av optisk fiber anses vara framtidssäker på grund av den höga överföringskapacitet som möjliggörs. Enligt färsk statistik är 75 % av alla fasta bredbandsabonnemang i Sverige baserade på fiberteknik och 95 % av de svenska hushållen har eller finns i absolut närhet av en fiberanslutning.[10]

Vad gäller mobilt bredband har flera operatörer aviserat att en avveckling av 2G- och 3G-näten kommer att ske under de närmaste åren. I Sverige förväntas utbyggnaden av 5G ta fart efter att PTS genom ett auktionsförfarande tilldelat operatörerna frekvenser i 3,5 GHz-frekvensbandet under år 2021. Inledningsvis förväntas utbyggnaden av 5G i Sverige främst ske genom uppgradering och återanvändning av befintlig infrastruktur för mobilnät. På längre sikt, och beroende av marknads-utveckling, teknikutveckling och tillgång till nya frekvensband, kan det dock behöva etableras nya sändarplatser och nybyggnation för att förbättra nätens kapacitet.

Enligt PTS datainsamling[11] om operatörers marknadsutveckling under 2020 framgår att datatrafiken i mobilnäten ökat med 36 % jämfört med samma tidpunkt föregående år. Antalet trafikminuter i mobilnäten har ökat med 11 %. Fast telefoni har minskat, liksom antalet abonnemang för bredband via det traditionella kopparnätet. Däremot har antalet abonnemang för fast bredband via fiber ökat under året. Rapporter från föregående år visar på samma mönster med en ökning av mobildatatrafik och bredband via fiber, medan en minskning skett gällande fast telefoni över tid.

Statistiken visar således på en tydlig ökning av ringda samtalsminuter samt användning av data i mobilnäten under år 2020, efter att ökningen legat på en jämn nivå under tidigare år. Denna märkbara ökning antas vara en effekt av covid-19-pandemin som från vintern år 2020 påverkade världen under lång tid. Under

[10] https://statistik.pts.se/media/05glngak/nbs_presentation_2020.pdf
[11] Svensk Telekommarknad 2020 PTS-ER-2021:21.

pandemin märktes en ökad användning av elektroniska kommunikationstjänster, både inom arbets- och privatlivet, då alltfler uppgifter, möten och andra sysslor utförs digitalt och på distans, t.ex. läkarbesök, utbildningar, skoluppgifter och föreningsliv.

Sammanfattningsvis har således användandet av mobilnät och fast bredband via fiber ökat och utgör nu en viktig beståndsdel av den elektroniska kommunikationen både hos individer, företag och i samhället i stort. Myndigheters ökade användning av e-tjänster, medborgares förändrade mediekonsumtion samt det ökade användandet av s.k. molntjänster är exempel på områden där användandet av elektroniska kommunikationers funktioner fått en betydande roll.

Ökat beroende

Det ökande användandet av elektroniska kommunikationsnät- och tjänster som beskrivs ovan har även fått till följd att samhällets beroende av desamma har ökat, både i det vardagliga livet och vid extraordinära händelser i fredstid, som t.ex. en olyckshändelse, en storm eller en pandemi. I alla sektorer i samhället finns ett ökat beroende av säker och pålitlig elektronisk kommunikation, då allt fler tjänster och samhällsfunktioner förlitar sig på fungerande nät och tjänster för allt från sjukvård till försörjning av livsmedel och dricksvatten. Därtill kommer faktorer som det kontantlösa samhällets beroende av att elektroniska transaktioner fungerar. Användare förväntar sig och agerar utifrån att kunna vara uppkopplade större delen av tiden. Elektroniska kommunikationer är dessutom av stor vikt för totalförsvarsplaneringen.

Den kommande 5G-utbyggnaden förmodas också både bredda och utöka användningen och beroendet av tillgängliga och säkra elektroniska kommunikationer. Bland annat får sakernas internet (*Internet of things*) en viktigare roll i samhället och medföra att både fler maskiner och människor kommer att vara uppkopplade och kommunicera med varandra.

Ett delmål för den svenska digitaliseringspolitiken är att elektroniska kommunikationer ska vara effektiva, säkra och robusta. Hög säkerhet och integritet, samt tillit till teknik är viktiga frågor inom detta område.

Ökad risk för sårbarheter och förändrat säkerhetspolitiskt läge

Den ökade digitaliseringen i samhället medför många möjligheter och har stora fördelar, men skapar också utmaningar i form av nya risker, hot och sårbarheter, vissa av hittills okänd karaktär. Det ökade beroendet av elektroniska kommunikationer och digitaliseringen av samhälleliga funktioner gör att både individer och samhället i allt större utsträckning utsätts för risker för olika typer av incidenter som kan få stora konsekvenser. Det blir därför allt viktigare med säkra, tillförlitliga och robusta nät och tjänster. Tillhandahållare måste därför agera och

anpassa sitt säkerhetsarbete utifrån de nya utmaningarna med både befintliga samt hittills okända risker och hot.

PTS har i samband med ett regeringsuppdrag om hot och risker mot säkerheten i elektroniska kommunikationsnät[12] tillsammans med berörda samrådsmyndigheter identifierat ett antal riskområden. Dessa är bl.a. obehörig åtkomst till system, kvaliteten på utrustningen, leverantörsberoenden och problem med interoperabilitet och diversifiering.

Rapporten *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures CG Publication 01/2020* (EU:s verktygslåda för 5G-säkerhet) bygger på en gemensam riskanalys genomförd av medlemsstaterna och Europeiska kommissionen, och innehåller rekommendationer i form av tekniska, strategiska och stödjande åtgärder för att stärka säkerheten i 5G-näten. Även om dessa risker och åtgärder framförallt fokuserar på 5G-näten kommer införandet av 5G-nät att innebära att infrastruktur går in i varandra, då näten och tjänsterna kommer att bestå av teknisk utrustning, samarbeten och beroenden som hör ihop och interagerar. Den säkerhetsproblematik som redogjorts för ovan bör därmed gälla alla tillhandahållare av elektroniska kommunikationstjänster, oavsett generation av kommunikationsnät. En annan aspekt är att när fler enheter och system kopplas ihop i 5G-tekniken blir den information som delas mer exponerad, vilket också gör den mer sårbar för angrepp och påverkan. Med sakernas internet väntas denna utveckling accelerera.

Det rådande säkerhetspolitiska läget i Europa och i vårt närområde gör att riskerna för angrepp eller påverkan på system ökar. Säkerhetspolisen har i sin årsbok för år 2020[13] uppgett att teknikutvecklingen och den ökade digitaliseringen bidragit till att främmande makt har utvecklat sin förmåga till cyberspionage och att cyberangrepp mot olika mål i samhället pågår hela tiden. Enligt Säkerhetspolisens bedömning har främmande makt både förmåga och vilja att bedriva cyberrelaterade säkerhetshot, i form av angrepp såväl som genom inhämtande av information.

Inrapporterade incidenter till PTS

Den utvecklade tekniken, komplexiteten i nät och tjänster samt nya leverantörskedjor och samarbeten, även över nationsgränser, kan medföra en ökad risk för rena tekniska fel. Även risker i form av den mänskliga faktorn, väder och olyckor eller risker för angrepp kan orsaka incidenter som kan leda till säkerhetsincidenter.

Tillhandahållare av elektroniska kommunikationer är enligt gällande reglering[14] skyldiga att rapportera in driftsstörnings- och integritetsincidenter till PTS. Under 2021

[12] PTS dnr. 20-5216.
[13] Säkerhetspolisens årsbok 2020.
[14] 5 kap. 6 c § och i 6 kap. 4 a § nuvarande LEK, PTSFS 2012:2 och förordning 611/2013.

inkom 25 rapporter om rapporteringspliktiga driftsstörningar och avbrott i elektroniska kommunikationer, och 404 integritetsincidenter till PTS.

Antalet rapporterade incidenter om driftsstörningar och avbrott (25 stycken år 2021) är lägre än något år tidigare. Rapporteringsskyldigheten infördes 2012. Antalet brukar ligga mellan 30 och 50 inrapporterade incidenter per år. Antalet inrapporterade integritetsincidenter (404 stycken år 2021) har successivt ökat kraftigt de senaste åren. Mellan år 2018 och 2019 ökade antalet inrapporterade integritetsincidenter med drygt 100 %, mellan år 2019 och år 2020 med nästan 50 %, och mellan år 2020 och 2021 med 36 %. PTS bedömer dock att denna utveckling sannolikt inte beror på att det faktiskt sker fler integritetsincidenter, utan snarare att tillhandahållarnas kunskap och förmåga att upptäcka dylika incidenter ökat, liksom medvetenheten om rapporteringsplikten för dessa.

Grundorsakerna till störningar och avbrott enligt inrapporterade incidenter år 2021 är: systemfel (15 stycken), mänsklig felbedömning eller misstag (7 stycken), fel hos tredje part (partner/underleverantör) (1 styck) och naturens kraft (1 styck).

Tidigare år har driftsstörningar och avbrott orsakade av hårt väder rapporterats, dock inte under år 2020 och 2021. Sett över en längre tidsperiod är konfigurationsfel och andra handhavandefel relaterat till den mänskliga faktorn den vanligaste orsaken till störningar och avbrott. Därefter följer fel i hård- och mjukvara följt av avbrott och störningar orsakade av överbelastningsattacker eller bristande kapacitet i nätutbyggnaden. Vanligtvis får driftsstörningar och avbrott endast regional eller lokal påverkan och endast en liten andel medför nationell påverkan.

De vanligaste bakomliggande orsakerna bakom de inrapporterade integritetsincidenterna är felregistrering eller förväxling av kunduppgifter, t.ex. genom felregistrerade e-postadresser. Den näst vanligaste bakomliggande orsaken är att obehöriga personer fått ut information eller kunnat ändra i kunders abonnemang, samt bedrägeri eller försök till bedrägeri.

Allvarliga konsekvenser

Det ökade beroendet av elektroniska kommunikationer medför att säkra nät och tjänster är en förutsättning för att vårt digitaliserade samhälle ska fungera. De nät och tjänster som tillhandahålls måste således hålla en hög nivå avseende tillgänglighet, autenticitet, riktighet och konfidentialitet. Det innefattar skydd av behandlade uppgifter. Säkerhetsbrister riskerar att leda till att samhällets behov av elektroniska kommunikationer inte tillgodoses och att tilliten till elektroniska kommunikationstjänster skadas, vilket skulle kunna få stora negativa samhällsekonomiska konsekvenser som följd.

2. Beskrivning av problemet, vad PTS vill uppnå och alternativa lösningar

I avsnitt 1 beskrivs de två stora förändringarna som har inträffat, dvs. införandet av ändringar i den överordnade regleringen och samhällsutvecklingen som skett under de senaste åren. Dessa två förändringar utgör de bakomliggande drivkrafterna som föranleder PTS förslag till nya föreskrifter. De nya föreslagna föreskrifterna syftar således till att säkerställa att bestämmelserna står i överensstämmelse med den överordnade regleringen samt att de motsvarar en säkerhetsnivå som är lämplig i förhållande till riskerna för incidenter och samhällets behov av säker elektronisk kommunikation.

I avsnitt 2.1–2.4 beskriver PTS, med utgångspunkt i de två bakomliggande drivkrafterna, de olika problem som motiverar att de föreslagna föreskrifterna införs. I samband med beskrivningen av de olika problemen beskriver PTS även vad myndigheten vill uppnå samt vilka alternativa lösningar som övervägts, vilket inkluderar vad effekterna blir om någon reglering inte kommer till stånd (det s.k. nollalternativet).

2.1 Anpassning till överordnad reglering och samhällets behov av säker elektronisk kommunikation

Tillhandahållare är enligt bestämmelser i 5 och 6 kap. nuvarande LEK skyldiga att vidta säkerhetsåtgärder och rapportera incidenter. PTSFS 2012:2, PTSFS 2014:1 och PTSFS 2015:2 innehåller bestämmelser om dessa skyldigheter.[15]

I sak motsvarar nya LEK i stora delar nuvarande LEK, dock med de ändringar och tillägg som föranleds av kodexen, se vidare avsnitt 1.1.3.

Ändringarna i nya LEK påverkar bestämmelserna i PTSFS 2012:2, PTSFS 2014:1 och PTSFS 2015:2. Dessutom påverkas bestämmelserna i PTSFS 1995:1 indirekt av ändringarna i nya LEK.

Bestämmelserna behöver därför anpassas för att säkerställa att de står i överens-stämmelse med den överordnade regleringen. Det är av vikt att bestämmelserna reglerar alla aspekter av säkerhet och skydd som varit lagstiftarens avsikt samt att de

[15] Med undantag för integritetsincidenter vilket regleras i förordning 611/2013.

säkerställer en säkerhets- och skyddsnivå som motsvarar samhällets behov av säker elektronisk kommunikation, se vidare avsnitt 1.

PTS har därför utrett hur PTSFS 1995:1, PTSFS 2012:2, PTSFS 2014:1 och PTSFS 2015:2 påverkas av nya LEK. Myndigheten har analyserat föreskrifterna i ljuset av de ändringar som införs genom kodexen och nya LEK samt i ljuset av de samhällsförändringar som har skett sedan nuvarande föreskrifter trädde i kraft. Syftet med utredningen och analysen har varit att identifiera vilka anpassningar som behöver göras och om det finns luckor eller brister i bestämmelserna, till följd av den nya överordnade regleringen eller samhällets behov av säker elektronisk kommunikation.

I utrednings- och analysarbetet har PTS beaktat myndighetens egna erfarenheter och iakttagelser från bland annat tillsyn.

PTS har även beaktat EU:s verktygslåda för 5G-säkerhet. EU:s verktygslåda för 5G-säkerhet innehåller ett antal rekommenderade åtgärder för att hantera risker som hotar säkerheten i 5G, vid utbyggnad och distribution av sådana mobilnät. Åtgärderna baseras på en riskanalys som Europeiska kommissionen och EU:s medlemsstater gemensamt har genomfört. Sverige har, genom PTS, MSB och andra myndigheter, deltagit i arbetet med riskanalysen och framtagandet av verktygslådan.

PTS har dessutom beaktat riktlinjer från EU:s cybersäkerhetsbyrå (ENISA) som är publicerade i rapporten *Guideline on Security Measures under the EECC.* Syftet med riktlinjerna är att säkerställa ett harmoniserat genomförande av artiklarna 40 och 41 i kodexen bland EU:s medlemsstater. Riktlinjerna, som är teknikneutrala, åtföljs av ett tillägg om 5G, *5G Supplement - to the Guideline on Security Measures under the EECC,* som syftar till att ge ledning kring hur risker som är specifikt kopplade till 5G ska hanteras. PTS har även beaktat föregångaren till ENISA:s riktlinjer, *Technical Guideline on Security measures for Article 4 and Article 13a*. Samtliga riktlinjer har tagits fram med hjälp av ENISA:s expertgrupp för säkerhet, *European Competent Authorities for Secure Electronic Communications* (ECASEC). PTS deltar regelbundet i ECASEC:s arbete.

Vidare har PTS under arbetets gång genomfört samråd med berörda aktörer, både tillhandahållare och myndigheter, och beaktat de synpunkter som framförts i dessa sammanhang, se vidare avsnitt 5.

2.1.1 Säkerhetsåtgärder

Problembeskrivning

PTSFS 2014:1 och PTSFS 2015:2 innehåller bestämmelser om säkerhetsåtgärder. Föreskrifterna tydliggör vilka säkerhetsåtgärder tillhandahållare ska vidta för att hantera riskerna för integritetsincidenter respektive för störningar och avbrott.

Bestämmelserna är generellt sett utformade som funktionskrav eller så kallade ”vad”-krav. Det innebär att bestämmelserna fastställer *vad* tillhandahållare ska uppnå vid vidtagande av olika säkerhetsåtgärder utan att ställa tekniskt detaljerade krav på *hur* detta ska uppnås. Tillhandahållare har således ett stort utrymme att göra egna bedömningar av hur bestämmelserna ska efterlevas och vilka exakta åtgärder som behöver vidtas utifrån hur deras verksamhet ser ut och de risker som de behöver hantera.

Som angetts ovan har PTS utrett och analyserat PTSFS 2014:1 och PTSFS 2015:2 i ljuset av de ändringar som införs genom den överordnade regleringen och samhällets behov av säker elektronisk kommunikation. I detta arbete har PTS bland annat beaktat myndighetens egna erfarenheter, framförda synpunkter från berörda aktörer och diverse internationella riktlinjer.

PTS konstaterar efter denna utredning och analys att nuvarande bestämmelser i PTSFS 2014:1 och PTSFS 2015:2 till övervägande del bör behållas oförändrade. Myndigheten har dock identifierat vissa luckor och brister i bestämmelserna som behöver åtgärdas för att säkerställa att en lämplig säkerhetsnivå uppnås.

Vad PTS vill uppnå

Syftet med PTSFS 2014:1 och PTSFS 2015:2 är att säkerställa en lämplig säkerhetsnivå i nät och tjänster genom att tydliggöra vilka säkerhetsåtgärder tillhandahållare ska vidta i sin verksamhet för att hantera risker för incidenter. Genom föreskrifterna blir det även tydligt för slutanvändare vilken säkerhet och vilket skydd de kan förvänta sig från sina tillhandahållare.

PTSFS 2014:1 och PTSFS 2015:2 bedöms till övervägande del fortsatt innehålla relevanta bestämmelser och dessa föreslås således till stora delar behållas. Mot bakgrund av ovanstående problembeskrivning anser dock PTS att det finns ett behov av att införa nedanstående ändringar av och tillägg till de nuvarande bestämmelserna, av de anledningar som anges i varje punkt nedan. Ändringarna och tilläggen föreslås, precis som nuvarande föreskrifter, generellt sett utformas som vad-krav, istället för hur-krav för att säkerställa flexibilitet.

- I syfte att säkerställa att nät och tjänster är säkra över tid anser PTS att det finns ett behov av att tydliggöra vad som bör beaktas i samband med uppföljning och utvärdering av vidtagna säkerhetsåtgärder. PTS föreslår att bestämmelser om övergripande säkerhetsarbete kompletteras med allmänna råd om detta, se vidare avsnitt 6.5.
- I syfte att säkerställa att bestämmelserna omfattar samtliga säkerhetsaspekter och att öka förutsättningarna för att potentiella risker identifieras anser PTS att det finns ett behov av att tillhandahållare genomför

riskanalyser. Dessa riskanalyser bör utökas och omfatta samtliga säkerhetsaspekter och i detta arbete bör tillhandahållarna även genomföra omvärldsbevakning, se vidare avsnitt 6.7.

- I syfte att säkerställa att planerade förändringar inte orsakar säkerhetsincidenter utifrån någon av säkerhetsaspekterna anser PTS att det finns ett behov av att säkerställa att tillhandahållare vidtar ytterligare åtgärder i samband med planerade förändringar, se vidare avsnitt 6.8.
- I syfte att säkerställa att föreskrifterna omfattar samtliga säkerhetsaspekter anser PTS att det finns ett behov av att införa bestämmelser om loggning av systemhändelser som ett komplement till nuvarande bestämmelser om övervakning och beredskap, se vidare avsnitt 6.11.
- I syfte att säkerställa att integritets- och säkerhetsincidenter upptäcks och hanteras snabbare anser PTS att det finns ett behov av att komplettera bestämmelserna om loggning med allmänna råd om automatisk övervakning av loggar, se vidare avsnitt 6.11.
- I syfte att säkerställa att bestämmelserna omfattar samtliga säkerhetshetsaspekter anser PTS att det finns ett behov av att införa bestämmelser om kryptering av vissa anslutningar för konfigurering och styrning av tillgångar, se vidare avsnitt 6.12.
- I syfte att säkerställa en lämplig nivå på skyddet av uppgifter om slutanvändare anser PTS att det finns ett behov av att ta bort den nuvarande möjligheten för den som berörs att medge att enstaka överföringar av behandlade uppgifter sker utan kryptering, se vidare avsnitt 6.12.
- I syfte att säkerställa att mobila nät och tjänster fungerar vid strömavbrott anser PTS att det finns ett behov av att ta bort den nuvarande möjligheten att prioritera vissa tjänster framför andra, se vidare avsnitt 6.13.
- I syfte att säkerställa att föreskrifterna omfattar samtliga säkerhetsaspekter anser PTS att det finns ett behov av att säkerställa att tillhandahållares övervakning och beredskap inte begränsas till driftstörning och avbrott utan även omfattar övriga säkerhetsincidenter, se vidare avsnitt 6.15.
- I syfte att tydliggöra vad den nya skyldigheten i nya LEK, om information till användare om konkreta och betydande hot om en incident, innebär anser PTS att det finns ett behov av att ta fram kompletterande bestämmelser kring detta, se vidare avsnitt 6.19.

Alternativa lösningar

PTS anser som tidigare angetts att nuvarande bestämmelser i PTSFS 2014:1 och PTSFS 2015:2 i huvudsak fortsatt är relevanta och myndigheten har redan vid framtagande av nu gällande föreskrifter bedömt att det är nödvändigt med en tvingande reglering i föreskriftsform. Denna bedömning kvarstår.

PTS har som alternativ lösning övervägt att behålla bestämmelserna i PTSFS 2014:1 och PTSFS 2015:2 oförändrade.

Om PTSFS 2014:1 och PTSFS 2015:2 skulle behållas oförändrade skulle bestämmelserna enligt PTS inte vara anpassade efter den överordnade regleringen. Det skulle finnas vissa luckor och brister i regleringen som skulle utgöra ett hot mot säkerheten vilket, i värsta fall, kan få stora samhälleliga konsekvenser. Det skulle vidare finnas en risk att tillhandahållare tolkar skyldigheterna att vidta säkerhetsåtgärder på olika sätt vilket kan leda till att otillräckliga åtgärder vidtas, vilket skulle få en negativ påverkan på säkerheten.

PTS kan visserligen i efterhand genom tillsyn och beslut i enskilda ärenden i viss mån försöka uppnå en enhetlig tillämpning över tid, men det finns då en betydande risk för rättsosäkerhet och att tillhandahållare långt senare behöver anpassa sina säkerhetsåtgärder efter PTS beslut till en högre kostnad, jämfört med om tydliga bestämmelser finns från början.

Integritets- och säkerhetsincidenter kan få stora negativa samhällsekonomiska konsekvenser. När elektroniska kommunikationstjänster drabbas av t.ex. ett avbrott innebär det att kostnader för både konsumenter och producenter, t.ex. företag som är beroende av elektronisk kommunikation för att producera sina varor och tjänster, ökar. I konsumentledet handlar det om privatekonomiska kostnader, som t.ex. kostnader som uppstår i och med att man inte kan läsa epost, att man inte kan komma åt sina molntjänster eller att man inte kan söka information. Avbrott i elektroniska kommunikationstjänster gör det svårt att kommunicera och informera t.ex. anhöriga vid olyckor, vilket också kan leda till oro och osäkerhet. Om avbrotten drabbar larmtjänster, som 112, finns även risk för liv och hälsa.

Det är vanskligt att beräkna den exakta kostnaden för t.ex. ett avbrott men en indikativ uppskattning kan göras. En studie skattade det dagliga ekonomiska värdet (kostnaden) om näten i Irland skulle gå ner till 70 miljoner euro per dag.[16] Om den svenska siffran skulle antas vara det dubbla (befolkningen är dubbelt så stor) och att näten har 14 ungefär lika aktiva timmar per dag, skulle värdet av en timmes avbrott i Sverige skattas till 10 miljoner Euro. Om detta händer med en sannolikhet om 20 % över ett års tid[17] (vilket något inkorrekt kan uttryckas som att ”det händer en gång vart femte år”) blir den förväntade årliga kostnaden 2 miljoner Euro.

[16] Lyons, S., Morgenroth, E., Tol, R. (2013). Estimating the value of lost telecoms connectivity. Electronic Commerce Research and Applications 12: 40–51.

[17] Dvs att det är en sannolikhet på 20%, under ett visst år, att under en (1) av årets 5110 för trafiken relevanta timmar (365×14) är nätet nere.

Sammantagen bedömning

PTS gör bedömningen att det är av vikt att bestämmelserna i föreskrifterna behålls med de ändringar och tillägg som beskrivs ovan i syfte att säkerställa en lämplig säkerhetsnivå i nät och tjänster som är anpassad efter den överordnade regleringen och samhällets behov av säker elektronisk kommunikation.

2.1.2 NI-ICS

Problembeskrivning

Bestämmelserna om säkerhetsåtgärder och rapportering av incidenter utökas i nya LEK till att även omfatta NI-ICS.

PTSFS 2012:2, PTSFS 2014:1 och PTSFS 2015:2 innehåller kompletterande bestämmelser till skyldigheterna att vidta säkerhetsåtgärder och rapportera incidenter. Föreskrifterna gäller med samma tillämpningsområde och bygger på samma definitioner som den överordnade regleringen, dvs. framöver även NI-ICS.[18] Även PTSFS 1995:1 bygger på samma definitioner som den överordnade regleringen och gäller – precis som de övriga föreskrifterna – samtliga tillhandahållare av allmänna nät och tjänster.

Ändringen i nya LEK får således till följd att PTSFS 1995:1, PTSFS 2012:2, PTSFS 2014:1 och PTSFS 2015:2 per automatik även kommer att gälla NI-ICS från och med att lagen träder i kraft. För att säkerställa att PTS föreskrifter fortsatt utgör ändamålsenliga regleringar har myndigheten genomfört en utredning för att ta reda på vad det ändrade tillämpningsområdet i nya LEK får för konsekvenser och om några justeringar behöver göras för det fall ändringen får oönskade effekter.

PTS anser att det är viktigt att säkerställa att samtliga nät och tjänster, däribland NI-ICS, är säkra och att de som utgångspunkt ska omfattas av de föreskrifter som PTS har meddelat i anslutning till skyldigheterna i nya LEK inom säkerhetsområdet. Myndigheten bedömer dock utifrån den utredning som genomförts att det finns ett antal bestämmelser i de nu gällande föreskrifterna som inte är motiverade att ställa på NI-ICS och ett antal som – på sätt som de nu är utformade – inte är anpassade efter dessa tjänsters särskilda egenskaper och betydelse vilket utgör ett problem.

[18] Förutom PTSFS 2014:1 som inte omfattar nättillhandahållare, det är dock inte relevant i detta sammanhang då frågan här handlar om regleringen av tjänstetillhandahållare.

Vad PTS vill uppnå

Mot bakgrund av ovanstående problembeskrivning konstaterar PTS att det finns ett behov av att ändra vissa bestämmelser i PTSFS 1995:1, PTSFS 2012:2, PTSFS 2014:1 och PTSFS 2015:2 så att reglerna blir ändamålsenliga och fungerar även för NI-ICS.

PTS anser att det saknas behov av att NI-ICS omfattas av bestämmelserna i PTSFS 1995:1 men att dessa tjänster ska omfattas av bestämmelserna i PTSFS 2012:2, PTSFS 2014:1 och PTSFS 2015:2, dock med vissa anpassningar.

Bestämmelserna i PTSFS 2012:2 förtydligar när och hur rapportering av säkerhetsincidenter ska ske vilket ger en tydlighet kring rättsläget. NI-ICS bör således omfattas av bestämmelserna i den föreskriften.

PTSFS 2014:1 och PTSFS 2015:2 innehåller bestämmelser om säkerhetsåtgärder. Bestämmelserna i dessa föreskrifter är, som tidigare angetts, generellt sett utformade som funktionskrav eller så kallade ”vad”-krav. Tillhandahållare har således ett stort utrymme att göra egna bedömningar av hur bestämmelserna ska efterlevas och vilka åtgärder som behöver vidtas utifrån hur deras verksamhet ser ut och de risker som de behöver hantera. I syfte att säkerställa en lämplig säkerhetsnivå är det motiverat att bestämmelserna i föreskrifterna omfattar även NI-ICS. Till övervägande del bedömer PTS att bestämmelserna är möjliga att tillämpa på dessa tjänster. Det finns dock några undantag där PTS konstaterar att det finns ett behov av att införa ändringar jämfört med nu gällande föreskrifter.

- När det gäller bestämmelser om redundans och reservkraftssystem anser PTS att det bör införas en särskild reglering för NI-ICS gällande hur tillgångar klassificeras. PTS bedömer vidare att det endast är motiverat att de NI-ICS som har 30 000 eller fler uppskattat antal användare i Sverige som kan drabbas av en säkerhetsincident som innebär störning eller avbrott till följd av att en tillgång upphört att fungera normalt, träffas av reglerna om redundans och reservkraftssystem. Se vidare avsnitt 6.13.
- När det gäller bestämmelser om rapportering av säkerhetsincidenter till PTS anser myndigheten att det finns ett behov av att införa vissa anpassningar gällande tröskelvärdena så att de kan tillämpas av NI-ICS (genom att incidentens omfattning bland annat kan beräknas som andelen berörda användare, inte bara antalet aktiva anslutningar), se vidare avsnitt 6.20.

För att NI-ICS ska omfattas av de föreslagna föreskrifterna krävs det att de omfattas av svensk jurisdiktion.

I kodexen finns ingen vägledning om när en tjänst ska anses tillhandahållas i ett visst land. Det finns inte heller några särskilda regler om hur tillsyn av dessa tjänster bör samordnas om de tillhandahålls i mer än en medlemsstat.

För att avgöra om en tjänst omfattas av svensk jurisdiktion är det avgörande om tjänsten tillhandahålls i Sverige. Enligt PTS får en tjänst anses tillhandahållas i Sverige om den endera har svenska slutkunder eller riktar sig till svenska slutkunder.

Alternativa lösningar

PTS har som alternativ lösning övervägt om NI-ICS, utöver bestämmelserna i PTSFS 2012:2, PTSFS 2014:1 och PTSFS 2015:2, även ska omfattas av bestämmelserna i PTSFS 1995:1. Myndigheten har dock inte identifierat något sådant behov. Det saknas i dagsläget totalförsvarsskäl att tjänsterna omfattas av bestämmelserna i PTSFS 1995:1 och det nuvarande tillämpningsområdet för bestämmelserna i PTSFS 1995:1 bör således behållas.

PTS har som alternativ lösning även övervägt att undanta NI-ICS helt från bestämmelserna i PTSFS 2012:2, PTSFS 2014:1 och PTSFS 2015:2 i syfte att minska den administrativa bördan för tillhandahållare av sådana tjänster. I en sådan situation skulle alltså skyldigheterna enligt nya LEK gälla dessa tillhandahållare men inte de mer detaljerade och kompletterande bestämmelserna i föreskrifterna. Enligt PTS bedömning är detta emellertid inte lämpligt ur rättssäkerhets- och säkerhets-synpunkt. PTS föreskrifter syftar till att säkerställa en lämplig säkerhetsnivå genom att tydliggöra vilka säkerhetsåtgärder tillhandahållare ska vidta i sin verksamhet för att hantera risker för integritets- och säkerhetsincidenter. Genom föreskrifterna blir det tydligt för tillhandahållare vad som gäller samt vad slutanvändare kan förvänta sig för skydd från sina tillhandahållare. Dessutom torde konsekvenserna till följd av föreskrifterna vara begränsade. Tillhandahållare av NI-ICS bedriver uppskattningsvis generellt ett fungerande säkerhetsarbete idag och omfattas även av annan reglering inom säkerhetsområdet, till exempel EU:s dataskyddsförordning.

Sammantagen bedömning

PTS gör bedömningen att NI-ICS ska undantas från bestämmelserna i PTSFS 1995:1 men att det är av vikt att tjänsterna omfattas av bestämmelserna i PTSFS 2012:2, PTSFS 2014:1 och PTSFS 2015:2 med de anpassningar som beskrivs ovan.

2.1.3 Nättillhandahållare som behandlar uppgifter

Problembeskrivning

5 kap. 6 b § nuvarande LEK stadgar att tillhandahållare av nät och tjänster ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att verksamheten

uppfyller rimliga krav på driftsäkerhet. Skyldigheten att vidta åtgärder faller således både på nät- och tjänstetillhandahållare. Vidare omfattas både nät- och tjänstetillhandahållare av skyldigheten i 6 kap. 3 § nuvarande LEK som stadgar att tjänstetillhandahållare ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att uppgifter som behandlas i samband med tillhandahållandet av tjänsten skyddas samt att nättillhandahållare ska vidta de åtgärder som är nödvändiga för att upprätthålla detta skydd i nätet. PTSFS 2015:2, som har meddelats i anslutning till 5 kap. 6 b § nuvarande LEK, omfattar både nät- och tjänstetillhandahållare. PTSFS 2014:1, som har meddelats i anslutning till 6 kap. 3 § nuvarande LEK, gäller emellertid endast tjänstetillhandahållare.

Genom kodexen tydliggörs att både nät- och tjänstetillhandahållare är skyldiga att vidta åtgärder för att på ett lämpligt sätt hantera risker som hotar näts och tjänsters säkerhet. Med näts och tjänsters säkerhet avses deras förmåga att vid en viss tillförlitlighetsnivå motstå åtgärder som undergräver tillgängligheten, riktigheten, autenticiteten eller konfidentialiteten hos dessa nät och tjänster samt hos lagrade eller överförda eller behandlade uppgifter.

PTS nuvarande reglering uppnår emellertid inte detta till fullo då nättillhandahållare inte omfattas av PTSFS 2014:1. Nättillhandahållare omfattas visserligen av skyldigheten i 6 kap. 3 § nuvarande LEK men inte av PTS föreskrifter på området, vilket kan ha en negativ påverkan på säkerheten.

Vad PTS vill uppnå

Mot bakgrund av ovanstående problembeskrivning konstaterar PTS att det finns ett behov av att säkerställa att bestämmelser i myndighetens föreskrifter i samtliga delar omfattar nättillhandahållare, dvs. även när det gäller skydd av behandlade uppgifter.

För att säkerställa att även nättillhandahållare upprätthåller säkerheten är det av vikt att de omfattas av de bestämmelser om säkerhetsåtgärder i de aktuella föreskrifterna som syftar till att skydda behandlade uppgifter.

Alternativa lösningar

PTS har som alternativ lösning övervägt att behålla nuvarande reglering, dvs att nättillhandahållare fortsatt undantas från bestämmelserna i PTSFS 2014:1. Ur rättssäkerhets- och säkerhetssynpunkt är det emellertid enligt PTS inte lämpligt. Bestämmelserna i PTS föreskrifter syftar till att säkerställa en lämplig säkerhetsnivå genom att tydliggöra vilka säkerhetsåtgärder tillhandahållare ska vidta i sin verksamhet för att hantera risker för integritets- och säkerhetsincidenter. Genom bestämmelserna blir det tydligt för tillhandahållare vad som gäller samt vad slutanvändare kan förvänta sig för skydd från sina tillhandahållare.

Sammantagen bedömning

PTS gör bedömningen att det är av vikt att regleringen utökas till att även innehålla skyldigheter för nättillhandahållare att skydda uppgifter. PTS gör därför bedömningen att det finns ett behov av att genomgående säkerställa att nättillhandahållare omfattas av de bestämmelser som ställer krav på att uppgifter ska skyddas.

2.2 Regelstruktur

Problembeskrivning

I enlighet med vad som angetts i avsnitt 2.1 finns det behov av att ändra vissa bestämmelser i PTSFS 1995:1, PTSFS 2012:2, PTSFS 2014:1 och PTSFS 2015:2.

Det rör sig alltså om behov av ändringar i bestämmelser som finns i fyra olika föreskrifter. Föreskrifterna har flera gemensamma nämnare. Samtliga har meddelats i anslutning till nuvarande LEK, riktar sig till nät- och tjänstetillhandahållare samt syftar till att nät och tjänster ska fungera och vara säkra, vare sig det rör sig om fred, extraordinära händelser eller höjd beredskap och krig. I och med de ändringar som införs genom nya LEK knyts dessutom regleringen om skyddsåtgärder för behandlade uppgifter och krav på driftssäkerhet i PTSFS 2014:1 och PTSFS 2015:2 närmare varandra. Det påverkar även indirekt PTSFS 2012:4, som i likhet med PTSFS 2014:1 och PTSFS 2015:2, innehåller bestämmelser om säkerhetsåtgärder (specifikt rörande uppgifter som lagras för brottsbekämpande ändamål).

Att nuvarande reglering är utspridd på flera föreskrifter trots de gemensamma nämnarna riskerar att göra regleringen svåröverskådlig och det finns en risk för bristande efterlevnad.

Vad PTS vill uppnå

I syfte att skapa ett tydligare, effektivare och mer lättillgängligt regelverk för tillämparna anser PTS att bestämmelser om säkerhetsåtgärder, incidentrapportering samt den fredstida planeringen för totalförsvarets behov av elektronisk kommunikation bör samlas i en gemensam författning.

Författningen bör upphäva och ersätta PTSFS 1995:1, PTSFS 2012:2, PTSFS 2012:4, PTSFS 2014:1 och PTSFS 2015:2.

Nuvarande bestämmelser ska behållas i föreskriftsform men inte i nuvarande struktur.

Alternativa lösningar

PTS har som alternativ lösning övervägt att behålla föreskrifterna och istället införa ändringarna, som redovisas i avsnitt 2.1, genom ändringsföreskrifter till de aktuella föreskrifterna.

PTS bedömer emellertid att en sådan utspridd reglering – särskilt mot bakgrund av de tillkommande ändringsföreskrifterna – riskerar att göra regleringen svåröverskådlig och att det därmed finns en risk för bristande efterlevnad.

Sammantagen bedömning

I syfte att få ett tydligare, effektivare och mer lättillgängligt regelverk anser PTS att nya föreskrifter ska antas som upphäver och ersätter PTSFS 1995:1, PTSFS 2012:2, PTSFS 2012:4, PTSFS 2014:1 och PTSFS 2015:2.

2.3 Förtydliganden och ensade krav

Problembeskrivning

Som redovisats i avsnitt 2.2 anser PTS att PTSFS 1995:1, PTSFS 2012:2, PTSFS 2012:4, PTSFS 2014:1 och PTSFS 2015:2 ska upphävas och ersättas av en ny författning.

De nuvarande föreskrifterna innehåller bestämmelser som i många delar reglerar samma eller liknande frågor. Emellertid har föreskrifterna tagits fram fristående från varandra och vid olika tidpunkter. Det har gjort att deras utförande och formuleringar många gånger skiljer sig åt, även om avsikten med regleringarna är samma eller åtminstone snarlik. Detta har blivit särskilt tydligt i arbetet med att ta fram de nya föreskrifterna.

PTS har därför genomfört en jämförelse av föreskrifterna för att identifiera vilka delar som kan slås samman och vilka delar som av olika anledningar behöver hållas åtskilda. I detta arbete har PTS konstaterat att i syfte att överhuvudtaget kunna ta fram nya förenklade sammanslagna föreskrifter och uppnå en enhetlig reglering föreligger det ett behov av att arbeta ihop och ibland ändra bestämmelserna som härrör från de olika föreskrifterna. Det finns annars en risk för bristande regelefterlevnad samt tolkningsproblem för både PTS och tillhandahållare.

Vad PTS vill uppnå

Målsättningen i samband med sammanslagningen av föreskrifterna är att inte sänka de säkerhets- och skyddsnivåer som finns i nuvarande föreskrifter. Bestämmelserna bör framför allt bearbetas språkligt i syfte att uppnå en enhetlig reglering. Ett fåtal ändringar bör emellertid göras i syfte att förtydliga och ensa de nuvarande bestämmelserna, vilket är något som kan innebära konsekvenser.

Samtliga ändringar redovisas i denna konsekvensutredning, se vidare avsnitt 6. I redovisningarna anges om det rör sig om materiella eller språkliga och redaktionella ändringar. Av de förtydliganden och ensade formuleringar som görs kan dock särskilt följande nämnas redan här.

- Nuvarande bestämmelser om riskanalys och åtgärder efter riskbedömning i PTSFS 2015:2 upplevs som komplicerade och delvis överlappande. Här föreslås en ny utformning av bestämmelserna som syftar till att förenkla och förtydliga förståelsen för hur riskanalyser ska göras och åtgärder vidtas.
- När det gäller bestämmelserna i PTSFS 2012:4 har sammanslagningen av regelverken gjort att det har identifierats behov av att säkerhetsarbetet kopplat till skyddet av uppgifter som lagras för brottsbekämpande ändamål bör omfattas av bestämmelser om kryptering och intern incidenthantering.

Alternativa lösningar

PTS har som alternativ lösning övervägt att inte arbeta ihop de olika föreskrifterna i den gemensamma författningen utan istället låta författningen bestå av olika kapitel som vart och en motsvarar de nuvarande föreskrifterna. PTS bedömer emellertid att det skulle göra regleringen otydlig och svåröverskådlig vilket utgör en risk för bristande efterlevnad och tolkningsproblem både för myndigheten och tillhandahållare.

Sammantagen bedömning

I syfte att ta fram tydliga och ändamålsenliga nya föreskrifter gör PTS bedömningen att det är av vikt att myndigheten slår samman nuvarande bestämmelser av samma slag och tar fram ensade formuleringar för dessa, även om det i sig kan leda till att vissa konsekvenser uppstår för tillhandahållare.

2.4 Den fredstida planeringen för totalförsvarets behov av elektronisk kommunikation

Problembeskrivning

PTSFS 1995:1 innehåller bestämmelser om den planering som tillhandahållare är skyldiga att genomföra i fredstid för de behov av elektronisk kommunikation som totalförsvaret kan ha i höjd beredskap och krig. PTS anser att föreskrifterna är relevanta men otydliga.

Elektroniska kommunikationer är grundläggande funktioner som är nödvändiga för att dagens samhälle ska fungera, såväl i normalläge och kris som i höjd beredskap och ytterst krig. Att elektroniska kommunikationer ska vara driftsäkra, dvs. att risken för störningar och avbrott hanteras, regleras idag i 5 kap. 6 b § nuvarande LEK och i

PTSFS 2015:2. Dessa bestämmelser omfattar såväl normala driftsförhållanden som extraordinära händelser. PTSFS 1995:1 kompletterar de grundläggande driftsäkerhetsbestämmelserna, som alltså gäller i normalläge och kris, genom att det dessutom ställs krav på att tillhandahållarna ska ha beredskap inför höjd beredskap och krig. Denna förberedelse är en förutsättning för att de elektroniska kommunikationerna ska kunna tillhandahållas även i höjd beredskap och i krig.

PTS har genomfört en uppföljning och utvärdering av PTSFS 1995:1.

PTS bedömer att bestämmelserna fortsatt är relevanta, inte minst mot bakgrund av att totalförsvarsplaneringen har återupptagits i Sverige till följd av det säkerhetspolitiska läget i vårt närområde. Som en följd är det av fortsatt stor betydelse att den administrativa beredskapen är så god som möjligt på området. Den aktuella regleringen syftar till att tillhandahållarna ska vara förberedda i ett läge av höjd beredskap eller krig. Bestämmelserna är emellertid otydliga och det finns risk att de kan tolkas på sätt som inte är avsedda. Regleringen är därför inte effektiv. Vidare bör den nära relationen tydliggöras avseende det vanliga driftsäkerhetsarbetet och förberedelserna inför höjd beredskap.

Vad PTS vill uppnå

Mot bakgrund av ovanstående problembeskrivning konstaterar PTS att det finns ett behov av att ta fram bestämmelser som är ändamålsenliga och lätta att förstå.

Avsikten är att bestämmelserna ska motsvara vad som redan gäller enligt nuvarande föreskrifter. Bestämmelserna behöver dock utformas på ett mer ändamålsenligt sätt. Förändringarna förväntas medföra en ökad tydlighet i regelverket.

Alternativa lösningar

PTS har som alternativa lösningar övervägt att föra över bestämmelserna i PTSFS 1995:1 i oförändrat skick eller att upphäva PTSFS 1995:1.

Om bestämmelserna i PTSFS 1995:1 skulle överföras oförändrade till de nya föreskrifterna skulle bestämmelserna fortsatt vara otydliga. Det finns en risk att tillhandahållare tolkar bestämmelserna på olika sätt vilket kan leda till att tillhandahållare vidtar planeringsåtgärder i alltför liten utsträckning vilket kan påverka tillhandahållandet av, och därmed totalförsvarets tillgång till, elektroniska kommunikationer i höjd beredskap och krig. Regleringen skulle därmed inte vara ändamålsenlig. De samhällsekonomiska kostnaderna, i ett krisläge, där sektorn elektronisk kommunikation är illa förberedd och där totalförsvaret inte skulle ha adekvat tillgång till kommunikation, kan bli mycket stora.

Om bestämmelserna i PTSFS 1995:1 skulle upphävas skulle regler helt saknas. Om regler saknas bedömer PTS det som sannolikt att tillhandahållarna i varierande utsträckning skulle förbereda sig för verksamhet under höjd beredskap, där flera skulle välja att inte förbereda sig alls då de saknar ekonomiska incitament för det. En sådan varierande grad av förberedelser skulle ha negativ påverkan på den sektorgemensamma förmågan att stödja totalförsvaret.

Tillhandahållarnas respektive egen förmåga är en förutsättning för sektorns förmåga. Inte minst mot bakgrund av totalförsvarsplaneringen så är det viktig att regler finns.

Sammantagen bedömning

PTS gör bedömningen att det är av vikt att regleringen behålls men att den behöver förtydligas. PTS gör därför bedömningen att det finns ett behov av att språkligt och redaktionellt omformulera kraven.

3. Rättsliga förutsättningar

3.1 Bemyndiganden och regeringens medgivande

PTS beslutanderätt grundar sig på följande bemyndiganden (under förutsättningar att PTS ges bemyndigande i den nya förordningen som väntas meddelas i anslutning till nya LEK).

- Enligt 1 kap. 11 § nya LEK får PTS meddela föreskrifter om den fredstida planeringen för totalförsvarets behov av elektroniska kommunikationer under sådana förhållanden som att Sverige är i krig eller krigsfara eller att det råder sådana utomordentliga förhållanden som är föranledda av att det är krig utanför Sveriges gränser eller av att Sverige varit i krig eller i krigsfara.
- Enligt 8 kap. 1 § nya LEK får PTS meddela föreskrifter om de tekniska och organisatoriska åtgärder som ska vidtas för att hantera risker som hotar säkerheten i nät och tjänster.
- Enligt 8 kap. 3 § nya LEK får PTS meddela föreskrifter om rapportering av säkerhetsincidenter som har haft en betydande påverkan på nät och tjänster.
- Enligt 8 kap. 4 § nya LEK får PTS meddela föreskrifter om skyldigheten att informera användare vid ett konkret och betydande hot om en säkerhetsincident.

- Enligt 8 kap. 5 § nya LEK får PTS meddela föreskrifter om de särskilda tekniska och organisatoriska åtgärder som ska vidtas i samband med lagring och annan behandling av uppgifter för brottsbekämpande ändamål.
- Enligt 8 kap. 6 § nya LEK får PTS meddela föreskrifter om de tekniska och organisatoriska skyddsåtgärder som ska vidtas för att säkerställa att uppgifter som behandlas i samband med tillhandahållandet av tjänsten skyddas.
- Enligt 8 kap. 9 § nya LEK får PTS meddela föreskrifter om innehållet i förteckningen över integritetsincidenter.

I bilagan i denna konsekvensutredning anges vilka bemyndiganden som har använts som stöd för att meddela respektive bestämmelser i de föreslagna föreskrifterna.

3.2 EU-rätt

PTS gör bedömningen att de föreslagna föreskrifterna överensstämmer med de skyldigheter som följer av Sveriges anslutning till EU.

Bestämmelser om tillhandahållares säkerhetsåtgärder och incidentrapportering, som har sitt ursprung i kodexen och e-dataskyddsdirektivet, finns i nya LEK. De föreslagna föreskrifterna har utformats i enlighet med dessa bestämmelser genom att de syftar till att uppnå en nivå på säkerheten som är lämplig i förhållande till risken. Föreskrifterna förtydligar vilka åtgärder som ska vidtas samt hur och när incidentrapportering ska ske.[19] PTS har dessutom, vid utarbetandet av föreskrifterna, beaktat riktlinjer utarbetade av ENISA (som syftar till att säkerställa ett harmoniserat genomförande av EU-direktiven) och EU:s verktygslåda för 5G, se vidare avsnitt 2.1. PTS bedömer således att bestämmelserna om säkerhetsåtgärder och incidentrapportering i de föreslagna föreskrifterna står i överensstämmer med både kodexen och e-dataskyddsdirektivet.

Bestämmelserna om den fredstida planeringen för totalförsvarets behov av elektroniska kommunikationer påverkas inte av den EU-rättsliga regleringen då frågorna avser nationell säkerhet för vilka nationell kompetens gäller.

[19] Dock endast säkerhetsincidenter. När och hur integritetsincidenter ska rapporteras regleras i förordning 611/2013.

4. Aktörer som berörs av regleringen

De aktörer som berörs av regleringen är tillhandahållare av nät och tjänster enligt den definition som framgår av nya LEK. Nedan beskrivs marknaden idag, med de tillhandahållare som träffas av nuvarande LEK. Därefter beskrivs de nya aktörer inom sektorn, tillhandahållare av NI-ICS, som kommer att omfattas av nya LEK.

Marknaden idag

Från att för 30 år sedan ha haft en monopolliknande marknadsstruktur med ett statligt företag som helt dominerande aktör har marknaden för elektronisk kommunikation avreglerats och huvuddelen av verksamheterna återfinns numer i den privata sektorn.[20] Marknaden har vidare genomgått en snabb tillväxt, vilket kan illustreras av den snabba framväxten av både mobiltelefoni och internetanvändning. Direkt relaterad till denna utveckling är också den snabba teknikutvecklingen, som bl.a. tar sig uttryck i form av nya och innovativa företag inom sektorn, nya konsumentbeteenden, förändringar i de traditionella aktörernas affärsmodeller, och nya säkerhetsutmaningar (se vidare avsnitt 1.2). En annan viktig faktor är att sektorn är diversifierad, innebärande att vissa företag säljer enbart slutkundstjänster, andra säljer grossisttjänster, vissa företag är enbart nätägare av passiv infrastruktur (s.k. svartfiber och kanalisation), medan andra är nätägare av aktiv infrastruktur, en del är vertikalt integrerade, några företag samarbetar i ägande av infrastruktur, osv. Det finns också s.k. virtuella tjänstetillhandahållare, där en tjänst helt och hållet produceras samt tillhandahålls i någon annans nät, men under ett eget varumärke. Ibland står underleverantörer för all infrastruktur och signalöverföring och företagen är renodlade tjänsteleverantörer. En följd av globaliseringen och tillhörande tjänsteutveckling är också att företag som verkar på den svenska marknaden inte nödvändigtvis äger nät eller har kontor i Sverige. Utländska företag på marknaden kan både vara exempelvis ett lokalt dotterbolag till en stor internationell aktör, men också en virtuell operatör utan någon fysisk närvaro.

Till den ovan beskrivna heterogena och dynamiska marknadsbilden ska dock läggas att ett fåtal aktörer har en stor andel av marknaden, och dessa aktörers marknads-andelar har varit relativt stabila över tid. Teknisk utveckling och förändringar i konsumentbeteende har lett till att intäktskällorna ser annorlunda ut idag än vad de

[20] Offentliga verksamheter finns dock fortfarande, exv. stadsnäten, där ett kommunalt bolag kan äga ett lokalt fibernät (och kanske också sälja tjänster i detsamma).

gjorde för 10–15 år sedan, men har inte på ett fundamentalt sätt förändrat marknadsstrukturen.

Ovanstående beskrivning kompletteras med de uppgifter PTS samlar in inom Svensk Telekommarknad (STM), en enkätbaserad undersökning som var sjätte månad går till de ca 600 aktörer som är anmälningspliktiga enligt nuvarande LEK. Bland dessa aktörer ryms, i stort, den ovan diskuterade heterogena grupp av privata och offentliga bolag som utgör sektorn elektronisk kommunikation. Från den senaste helårsrapporten (STM 2020, med en svarsfrekvens på 97%) framgår att sektorn sammanlagt sysselsätter ca 18 500 personer och att årsintäkterna i sektorn överstiger 76 miljarder kronor.[21] De fyra största företagen har 58 miljarder kronor i årsintäkter (från den svenska marknaden).

Fördelningen på mikro-, små-, medel- och stora aktörer ser ut som i tabell 1, där PTS i stort följer Tillväxtverkets mall för storleksindelning av företag (se vidare i tabellens förklarande text).

Tabell 1: Berörda aktörer (aktörer som omfattas av nuvarande LEK)

Storlek	En aktör tillhör respektive kategori om	Antal	Andel
Mikro	Antal anställda < 10 & Årsintäkt < 20 MSEK *(varav högst en anställd och intäkt < 2 MSEK)*	410 *(120)*	70 %
Små	Antal anställda < 50 & Årsintäkt < 100 MSEK Minst en av variablerna är större än för mikrokategorin	132	22 %
Medel	Antal anställda < 250 & Årsintäkt < 500 MSEK Minst en av variablerna är större än för kategorin av små aktörer	35	6 %
Stora	Antal anställda ≥ 250 eller Årsintäkt ≥ 500 MSEK	11	2 %
Totalt		**588**	**100 %**

Tabell 1. Antal och storleksindelning av aktörerna enligt Svensk Telekommarknad 2020 (för de 97% som svarade på PTS enkät). Indelningen betraktar de två variablerna antal anställda och årsintäkt (båda variablerna avser den del av aktörens verksamhet som regleras av nuvarande LEK). Om ett företag (hypotetiskt) skulle klassificeras som t.ex. ”mikroföretag” enligt ena variabeln (0-9 anställda) men ”småföretag” enligt den andra variabeln (intäkt mellan 20 och 100 miljoner kronor), är det den större av de två kategorierna som bestämmer klassificeringen, enligt ovan. Indelningen följer i stort Tillväxtverkets rekommendation[22] om att använda en variabel som fångar storleken på personalstyrka och därtill en ekonomisk variabel. I brist på data på årsomsättning har vi använt årsintäkt. Indelningen följer vidare Tillväxtverkets rekommendation om särskild hänsyn till små företag.[23] Tabellen innehåller ett 80-tal

[21] 588 av 605 aktörer svarade i STM 2020. 62 aktörer med sammanlagt 289 anställda rapporterade inte någon intäktssiffra i STM 2020, den i texten givna totala intäktssiffran är därför en nedre gräns.
[22] Vilka företag berörs? - Tillväxtverket (tillvaxtverket.se).
[23] Särskild hänsyn till små företag - Tillväxtverket (tillvaxtverket.se).

utländska aktörer, indelningen svensk/utländsk diskuteras dock inte vidare. MSEK – miljoner kronor. Källa: STM 2020 (PTS).

PTS har utöver indelningen i tabell 1 gjort följande ytterligare indelningar av de tillhandahållare som omfattas av nuvarande LEK inom ramen för denna konsekvensutredning.

- I tabell 1 har mikrokategorin en underkategori som består av 120 aktörer som har högst en anställd och mindre än 2 miljoner kronor i årsintäkt. PTS använder denna underkategori som en proxy för en grupp av aktörer som, i praktiken, träffas mindre av den nya regleringen. PTS bedömer att det inom mikrokategorin återfinns många aktörer som exempelvis vidareförsäljer en kommunikationstjänst utan att själva producera denna tjänst i ett eget nät. Tjänsten köps in och säljs sedan vidare. Även om dessa aktörer omfattas av regleringen träffas de troligen i lägre grad eftersom tjänsten i praktiken produceras hos en annan aktör.
- De aktörer som är enbart nättillhandahållare påverkas av de föreslagna föreskrifterna på ett annat sätt än tjänstetillhandahållare (med eller utan nät). Därför är det av intresse att vidare dela upp aktörerna i dessa två kategorier (tabell 2). Ett problem är dock att det inte går att klassificera alla aktörerna i någon av de två kategorierna. Tabell 2 delar därför in aktörerna i tre kategorier, där den tredje kategorin kallas ”icke-klassificerade” (se vidare i tabellens förklarande text och i avsnitt 6).
- PTS bedömer att de 155 icke-klassificerade aktörerna i tabell 2 består av två ungefärligen lika stora grupper, där endast den ena gruppen är relevant för analysen. I kostnadsestimaten i avsnitt 6 räknar vi därför in 80 av de 155 icke-klassificerade aktörerna.

Tabell 2: Berörda aktörer (aktörer som omfattas av nuvarande LEK) indelade efter storlek och på nättillhandahållare, tjänstetillhandahållare (med/utan nät) respektive på de aktörer som inte går att klassificera enligt de data som finns i STM.

	Typ av aktör		
Storlek (enligt definition i tabell 1)	**Endast nättillhandahållare**	**Tjänstetillhanda-hållare (med/utan nät)**	**Icke-klassificerade**
Mikro *(varav ≤1 anställd och intäkt <2 MSEK)*	78 *(13)*	205 *(66)*	127 *(41)*
Små	25	88	19

Medel	1	25	9
Stora	1	10	0
Totalt	**105**	**328**	**155**
Kolumn	A	B	C

Tabell 2. Indelning av aktörerna från tabell 1 i enbart nättillhandahållare respektive tjänstetillhandahållare (med/utan nät). Data på nättillhandahållare kommer från PTS Bredbandskartläggning 2020, med tillägg av ett fåtal mobilnätsaktörer. Som tjänstetillhandahållare definieras de aktörer som har någon intäkt, i STM-data, från sådana tjänster som PTS bedömer omfattas av den aktuella föreskriften. Aktörer som är både nättillhandahållare och har positiva tjänsteintäkter återfinns i kolumn B. I kolumn C återfinns de aktörer som, i data, inte är nättillhandahållare och som har noll i (för regleringen relevanta, enligt nuvarande bedömning) tjänsteintäkter, eller inte har rapporterat intäkter i STM. Två faktorer gör alltså att vissa aktörer hamnar i denna kategori: aktörerna har inte rapporterat intäkter i STM eller aktörerna har tjänsteintäkter som är av en art att PTS, i nuläget, bedömer att de inte omfattas av regleringen.[24] Varje rad i tabell 2 summerar till siffran i motsvarande rad i tabell 1. Källor: STM 2020, Bredbandskartläggningen 2020 (PTS).

Vissa andra underleverantörer till aktörerna kan också komma att träffas av de nya föreskrifterna. Dock är en aktör ansvarig för att den tjänst den tillhandahåller är säker, oberoende av om den är producerad internt i företaget eller upphandlad (tillhandahållare kan inte kontraktera bort sitt ansvar).[25]

Nya aktörer i företagssektorn

När nya LEK träder i kraft kommer även tillhandahållare av NI-ICS att omfattas av regelverket, vilket de inte gör idag enligt nuvarande LEK, se vidare avsnitt 1.1.3. Dessa aktörer ingår inte i tabellerna 1 och 2 ovan och PTS har i dagsläget heller ingen formell möjlighet att begära in information från dessa aktörer.

Tillhandahållare av NI-ICS är en relativt ”ny” ”grupp” av företag, troligen mycket heterogen, som hittills inte varit reglerad i telekomsektorn. Exempel på sådana tjänster är tjänster där en chattfunktion är själva huvudtjänsten. Några andra exempel kan vara e-posttjänster och vissa videosamtals- och internettelefonitjänster. Kategorin kan även omfatta chatt- och samtalsfunktioner på dejtingsajter och i online-spel. Några av världens största it-bolag har tjänster inom NI-ICS-kategorin, men här återfinns också mikroföretag.

Två utmärkande drag för dessa företag är att de ofta tillhandahåller tjänster i någon annans nät och att tjänsterna inte är direkt platsberoende (ett företag kan drivas från exempelvis Kalifornien och erbjuda tjänster i Sverige). Tjänsterna och infrastrukturen kan dock komma att bli mer platsberoende över tid om exempelvis en marknad växer

[24] Utöver kategorin av icke-klassificerade går det inte att utesluta att ett fåtal aktörer skulle kunna vara felkategoriserade mellan nät- och tjänstetillhandahållarkategorierna, pga. databegränsningar.

[25] I våra kostnadsskattningar avsnitt 6 kan vi inte utesluta att en del underleverantörer, som inte själva är LEK-aktörer, skulle kunna få ökade kostnader. Sådana kostnader tas inte om hand av de estimat vi tagit fram. En kartläggning av sådana förhållanden skulle innebära ett mycket omfattande arbete och de stora kostnaderna faller troligen på LEK-aktörerna själva.

väldigt mycket (lokal utrustning kan komma att behövas, bl.a. för att kunna erbjuda en snabb tjänst).

Ett annat utmärkande drag för ”NI-ICS-marknaden” är dess dynamik och att uppstartskostnaderna i många fall kan vara låga. Detta i sig gör sektorn svår att kartlägga, eftersom appar och andra tjänster kan skapas och växa snabbt, men också försvinna snabbt. I PTS kostnadsestimat i avsnitt 6 har myndigheten utgått från vad som krävs för att tillhandahålla en NI-ICS, utan att säga något specifikt om den finansiella och organisatoriska storleken på tillhandahållaren. PTS har därefter skattat dess regleringskostnader med hjälp av viss informationsinhämtning från marknaden samt intern och extern säkerhets- och regleringskompetens. I avsnitt 6 diskuteras ytterligare de begränsningar som funnits i kartläggningen av kostnaderna för tillhandahållare av NI-ICS.

5. Samråd med berörda aktörer

Enligt artikel 41.5 i kodexen ska PTS, såsom behörig myndighet, samråda och samarbeta med de myndigheter som anges i artikeln. Av nuvarande LEK och förordningen (2003:396) om elektronisk kommunikation följer dessutom att PTS i samband med regelgivning ska samråda med ett antal angivna myndigheter.

PTS har därför i arbetet med de nya föreskrifterna genomfört samråd med Energimyndigheten, Finansinspektionen, Försvarsmakten, Inspektionen för vård och omsorg, Integritetsskyddsmyndigheten, Livsmedelsverket, Myndigheten för samhällsskydd och beredskap, Polismyndigheten, Säkerhetspolisen, Transportsstyrelsen och Tullverket.

Först genomfördes ett tidigt samråd med myndigheterna i syfte att informera om det påbörjade arbetet och förankra den inriktning PTS hade i arbetet. Syftet var även att samla in förslag, information och synpunkter i ett tidigt skede av processen för att säkerställa en ändamålsenlig reglering. Senare i processen har ytterligare ett samråd med myndigheterna genomförts genom ett skriftligt förfarande. I detta samråd har PTS uppdaterat myndigheterna om arbetets inriktning och den fortsatta processen.

Särskilt Säkerhetspolisen har inom ramen för samrådet framfört synpunkter på de föreslagna föreskrifterna, i form av ett antal styrande principer. PTS har i den mån det

har varit relevant för detta arbete och utifrån vad som ryms inom myndighetens bemyndigande beaktat dessa synpunkter.

Utöver samråd med myndigheter har PTS också genomfört dialogmöten med representanter från marknadens aktörer. I syfte att informera samt inhämta information och underlag till arbetet har PTS haft dialog med de fyra största mobiloperatörerna samt med Svenska stadsnätsföreningen och TechSverige (tidigare IT- och Telekomföretagen).

För att få ett bra underlag till beräkningar av kostnader och bedömningar av konsekvenser av de föreslagna kraven har PTS dessutom skickat ut frågeformulär till ett urval av berörda tillhandahållare.

Ett frågeformulär om vilka kostnader och konsekvenser som följer av de föreslagna föreskrifterna för NI-ICS har skickats till ett urval av tillhandahållare ur denna kategori.

Ytterligare ett frågeformulär om vilka kostnader och konsekvenser de förändrade bestämmelserna i de föreslagna föreskrifterna skulle medföra har skickats till ett urval av aktörer som är anmälda till PTS enligt 2 kap. nuvarande LEK. Urvalet har gjorts utifrån olika kategorier av nät- och tjänstetillhandahållare utifrån uppdelningen mikro, små, medelstora och stora aktörer.

PTS finner de genomförda samråden värdefulla och uppskattar den konstruktiva dialog som varit. PTS vill härmed tacka de myndigheter och tillhandahållare som har bidragit med information, synpunkter, underlag och förslag i arbetet.

6. Föreslagna krav och ekonomiska effekter för företag och andra aktörer

6.1 Allmänt om redovisningen i avsnitt 6

Dispositionen i kommande avsnitt

Avsnitten 6.3–6.20 redovisar innebörden av samtliga bestämmelser och allmänna råd i de föreslagna föreskrifterna samt de ekonomiska effekter som dessa krav får för de olika typerna av tillhandahållare. Varje avsnitt motsvarar ett område (kapitel) som regleras i föreskriften. Avsnitt 6.21 sammanfattar alla kostnadsskattningar i tabellform.

Varje avsnitt inleds med en redovisning om vad bestämmelserna inom det aktuella området handlar om, hur de förhåller sig till nuvarande föreskrifter och vilka tillhandahållare som ska tillämpa bestämmelserna. Därefter beskrivs själva regleringen, dvs. bestämmelsernas syfte och innebörd. Efter det redovisas de ekonomiska konsekvenser som bestämmelserna innebär för de olika kategorier av tillhandahållare som omfattas, med undantag för avsnitten 6.3 och 6.4, som inte bedöms medföra några konsekvenser.

Notera att det i anslutning till vissa bestämmelser ges exempel på säkerhetsåtgärder. Dessa exempel utgör endast generella förtydliganden kring en viss reglering och ska inte nödvändigtvis ses som en rekommendation eller en garanti för att ett krav med säkerhet uppfylls om just den säkerhetsåtgärden vidtas. Det måste alltid göras en prövning i det enskilda fallet. Sektorn är diversifierad, den inkluderar både små och stora tillhandahållare av olika karaktär som erbjuder olika typer av tjänster. I varje enskilt fall är riskerna olika och vad som är lämpligt att göra i ett fall för att hantera en viss risk kan vara otillräckligt eller för långtgående i andra fall.

Övergripande om kostnadsmässiga och andra konsekvenser av föreslagna krav och allmänna råd

Flera bestämmelser överförs i huvudsak oförändrade från nuvarande gällande föreskrifter till de nya föreskrifterna. Dessa kommer inte att medföra några nya kostnader eller administrativa bördor i dessa delar för de tillhandahållare som redan omfattas av de nuvarande föreskrifterna. Konsekvenserna av dessa bestämmelser har bedömts inför att dessa föreskrifter togs fram.

Ett antal bestämmelser i de nya föreskrifterna motsvarar delvis regleringen i nuvarande föreskrifter. I dessa fall anges att bestämmelsen i huvudsak eller delvis motsvarar en viss bestämmelse i nuvarande föreskrifter. Ett antal bestämmelser är nya och saknar därmed motsvarighet i nuvarande föreskrifter. När det anges att en bestämmelse är ny eller ändras, avses nyheter och ändringar i förhållande till nuvarande föreskrifter. Det är för dessa nya krav samt för justerade krav i materiellt hänseende som PTS skattar och redovisar de ekonomiska konsekvenserna.

PTS har använt två metoder för kostnadsskattningar, dels egna skattningar med bas i PTS egen kunskap om vad regleringen innebär för aktörerna, dels inhämtning av information från marknaden.

PTS har inhämtat upplysningar om bedömd tidsåtgång för initiala och årliga administrativa kostnader samt övriga kostnader med anledning av de föreslagna föreskrifterna. Upplysningar har inhämtats från ett urval av nät- och tjänstetillhandahållare på marknaden. 20 tillhandahållare har inkommit med upplysningar. Dessa representerar tillhandahållare inom mikro, små, medelstora och

stora aktörer. PTS har också inhämtat upplysningar från den tidigare oreglerade kategorin av aktörer, tillhandahållare av NI-ICS. Tre av dessa tillhandahållare har inkommit med upplysningar.[26]

De kostnader som redovisas i avsnitten 6.5–6.20 baseras på PTS egna skattningar med beaktande av de inkomna upplysningarna från marknaden. I avsnitt 6.21, där kostnaderna sammanställs, diskuteras mer i detalj hur PTS skattningar förhåller sig till den information som inhämtats från marknaden.

Generellt gäller att storleken på kostnader som föranleds av de föreslagna föreskrifterna beror på vilka tekniska och organisatoriska säkerhetsåtgärder som tillhandahållare redan vidtar. I vissa fall har PTS valt att exemplifiera åtgärder som kan ge upphov till kostnader.

De föreslagna bestämmelserna får i många fall olika konsekvenser för olika kategorier av tillhandahållare. I dessa fall redovisas således kostnaderna utifrån respektive kategori.

För tillhandahållare av NI-ICS redovisas en skattad kostnad per aktör som baseras på kostnaden att tillhandahålla tjänsten. För nättillhandahållare och övriga tjänstetillhandahållare redovisas en skattad kostnad uppdelat på storleken på tillhandahållarna (mikro-, små-, medelstora och stora företag).

Kostnader redovisas som administrativa engångskostnader, administrativa årliga kostnader och övriga kostnader.

När det gäller de administrativa kostnaderna baseras dessa på det skattade antalet timmar som krävs för att efterleva ett visst krav (exempelvis genom att initialt upprätta eller komplettera processer och, därefter, de årliga kostnaderna för exempelvis revidering av dessa) multiplicerat med en timkostnad, som utgörs av en genomsnittlig lönekostnad per timme.

PTS har tagit fram den genomsnittliga lönekostnaden per timme utifrån löneuppgifter i SCB-data år 2020, redovisade enligt standarden för svensk yrkesklassificering 2012 (SSYK2012). PTS har beaktat månadslönerna för ett antal olika yrkesroller inom privat sektor (där de flesta aktörerna återfinns), som PTS bedömer kan vara aktuella vid

[26] Upplysningarna inhämtades genom att PTS tog fram och skickade ut två enkäter. Den första enkäten skickades till tillhandahållare av NI-ICS. Den andra enkäten skickades till nät- respektive övriga tjänstetillhandahållare. Enkäterna var frivilliga. Den första enkäten skickades till ett tiotal tillhandahållare av NI-ICS med någon form av etablering i Sverige. Den andra enkäten skickades till 89 tillhandahållare som valdes ut slumpmässigt (stratifierat slumpmässigt urval). Svarsfrekvensen gällande den andra enkäten är hög bland de stora aktörerna, men mycket låg bland aktörerna i mikrokategorin. PTS kan inte utesluta att även om de 89 aktörerna valdes ut slumpmässigt är de aktörer som svarade ett selekterat snarare än representativt urval.

genomförandet av arbetet. Utifrån dessa uppgifter har en genomsnittlig månadslön om 47 000 kronor per månad beräknats. Månadslönen har sedan multiplicerats med schablonvärdet 1,84 för att inkludera semesterersättning, arbetsgivaravgifter och overhead enligt Tillväxtverkets handledning, vilket ger en månadskostnad på 86 480 kronor och därmed en kostnad på 541 kronor per timme, utifrån schablonvärdet 160 arbetstimmar per månad används.

När det gäller övriga kostnader kan dessa exempelvis utgöras av kostnader för anskaffning av ny hårdvara, mjukvara och licenser samt personalkostnader hänförliga till utbildningskostnader.

I avsnitt 6.21 redovisar PTS den samlade, totala kostnaden för de föreslagna föreskrifterna. För samtliga tillhandahållare förutom tillhandahållare av NI-ICS summeras kostnaderna för de olika storlekarna mikro, små, medelstor och stor med avseende på hur många aktörer som ingår i respektive kategori. Kostnads-redovisningen ser olika ut beroende på om kraven träffar nättillhandahållare eller tjänstetillhandahållare (med/utan nät). Antal anmälda tillhandahållare i respektive kategori och storleksklass framgår av tabell 2 i avsnitt 4. I avsnitt 6.21 görs en korrektion för att vissa av aktörerna i mikrokategorin (de minsta) bedöms träffas lindrigare, enligt resonemang i avsnitt 4. Vidare finns, som diskuterades i avsnitt 4, 155 aktörer som svarat på STM men för vilka PTS saknar tillräcklig information för att de ska kunna klassificeras. I denna grupp bedömer PTS att 80 aktörer bör tas med i kostnadsskattningarna och att kostnaderna är som för tjänstetillhandahållarna. De 80 aktörerna har lagts till, i tjänstetillhandahållarkategorin, enligt storleksfördelningen i kolumn C i tabell 2 i avsnitt 4.

6.2 Allmänt om föreskrifterna

Tillhandahållare

De föreslagna föreskrifterna gäller alla som tillhandahåller allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster.[27]

Skyldigheten att vidta säkerhetsåtgärder i de föreslagna föreskrifterna gäller för tillhandahållare oaktat om arbetet utförs i egen regi eller om extern aktör uppdras att utföra arbetet. Det är därmed av vikt att de tillhandahållare som väljer att använda sig av externa aktörer säkerställer att kraven på säkerhet och integritet regleras i avtal samt att tillhandahållare följer upp säkerhetsarbetet både innan och under avtalstiden för att säkerställa att kraven efterlevs av underleverantören. Bristande kravställning

[27] Det innebär, till följd av att definitionen av vad som utgör en elektronisk kommunikationstjänst har fått en delvis annan utformning i nya LEK, att även den som tillhandahåller NI-ICS numera omfattas av föreskrifterna.

och kontroll av underleverantörer kan medföra bristande säkerhet. Sådana brister är något tillhandahållare hålls ansvariga för.

Säkerhet i nät och tjänster samt skydd av och säkerhet för behandlade uppgifter

De föreslagna föreskrifterna innehåller till övervägande del bestämmelser om de tekniska och organisatoriska åtgärder som ska vidtas enligt 8 kap. 1, 5 och 6 §§ nya LEK. Det handlar alltså om de åtgärder som tillhandahållare ska vidta för att hantera risker som hotar säkerheten i nät och tjänster, säkerställa skyddet för uppgifter som behandlas i samband med tillhandahållandet av tjänsten samt säkerställa skydd för uppgifter som ska lagras för brottsbekämpande ändamål enligt 9 kap. 19 § nya LEK.

Skyldigheterna enligt 8 kap. 1, 5 och 6 §§ nya LEK är delvis överlappande men syftet med respektive bestämmelse skiljer sig delvis åt och nivån på säkerheten eller skyddet som ska uppnås kan vara olika. Det gör att de konkreta åtgärder som tillhandahållare behöver vidta för att hantera en viss risk och uppnå ett visst syfte kan skilja sig åt beroende på den enskilda verksamhetens förutsättningar. I denna konsekvensutredning används dock begreppen ”åtgärder” eller ”säkerhetsåtgärder” för samtliga de åtgärder som ska vidtas enligt 8 kap. 1, 5 och 6 §§ nya LEK jämte de föreslagna föreskrifterna. För det fall att åtgärderna behöver anpassas för att uppfylla de olika förutsättningarna som anges i 8 kap. 1, 5 respektive 6 §§ nya LEK så framgår det av respektive bestämmelse vad som gäller.

Säkerhet och skydd

Vad som avses med säkerhet i nät och tjänster anges i 1 kap. 7 § nya LEK. Uttrycket definieras som elektroniska kommunikationsnäts och elektroniska kommunikationstjänsters förmåga att vid en viss tillförlitlighetsnivå motstå händelser som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos näten eller tjänsterna, hos lagrade, överförda eller behandlade uppgifter eller hos de närliggande tjänster som erbjuds genom eller är tillgängliga via dessa elektroniska kommunikationsnät eller elektroniska kommunikationstjänster.

Skydd av och säkerhet för behandlade uppgifter handlar om att skydda uppgifterna mot oavsiktlig eller otillåten utplåning, förlust eller ändring eller otillåtet avslöjande av eller otillåten åtkomst till uppgifter, dvs. integritetsintrång. Jämför definitionen av integritetsincidenter i 1 kap. 7 § nya LEK.

I 9 kap. nya LEK stadgas vilka uppgifter en tillhandahållare får eller ska behandla. Vissa uppgifter behöver tillhandahållare behandla och därmed skydda för att framför allt säkerställa att avtalsförhållandet mellan tillhandahållare och dennes kund fullgörs. Andra uppgifter behöver tillhandahållare behandla för att brottsbekämpande myndigheter ska kunna avslöja och utreda brott. Tillhandahållare behöver säkerställa

att dessa uppgifter ska kunna användas av de brottsbekämpande myndigheterna, att de skyddas och att de har en hög kvalitet.

Tekniska och organisatoriska åtgärder

Åtgärderna som ska vidtas kan vara både tekniska och organisatoriska.

Tekniska åtgärder är t.ex. åtgärder som skyddar nät, tjänster och uppgifter mot obehörig åtkomst, oavsiktlig eller olaglig förstörelse, förlust eller ändring samt skydd av lokaler och utrustning. I organisatoriska åtgärder ingår t.ex. att säkerställa att endast auktoriserad personal får tillgång till uppgifter samt att upprätta rutiner och processer för säkerhetsarbetet.

Nivå på säkerhet

Skyldigheten att vidta tekniska och organisatoriska åtgärder enligt 8 kap. 1, 5 och 6 §§ nya LEK är kopplad till den risk som hotar säkerheten i nät och tjänster respektive skyddet av uppgifterna. Som angetts ovan uppställer dock de olika paragraferna något olika krav på nivån på säkerheten eller skyddet som ska uppnås vilket gör att tillhandahållare behöver anpassa åtgärderna efter detta för att efterleva lagstiftningen.

När det gäller åtgärder enligt 8 kap. 1 § nya LEK följer det av den bestämmelsen att tillhandahållare ska säkerställa en nivå på säkerheten som är lämplig i förhållande till risken.

I att åtgärderna ska säkerställa en lämplig nivå på säkerheten ligger bl.a. att de tekniska lösningar som är tillgängliga på marknaden vid varje given tidpunkt ska beaktas. Teknisk utveckling kan därför leda till att behovet av säkerhetsåtgärder förändras eller innebära nya möjligheter att vidta effektiva säkerhetsåtgärder. Kravet på att beakta den tekniska utvecklingen ligger i att säkerhetsåtgärderna ska ligga på en lämplig säkerhetsnivå (jfr prop. 2017/18:205 s. 41). Risken bör bedömas utifrån en identifiering av samtliga relevanta hot mot och sårbarheter hos tillgångar eller förbindelser, inklusive de komponenter, utrustningar, leverantörer och serviceavtal som används. I riskbedömningen ska hänsyn tas till sannolikheten för att ett hot realiseras och vilka konsekvenser det får om hotet realiseras. Dessa faktorer kan förändras över tid. Det kan t.ex. ske genom händelser i omvärlden som påverkar hotbilden eller förändringar i samhället som påverkar beroendet av kommunikationstjänsterna och därmed de potentiella konsekvenserna i händelse av att ett hot förverkligas. I lämplighetsbedömningen ingår även att beakta kostnaderna för att genomföra olika åtgärder. Med hänsyn till att vad som är en lämplig nivå på säkerheten ändras över tid, t.ex. genom förändringar i risker eller genom nya tekniska

lösningar, behöver aktörerna regelbundet och vid behov se över sina riskbedömningar och bedöma vilka säkerhetsåtgärder som är lämpliga att vidta.[28]

När det gäller åtgärder enligt 8 kap. 6 § nya LEK följer att de åtgärderna ska vara lämpliga för att säkerställa att uppgifter som behandlas i samband med tillhandahållandet av tjänsten skyddas. Åtgärderna ska vara ägnade att säkerställa en säkerhetsnivå som, med beaktande av tillgänglig teknik och kostnaderna för att genomföra åtgärderna, är anpassad till risken för integritetsincidenter.

När det gäller uppgifter som lagras för brottsbekämpande ändamål enligt 9 kap. 19 § nya LEK framgår det av 8 kap. 5 § nya LEK att den som är skyldig att lagra sådana uppgifter ska vidta de *särskilda* tekniska och organisatoriska åtgärder som behövs för att skydda de lagrade uppgifterna vid behandling. Detta är således en särskild bestämmelse om de åtgärder som ska vidtas för att skydda uppgifter som lagras för brottsbekämpande ändamål som till skillnad från 8 kap. 6 § nya LEK tar sikte på ett grundskydd för behandlingen av uppgifter.

Till skillnad från vad som gäller enligt 8 kap. 6 § nya LEK lämnas i 8 kap. 5 § nya LEK inte något utrymme att bestämma säkerhetsnivån genom en avvägning mellan teknik, kostnader och risken för integritetsintrång. Istället måste tekniska och organisatoriska åtgärder vidtas som säkerställer att uppgifterna skyddas vid behandling.[29] Av praxis framgår vidare att tillhandahållare måste garantera en särskilt hög skydds- och säkerhetsnivå med hänsyn till att det är fråga om en stor mängd uppgifter, att dessa är av känslig natur och att det finns en risk för otillåten tillgång till uppgifterna.[30]

6.3 Tillämpningsområde

1 kap. 1 § inleder de föreslagna föreskrifterna med att klargöra föreskrifternas tillämpningsområde. Bestämmelsen medför inte några konsekvenser.

De föreslagna föreskrifterna gäller alla som tillhandahåller allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster.

Varje enskild bestämmelse i de föreslagna föreskrifterna gäller dock inte samtliga tillhandahållare. Det finns ett antal bestämmelser som endast gäller en viss utpekad

[28] Se prop. 2021/22:136 Genomförande av direktivet om inrättande av en europeisk kodex för elektronisk kommunikation, s 315.

[29] Se prop. 2018/19:86 *Datalagring vid brottsbekämpning – anpassningar till EU-rätten*, sid 100 som i sin tur hänvisar till prop. 2010/11:46 *Lagring av trafikuppgifter för brottsbekämpande ändamål - genomförande av direktiv 2006/24/EG* s. 75.

[30] Se EU-domstolens dom av den 21 december 2016, C-203/15 och C-698/15, EU:C:2016:970, punkt 122.

grupp av tillhandahållare eller först när vissa förutsättningar är uppfyllda. Det framgår av respektive bestämmelse vilket tillämpningsområde som gäller.

6.4 Ord och uttryck

De föreslagna föreskrifterna förklarar i 2 kap. de ord och uttryck som används i föreskriften.

Bestämmelserna om de ord och uttryck som används i föreskriften medför inte några konsekvenser.

Följande ord och uttryck är av särskild betydelse i föreskrifterna.

Tillgång och informationsbehandlingstillgång

I föreskrifterna användas begreppen ”tillgång” och ”informationsbehandlingstillgång”. Begreppen är delvis överlappande.

Begreppet ”tillgång” används i föreskrifterna för att beteckna en funktion som är nödvändig för att tillhandahålla kommunikationsnätet eller kommunikationstjänsten och som utgör en avgränsad del av nätet eller tjänsten som är avsedd att användas för att sända, motta, bearbeta eller lagra information. En tillgång utgör således en aktiv del av nätet eller tjänsten.

Tekniska system som används för elektronisk kommunikation använder traditionellt en kombination av hård- och mjukvara för att fungera, och består normalt av ett antal olika tillgångar. Exempel på tillgångar i kommunikationsnät och kommunikationstjänster kan vara routrar, switchar, olika typer av servrar, lastbalanserare, basstationer, virtuella maskiner, anropsgränssnitt hos tredjepartstjänster och gateways.

Att en tillgång ska vara *nödvändig* för tillhandahållandet av nätet eller tjänsten innebär att det är fråga om inte helt oväsentliga funktioner i nätet eller tjänsterna. Att en tillgång ska utgöras av en *avgränsad del* med ett visst *avgränsat syfte* innebär å andra sidan att en tillgång inte heller kan vara hur betydande som helst, t.ex. kan inte en tillhandahållares hela kärnnät anses utgöra en tillgång.

Det är tillhandahållare som själva definierar vilka funktioner i deras nät och tjänster som utgör tillgångar. Tillhandahållare bedömer således själva om t.ex. en teknikbod ska ses som en tillgång i sin helhet eller om enskilda routrar och switchar i boden ska ses som tillgångar. Vid bedömningen är det dock viktigt att komma ihåg att tillgången måste vara *nödvändig* för att tillhandahålla tjänsten vilket gör att en tillgång t.ex. åtminstone behöver vara av viss omfattning och betydelse.

Begreppet ”informationsbehandlingstillgång” används i föreskriften för system, databaser och fysiska resurser som används för informationsbehandling.

Informationsbehandlingstillgång är således resurser som hanterar de uppgifter tillhandahållare får eller ska behandla enligt bestämmelserna i 9 kap. nya LEK. Det inkluderar därmed även sådana uppgifter som en tillhandahållare kan vara skyldig att lagra för brottsbekämpande ändamål enligt 9 kap. 19 § nya LEK.

Aktiv anslutning

Begreppet ”aktiv anslutning” används i föreskrifterna för att beteckna en anslutning till ett kommunikationsnät eller en kommunikationstjänst som möjliggör omedelbar användning av kommunikationstjänster.

Eftersom föreskrifterna endast gäller nät och tjänster som är allmänna omfattas inte anslutningar inom ett nät eller tjänst som inte är allmänna, t.ex. användare bakom en företagsbrandvägg om dessa användares utrustningar endast är anslutna till detta slutna nät.

Det faktum att en aktiv anslutning möjliggör omedelbar användning innebär inte att anslutningen, t.ex. mobiltelefonen, måste vara påslagen och i bruk just i detta nu, men för att räknas in under begreppet ska mobilanvändaren kunna använda sin anslutning, dvs. den ska vara aktiverad av tillhandahållare.

6.5 Övergripande säkerhetsarbete

3 kap. i förslaget till nya föreskrifter innehåller bestämmelser om övergripande säkerhetsarbete.

Säkerhetsarbetet avser det arbete som tillhandahållare ska bedriva för att kunna:

- hantera risker som hotar säkerheten i nät och tjänster,
- säkerställa att uppgifter som behandlas i samband med tillhandahållandet av tjänsten skyddas,
- säkerställa att uppgifter som lagras för brottsbekämpande ändamål skyddas, samt
- säkerställa totalförsvarets behov av elektroniska kommunikationer vid höjd beredskap eller krig.

Bestämmelserna motsvarar 3 § PTSFS 1995:1, delvis 3 §, andra och fjärde styckena i allmänna råd till 3 § och första stycket i allmänna råd till 4 § PTSFS 2012:4, 3 § PTSFS 2014:1, samt 3 § PTSFS 2015:2, med vissa ändringar.

De föreslagna bestämmelserna omfattar samtliga tillhandahållare. För tillhandahållare av NI-ICS är bestämmelserna nya. Tillhandahållare av NI-ICS är emellertid inte

skyldiga att säkerställa att uppgifter som lagras för brottsbekämpande ändamål skyddas eftersom dessa inte omfattas av skyldigheten att lagra sådana uppgifter. Tillhandahållare av NI-ICS är inte heller skyldiga att säkerställa totalförsvarets behov av elektroniska kommunikationer vid höjd beredskap eller krig. För övriga tillhandahållare – som redan omfattas av nuvarande föreskrifter – kan vissa delar i bestämmelserna vara nya.

6.5.1 Beskrivning av bestämmelserna

3 kap. 1 § innehåller krav om att tillhandahållares säkerhetsarbete ska vara långsiktigt, kontinuerligt och systematiskt. Regleringen utgör en portalparagraf och ska beaktas vid tillämpningen av övriga bestämmelser i föreskrifterna.

Ett långsiktigt, kontinuerligt och systematiskt säkerhetsarbete i hela verksamheten är enligt PTS en grundläggande förutsättning för att tillhandahållare på ett effektivt sätt, som ständigt utvecklas och förbättras, ska kunna säkerställa skydd av och säkerhet för nät, tjänster och uppgifter. Det är också en förutsättning för att i fredstid kunna planera för att tillgodose totalförsvarets behov av elektroniska kommunikationer.

Det övergripande säkerhetsarbetet ska beakta och omfatta såväl normala förhållanden som extraordinära händelser. Det innebär att arbetet ska hantera allt från mindre incidenter som kan inträffa ofta till katastrofscenarier som kan påverka hela eller stora delar av verksamheten.

Ett säkerhetsarbete som är *långsiktigt* innebär att tillhandahållare säkerställer att arbetet är framåtsyftande och kan förebygga t.ex. säkerhets- och integritetsincidenter. Säkerhetsarbetet är således inte en engångsinsats som utförs på förekommen anledning, även om säkerhetsarbetet självklart också måste bestå av åtgärder som inriktas på att hantera inträffade säkerhetsincidenter.

Ett säkerhetsarbete som är *kontinuerligt* innebär att tillhandahållare har ett upprepande och återkommande angreppssätt i arbetet, t.ex. genom att följa upp införda säkerhetsåtgärder, förnya riskanalyser och se till att ny personal utbildas i befintliga processer för att inte riskera att säkerhetsarbetet blir godtyckligt eller förändras vid personalomsättning.

Ett säkerhetsarbete som är *systematiskt* innebär att tillhandahållare måste arbeta metodiskt och planerat, t.ex. genom att i förväg upprätta och sedan följa processer och planer för säkerhetsarbetet i syfte att bibehålla en given säkerhetsnivå, samt kunna agera effektivt på säkerhets- och integritetsincidenter.

I allmänna råd till 1 § anges att etablerade standarder i ISO/IEC 27000-serien eller motsvarande bör användas till stöd för att kunna bedriva ett långsiktigt, kontinuerligt och systematiskt säkerhetsarbete. Exempel på sådana etablerade standarder är SS-

ISO/IEC 27001 *Ledningssystem för informationssäkerhet*, SS-ISO/IEC 27002 *Riktlinjer för styrning av informationssäkerhet* och SS-ISO/IEC 27005 *Riskhantering för informationssäkerhet*.

3 kap. 2 § föreskriver vidare att tillhandahållare ska ha en tydlig rollfördelning med särskilt utpekade ansvariga för säkerhetsarbetet. Rollfördelningen ska dokumenteras. Det är enligt PTS av vikt att det finns befattningar eller personer som har ett ansvar för säkerhetsarbetet så att arbetet upprätthålls och drivs framåt.

Tillhandahållare ska även, enligt 3 kap. 3 §, upprätta och dokumentera de processer, rutiner, planer och tester som regleras i övriga bestämmelser i föreskriften. Processer, rutiner och planer ska dessutom revideras vid behov. Revidering kan t.ex. vara motiverat att göra efter inträffade säkerhets- eller integritetsincidenter, efter att en plan (t.ex. kontinuitetsplanen) använts eller övats eller i samband med att en standard – som en viss process baseras på – uppdateras.

Vidare ska tillhandahållare, enligt 3 kap. 4 §, säkerställa att anställda och uppdragstagare har kunskap om och tillämpar de processer, rutiner och planer som de berörs av. Att processer, rutiner och planer är etablerade samt att de är kända för anställda och uppdragstagare är enligt PTS en viktig förutsättning för att säkerställa att säkerhetsarbetet efterlevs i praktiken samt att det ska kunna följas upp och utvecklas.

Slutligen föreskrivs i 3 kap. 5 § att ett antal åtgärder som anges i föreskrifterna ska dokumenteras samt följas upp årligen och vid behov. Att åtgärderna dokumenteras är enligt PTS en förutsättning för att tillhandahållare ska ha kontroll över vilka åtgärder som vidtagits och kunna följa upp dem över tid. Att åtgärderna regelbundet och vid behov följs upp är enligt PTS viktigt för att tillhandahållare ska kunna säkerställa att vidtagna åtgärder är ändamålsenliga. Till exempel kan det – efter att en viss åtgärd genomförts – visa sig att den inte var tillräcklig för att hantera en viss risk eller så kan nya tekniska lösningar göra att behovet av åtgärder förändras. En tillhandahållare bör analysera och överväga hur den aktuella dokumentationen ska hanteras.

I allmänna råd till 5 § anges att tillhandahållare vid uppföljning av vidtagna åtgärder bör använda sig av erfarenheter och resultat från exempelvis genomförda tester.

Olika former av tester, kontroller och utvärderingar är verktyg som kan användas för att kontrollera om vidtagna åtgärder är ändamålsenliga. I den utsträckning tillhandahållare genomför tester m.m. anser PTS att det är av vikt att resultatet av dessa används och läggs till grund för den uppföljning av vidtagna åtgärder tillhandahållare ska göra.

Att vissa tester ska genomföras framgår av de föreslagna föreskrifterna. Till exempel föreskrivs om funktionstest av reservkraftssystem och återläsning av säkerhetskopior. Utöver det anges i de allmänna råden till 5 § att penetrationstester bör göras. Ett penetrationstest är en metod för att identifiera sårbarheter i tillhandahållares it-infrastruktur, system och tjänster. Resultatet av genomförda penetrationstest kan även ge en indikation på kvaliteten av vidtagna säkerhetsåtgärder – hur väl säkerhetsarbetet fungerar. Med hjälp av sådana tester kan tillhandahållare ta reda på om verksamheten kan upptäcka, verifiera, larma, motstå och återhämta sig från angrepp och därmed upprätthålla säkerhet (tillgänglighet, riktighet, konfidentialitet och autenticitet) i nät och tjänster. Penetrationstester genomförs som ett eller flera intrångsförsök, oftast med flera olika angreppssätt. Utöver det som framgår av de föreslagna föreskrifterna kan dessutom tillhandahållare på eget initiativ välja att utföra ytterligare tester m.m. av vidtagna åtgärder.

6.5.2 Föreslagna ändringar och dess konsekvenser

PTS bedömer att bestämmelserna om övergripande säkerhetsarbete kan medföra vissa kostnader i de fall tillhandahållare inte har omfattats av bestämmelser om detta tidigare och i de fall vissa anpassningar för att säkerställa överensstämmelse med de föreslagna bestämmelserna behöver ske. Dessa kostnader redovisas i detta avsnitt. Konsekvenserna av bestämmelserna om att processer, rutiner och planer ska upprättas, dokumenteras och revideras vid behov, genomförda tester ska dokumenteras, att anställda och uppdragstagare har kunskap om och tillämpar de processer, rutiner och planer som de är berörda av, redovisas emellertid inte i detta avsnitt utan redovisas istället av respektive efterföljande krav i föreskrifterna.

Tillhandahållare av NI-ICS

För tillhandahållare av NI-ICS är de föreslagna bestämmelserna i 3 kap. om övergripande säkerhetsarbete nya. Tillhandahållare av NI-ICS är emellertid inte skyldiga att säkerställa att uppgifter som lagras för brottsbekämpande ändamål skyddas eftersom dessa inte omfattas av skyldigheten att lagra sådana uppgifter. Tillhandahållare av NI-ICS är inte heller skyldiga att säkerställa totalförsvarets behov av elektroniska kommunikationer vid höjd beredskap eller krig. Det övergripande säkerhetsarbetet för dessa aktörer omfattar således inte dessa delar.

Även om bestämmelserna om övergripande säkerhetsarbete är nya för tillhandahållare av NI-ICS bedömer PTS att dessa redan bedriver ett grundläggande långsiktigt, kontinuerligt och systematiskt säkerhetsarbete. PTS gör denna bedömning givet att dessa tillhandahållare behöver tillhandahålla konkurrenskraftiga och tillförlitliga tjänster på en annars redan väletablerad marknad. PTS bedömning är

att föreslagna bestämmelser därmed handlar om eventuella anpassningar av detta arbete.

PTS bedömer att de administrativa engångskostnaderna avser eventuella anpassningar av det övergripande säkerhetsarbetet för att efterleva bestämmelserna, eventuell revidering av dokumentationen över rollfördelningar och tillgängliggörandet av processer med mera för anställda (PTS bedömer att det är ett sätt att säkerställa att anställda och uppdragstagare har kunskap om och tillämpar processer, rutiner och planer). PTS uppskattar att eventuella anpassningar av det övergripande säkerhetsarbetet kostar 21 640 kronor, givet en tidsåtgång om 40 timmar och en lönekostnad om 541 kronor/timme.

PTS bedömer att kostnaden för eventuell revidering av dokumentationen över rollfördelningar uppgår till 2 164 kronor, givet en tidsåtgång om 4 timmar och en lönekostnad om 541 kronor/timme. PTS bedömer vidare att tillgängliggörandet av processer, rutiner och planer för anställda och uppdragstagare uppgår till en kostnad om 10 820 kronor, givet en tidsåtgång om 20 timmar och en lönekostnad om 541 kronor/timme.

De administrativa årliga kostnaderna skulle kunna bestå av årlig genomgång och uppdateringar av rollfördelningar samt årlig uppföljning och dokumentation av vidtagna åtgärder. PTS uppskattar att den administrativa årliga kostnaden uppgår till 35 165 kronor, givet en tidsåtgång om 65 timmar och en lönekostnad om 541 kronor/timme.

Kostnader som kan uppstå med anledning av de föreslagna allmänna råden till bestämmelserna om övergripande säkerhetsarbete skulle kunna bestå av inköp av åtkomst till ISO-27000-standard (ca 1 500 kronor/standard[31]), att ett visst antal anställda går en ISO-27000-kurs för att få kännedom om innebörden av ett ledningssystem för informationssäkerhet, och av kostnader för genomförande av penetrationstester i enlighet med det föreslagna allmänna rådet.

PTS uppskattar att kostnaden för att låta en anställd gå en introduktionsutbildning i ISO-27000 uppgår till 10 000 kronor.

PTS bedömning är att tillhandahållare av NI-ICS redan genomför penetrationstester, antingen i egen regi eller som en del av den molntjänst som anlitas för att tillhandahålla tjänsten. Större organisationer har ofta en egen organisation för detta med utpekade roller för att öva it-angrepp och it-försvar (s.k. *red teams* och *blue*

[31] Standard - Informationsteknik - Säkerhetstekniker - Ledningssystem för informationssäkerhet - Krav (ISO/IEC 27001:2013 med Cor 1:2014 and Cor 2:2015) SS-EN ISO/IEC 27001:2017 - Svenska institutet för standarder, SIS.

teams). För dessa tillhandahållare innebär det allmänna rådet om penetrationstester inga kostnader.

För en tillhandahållare som däremot inte använder penetrationstester idag medför det allmänna rådet konsekvenser. PTS uppskattar att ett kvalificerat, men begränsat, penetrationstest på hela eller delar av en viss tjänst (vilket även inkluderar planering, rapportering och rekommendation av säkerhetsåtgärder) tar mellan 40 och 160 timmar.

PTS bedömer att tillhandahållare i genomsnitt kan behöva genomföra två penetrationstester per år, där varje test tar 80 timmar. Det medför en administrativ årlig tidsåtgång om 160 timmar. PTS uppskattar att den administrativa årliga kostnaden för en tillhandahållare av NI-ICS som anlitar en konsult för att genomföra dessa penetrationstester uppgår till 192 000 kronor årligen, givet en konsultkostnad om 1200 kronor/timme. Om tillhandahållare har egen expertis på området kan tidsåtgången, och därmed kostnaden, uppskattas bli något lägre eftersom testerna kan utföras som en del av linjeverksamheten.

Övriga tillhandahållare

Övriga tillhandahållare, dvs. samtliga tillhandahållare förutom tillhandahållare av NI-ICS, omfattas redan av bestämmelserna i 3 kap. om övergripande säkerhetsarbete. Som ovan angetts motsvarar de föreslagna bestämmelserna 3 § PTSFS 1995:1, delvis 3 §, andra och fjärde styckena i allmänna råd till 3 § och första stycket i allmänna råd till 4 § PTSFS 2012:4, 3 § PTSFS 2014:1, samt 3 § PTSFS 2015:2, med vissa ändringar.

Följande ändringar föreslås i förhållande till nuvarande föreskrifter:

- Nättillhandahållare som behandlar uppgifter omfattas inte av PTSFS 2014:1, men omfattas av den nu föreslagna bestämmelsen. För dessa tillhandahållare är därmed bestämmelserna om övergripande säkerhetsarbete avseende skydd av behandlade uppgifter nytt. För att säkerställa att behandlade uppgifter skyddas är det enligt PTS av vikt att även dessa tillhandahållare fortsättningsvis omfattas av bestämmelserna.
- Bestämmelserna stadgar att säkerhetsarbetet ska bedrivas långsiktigt, kontinuerligt och systematiskt. Motsvarande krav finns i PTSFS 1995:1, PTSFS 2012:4, PTSFS 2014:1 och PTSFS 2015:2, men med ett nytt tillägg i allmänna råd om att standarder bör användas som ett stöd för att kunna bedriva ett långsiktigt, kontinuerligt och systematiskt säkerhetsarbete. I förhållande till PTSFS 1995:1 är kravet dessutom omformulerat från att idag stadga att i fredstid hålla en organisation för verksamheten vid höjd beredskap och i krig aktuell.

- Bestämmelserna stadgar att tillhandahållare ska ha en tydlig rollfördelning med särskilt utpekade ansvariga för arbetet och att rollfördelningen ska dokumenteras. Motsvarande krav finns i PTSFS 1995:1, PTSFS 2012:4, PTSFS 2014:1 och PTSFS 2015:2. Kravet utformas i enlighet med hur det är formulerat i PTSFS 2014:1. I förhållande till 1995:1 förtydligas det att rollfördelningen ska dokumenteras och kravet omformuleras från att idag stadga att en organisation för verksamheten ska hållas aktuell. I förhållande till PTSFS 2012:4 omformuleras kravet från allmänna råd om ansvarsbeskrivningar för personalens roller och ansvar samt att allt säkerhetsarbete som utförs bör kontrolleras, godkännas och följas upp av för detta ändamål särskilt utsedd personal inom organisationen (PTS bedömer att det är tillräckligt att föreskriften nu innehåller krav på att en dokumenterad rollfördelning ska finnas istället för detaljerade allmänna råd om hur rollfördelningen ska se ut). I förhållande till PTSFS 2015:2 förtydligas att rollfördelningen ska dokumenteras.
- Bestämmelserna stadgar att processer, rutiner och planer ska upprättas, dokumenteras och revideras vid behov. Motsvarande krav finns i PTSFS 2012:4, PTSFS 2014:1 och PTSFS 2015:2. I förhållande till PTSFS 1995:1 är kravet nytt. I förhållande till PTSFS 2014:1 och PTSFS 2015:2 är förtydligandet om revidering nytt.
- Bestämmelserna innehåller krav om att anställda och uppdragstagare ska ha kunskap om och tillämpa processer, rutiner och planer. Motsvarande krav finns i PTSFS 2012:4, PTSFS 2014:1 och PTSFS 2015:2. I förhållande till PTSFS 1995:1 är kravet nytt. I förhållande till PTSFS 2012:4 omformuleras kravet från allmänna råd om att personal som hanterar eller kommer i kontakt med uppgifter som lagras för brottsbekämpande ändamål regelbundet bör få utbildning och information om vikten av att skyddsnivån upprätthålls. I förhållande till PTSFS 2014:1 omformuleras kravet från att idag stadga att relevant utbildning ska finnas och allmänna råd om vad utbildningen bör innehålla. I förhållande till PTSFS 2015:2 förtydligas att tillhandahållare inte bara ska säkerställa att personalen har kunskap om utan även tillämpar de processer, rutiner och planer de berörs av.
- Bestämmelserna stadgar att åtgärder som vidtas ska dokumenteras och följas upp årligen och vid behov. Bestämmelserna motsvarar PTSFS 2012:4, PTSFS 2014:1 och PTSFS 2015:2 men med ett nytt tillägg i nya allmänna råd om att erfarenheter och resultat från tester m.m. bör användas samt att penetrationstester bör genomföras. I förhållande till PTSFS 2012:4 omformuleras kravet från allmänna råd om att åtgärderna ska dokumenteras och vidare tas allmänna råd om att dokumentation bör behandlas konfidentiellt bort (PTS bedömer att det är tillräckligt att kräva att

dokumentation ska ske men inte hur tillhandahållare väljer att hantera dokumentationen eller skydda eventuell känslig information).

Flera av de genomförda ändringarna är språkliga och redaktionella, där någon ändring av bestämmelsernas innebörd i sak inte är avsedd.

Beroende på hur respektive tillhandahållares övergripande säkerhetsarbete genomförs idag, kan dock bestämmelserna medföra behov av vissa mindre anpassningar. Bestämmelserna kan t.ex. medföra att ytterligare dokumentation av rollfördelning eller behov av anpassningar i tillhandahållares arbete med att dokumentera och följa upp vidtagna åtgärder årligen och vid behov.

PTS bedömer att tillhandahållare överlag bedriver ett grundläggande övergripande säkerhetsarbete som är i linje med de nu föreslagna bestämmelserna. Dock kan samtliga tillhandahållare behöva se över och anpassa sitt säkerhetsarbete för att det ska stå i överenskommelse med kravet, t.ex. kan nättillhandahållare eventuellt behöva utöka sitt övergripande säkerhetsarbete avseende skydd av behandlade uppgifter. PTS uppskattar att anpassningen av det befintliga säkerhetsarbetet kan medföra en administrativ engångskostnad om 16 230 kronor för stora tillhandahållare (givet en tidsåtgång om 30 timmar och en lönekostnad om 541 kronor/timme), 10 820 kronor för medelstora tillhandahållare (givet en tidsåtgång om 20 timmar och en lönekostnad om 541 kronor/timme), 5 410 kronor för små tillhandahållare (givet en tidsåtgång om 10 timmar och en lönekostnad om 541 kronor/timme) och 3 246 kronor för mikroföretag (givet en tidsåtgång om 6 timmar och en lönekostnad om 541 kronor/timme).

PTS bedömer att en årlig administrativ kostnad för tillhandahållare för att upprätthålla och vid behov revidera det övergripande säkerhetsarbetet kan uppgå till 35 165 kronor för stora tillhandahållare (givet en tidsåtgång om 65 timmar och en lönekostnad om 541 kronor/timme), 21 640 kronor för medelstora tillhandahållare (givet en tidsåtgång om 40 timmar och en lönekostnad om 541 kronor/timme), 10 820 kronor för små tillhandahållare (givet en tidsåtgång om 20 timmar och en lönekostnad om 541 kronor/timme) samt 5410 kronor för mikroföretag (givet en tidsåtgång om 10 timmar och en lönekostnad om 541 kronor/timme).

När det gäller kostnader som föranleds av föreslagna allmänna råd relaterade till krav på det övergripande säkerhetsarbetet är storleken på kostnaderna beroende av i vilken utsträckning tillhandahållare redan vidtar angivna eller motsvarande säkerhetsåtgärder idag.

Kostnader som kan uppstå med anledning av de föreslagna allmänna råden till kraven om det övergripande säkerhetsarbetet skulle kunna bestå av inköp av åtkomst till ISO-27000-standard (ca 1 500 kronor/standard), att ett visst antal

anställda går en ISO-27000-kurs för att få kännedom om innebörden av ett ledningssystem för informationssystem, samt av kostnader för genomförande av penetrationstester i enlighet med det föreslagna allmänna rådet.

PTS bedömer att det allmänna rådet kan medföra en engångskostnad när det gäller utbildning i ISO-27000-kurs. En introduktionsutbildning till ISO-27000 (t.ex. SS-ISO/IEC 27001 (säkerhetskrav), 27002 (riktlinjer) och 27003 (vägledning)) under två dagar för en stor tillhandahållare uppgår uppskattningsvis till 100 000 kronor givet tio deltagare, 40 000 kronor för en medelstor tillhandahållare givet fyra deltagare, 10 000 kronor för små respektive mikrotillhandahållare givet en deltagare.

När det gäller penetrationstester bedömer PTS att åtminstone större tillhandahållare i viss utsträckning använder penetrationstester som en del av sitt säkerhetsarbete. I det fall tillhandahållare behöver genomföra ytterligare penetrationstester per år än vad de genomför idag uppskattar PTS att den årliga kostnaden blir 192 000 kronor/år för stora tillhandahållare (givet att 2 ytterligare tester behöver genomföras à 80 timmar/test), 96 000 kronor/år för medelstora (givet att 2 ytterligare tester à 40 timmar/test behöver genomföras), 60 000 kronor för små tillhandahållare per år (givet att 2 ytterligare tester à 25 timmar/test per år behöver genomföras) samt 48 000 kronor/år för mikroföretag (givet att 2 ytterligare tester à 20 timmar/test behöver genomföras) och en konsultkostnad om 1 200 kronor/timme.

6.6 Identifiering och dokumentation av tillgångar, informationsbehandlingstillgångar, förbindelser och uppdragstagare

4 kap. 1 § i de förslagna föreskrifterna innehåller krav på att tillhandahållare ska identifiera och dokumentera alla sina tillgångar, informationsbehandlingstillgångar, förbindelser och uppdragstagare.

Bestämmelsen motsvarar 4 § första stycket PTSFS 2014:1 och 4 § PTSFS 2015:2 med språkliga och redaktionella ändringar samt ett antal materiella ändringar. De materiella ändringarna innebär att bestämmelsen nu anger vilka uppgifter om respektive informationsbehandlingstillgång som ska dokumenteras (utöver det nuvarande kravet som endast anger att informationsbehandlingstillgångarna ska dokumenteras) och att varje version av dokumentationen av informations-behandlingstillgångarna ska bevaras i fem år.

Den föreslagna bestämmelsen om identifiering och dokumentation av tillgångar, informationsbehandlingstillgångar, förbindelser och uppdragstagare omfattar samtliga tillhandahållare. För tillhandahållare av NI-ICS är bestämmelsen ny. För övriga tillhandahållare, som redan omfattas av nuvarande föreskrifter, är kraven avseende vilka uppgifter om respektive informationsbehandlingstillgång som ska dokumenteras

och att dokumentationen ska bevaras viss tid nya. Nättillhandahållare som behandlar uppgifter omfattas inte av PTSFS 2014:1, men omfattas av den föreslagna bestämmelsen. För dessa tillhandahållare är därmed dessutom kravet på dokumentation av informationsbehandlingstillgångar nytt.

6.6.1 Beskrivning av bestämmelsen

Att ha en aktuell och samlad bild över samtliga tillgångar, informationsbehandlingstillgångar, förbindelser och uppdragstagare är enligt PTS en förutsättning för att ha kontroll över verksamheten och fastställa vad som omfattas av säkerhetsarbetet. Identifieringen och dokumentationen är utgångspunkten för arbetet med riskanalyser och vidtagandet av säkerhetsåtgärder. Utan detta är det inte möjligt att genomföra en korrekt riskanalys eller avgöra vilka åtgärder som behöver vidtas för att hantera eventuella risker. Dokumentationen är även en viktig del för att kunna följa upp och kontrollera säkerhetsarbetet, t.ex. ta reda på vilka säkerhetsåtgärder som har vidtagits för en viss tillgång eller vilken uppdragstagare som har utfört ett visst uppdrag även sedan en viss tid förflutit. Om en tillgång, informationsbehandlingstillgång eller förbindelse inte identifieras och dokumenteras finns det en risk att denna faller utanför det systematiska säkerhetsarbetet och över tid löper risk att bli exponerad för t.ex. angrepp eller oförutsedda händelser som kan leda till säkerhets- eller integritetsincidenter. Om en uppdragstagare inte identifieras eller dokumenteras finns det en risk att tillhandahållare tappar översikten och kontrollen över vilka som har kontrakterats, och därmed vilken åtkomst till tillgångar och förbindelser som ges uppdragstagare och under vilka förutsättningar detta görs vilket kan leda till en säkerhets- eller integritetsincident.

Bestämmelsen innebär att tillhandahållare ska identifiera och dokumentera sina tillgångar, dvs. de funktioner som utgörs av en avgränsad del av ett kommunikationsnät eller en kommunikationstjänst och som är nödvändiga för att tillhandahålla ett sådant nät eller en sådan tjänst, samt som används för att sända, motta, bearbeta eller lagra information. De ska även identifiera och dokumentera sina informationsbehandlingstillgångar, dvs. de system, databaser och fysiska tillgångar som används för informationsbehandling. Begreppen tillgångar och informationsbehandlingstillgångar är delvis överlappande, se en mer utförlig beskrivning av begreppen i avsnitt 6.4. Vidare ska tillhandahållare identifiera och dokumentera sina förbindelser, dvs. de delar av kommunikationsnät mellan två tillgångar eller mellan en tillgång och en anslutning till ett kommunikationsnät. Slutligen ska tillhandahållare identifiera och dokumentera de uppdragstagare som har anlitats för att utföra installation, underhåll, felavhjälpning, drift eller liknande hantering av tillgångar, informationsbehandlingstillgångar och förbindelser.

I bestämmelsen anges vilka uppgifter som åtminstone ska dokumenteras för varje tillgång, informationsbehandlingstillgång och förbindelse respektive för varje uppdragstagare.

För tillgångar, informationsbehandlingstillgångar och förbindelser ska tillhandahållare åtminstone dokumentera en unik beteckning, funktion samt en hänvisning till aktuell riskanalys och tillverkare. Även dess geografiska placering ska dokumenteras, under förutsättning att en sådan finns. Vidare ska tillhandahållare avseende tillgångar dokumentera tillgångens klass enligt bestämmelserna om klassificering i de föreslagna föreskrifterna.

Att ge en tillgång, informationsbehandlingstillgång eller förbindelse en unik beteckning samt dokumentera dess funktion, geografiska placering och tillverkare är viktigt för att kunna få en överblick och spårbarhet av dem. Dokumentationen av dessa uppgifter kan t.ex. effektivisera genomförandet av riskanalyser om en tillhandahållare behöver hantera ett visst geografiskt begränsat hot eller om det visar sig att en viss tillverkares utrustning är behäftad med sårbarheter. Dokumentationen underlättar även för att kunna hitta till tillgångar som fysiskt har gått sönder och behöver repareras eller bytas ut. En dokumenterad hänvisning till tillgångens, informationsbehandlingstillgångens eller förbindelsen riskanalys är av vikt för att tillhandahållare på ett systematiskt sätt ska kunna kontrollera att analyser har genomförts samt att det i efterhand ska kunna kontrolleras vilka bedömningar som gjorts. Dokumentation av tillgångens klass är viktigt för att tillhandahållare ska veta vilka åtgärder som denne måste vidta för olika tillgångar enligt bestämmelserna om redundans och reservkraft. Detta bedöms även kunna underlätta avgörandet av vilka tillgångar som ska prioriteras vid störningar eller avbrott i nät och tjänster för att så många abonnenter som möjligt ska få tillbaka tillgången till sina tjänster.

För uppdragstagare ska tillhandahållare åtminstone dokumentera uppdragstagarens namn, organisationsnummer och kontaktuppgifter, samt en beskrivning av uppdraget. Det är av vikt för att få en överblick över vilka utomstående som ges åtkomst till tillgångar, informationsbehandlingstillgångar och förbindelser samt under vilka förutsättningar det sker.

Det ställs inga krav på vilken form som dokumentationen ska ha. Det är således upp till tillhandahållare att själva avgöra hur detta ska göras.

Dokumentationen av tillgångar, informationsbehandlingstillgångar, förbindelser och uppdragstagare ska hållas uppdaterad. Varje fastställd version ska bevaras i fem år från det att dokumentationen upprättats eller uppdaterats.

6.6.2 Föreslagna ändringar och dess konsekvenser

Tillhandahållare av NI-ICS

För NI-ICS är den föreslagna bestämmelsen om identifiering och närmare dokumentation av tillgångar, informationsbehandlingstillgångar, förbindelser och uppdragstagare ny. Dessa innehar/tillhandahåller i regel dock inte några förbindelser, inte i den bemärkelse som tillhandahållare av nät (nätägare) gör.

PTS bedömer att i stort sett samtliga NI-ICS redan har dokumentation av tillgångar, informationsbehandlingstillgångar och uppdragstagare, i den mån de har tillgångar, informationsbehandlingstillgångar samt uppdragstagare.

Administrativa engångskostnader kan bestå av genomförande av vissa anpassningar eller kompletteringar av dokumentationen för att efterleva kravet. I det fall en tillhandahållare av NI-ICS har 50 tillgångar och informationsbehandlingstillgångar samt 20 uppdragstagare och tillhandahållare behöver justera sin dokumentation i enlighet med föreslaget krav, uppskattar PTS att kravet kan medföra en tidsåtgång om totalt 35 timmar, givet att arbetet med att anpassa dokumentationen tar 30 minuter per tillgång, informationstillgång och uppdragstagare. Med en lönekostnad om 541 kronor/timme uppgår därmed den totala administrativa engångskostnaden till 18 935 kronor.

Administrativa årliga kostnader kan bestå av löpande (årlig) uppdateringar av dokumentationen över tillgångar, informationsbehandlingstillgångar och uppdragstagare vid förändringar i enlighet med förslaget krav. PTS uppskattar att den administrativa årliga kostnaden för att hålla dokumentationen över tillgångar, informationsbehandlingstillgångar och uppdragstagare uppgår till 8 115 kronor, givet en tidsåtgång om 15 timmar och en lönekostnad om 541 kronor/timme.

Kravet på att viss dokumentation ska bevaras i fem år kan medföra administrativa årliga kostnader för det fall leverantören i nuläget inte sparar denna information under så lång tid. PTS bedömer att det i snitt tar tre timmar per år att spara ned och bevara dokumentationen på valfritt sätt. Med en lönekostnad om 541 kronor/timme uppgår den totala administrativa årliga kostnaden för bevarande av dokumentationen till 1 623 kronor.

PTS bedömer att kravet inte medför några övriga kostnader.

Övriga tillhandahållare

Övriga tillhandahållare, dvs. samtliga tillhandahållare förutom tillhandahållare av NI-ICS, omfattas redan av bestämmelser om identifiering och dokumentation av tillgångar, informationsbehandlingstillgångar, förbindelser och uppdragstagare, med undantag för nättillhandahållare som inte omfattas av PTSFS 2014:1 (och därmed inte

krav avseende informationsbehandlingstillgångar). För att säkerställa att behandlade uppgifter skyddas, är det enligt PTS av vikt att även dessa tillhandahållare omfattas av bestämmelsen. Som ovan angetts motsvarar bestämmelsen 4 § första stycket PTSFS 2014:1 och 4 § PTSFS 2015:2 med vissa ändringar. Bestämmelsen är utformad i enlighet med formuleringen i PTSFS 2015:2 (med den redaktionella ändringen att två paragrafer har blivit en). I förhållande till PTSFS 2014:1 förtydligas det vilka uppgifter dokumentationen av informationsbehandlingstillgångarna åtminstone ska innehålla och att varje version av dokumentationen ska bevaras i fem år.

För nättillhandahållare medför det föreslagna kravet närmare dokumentation av eventuella informationsbehandlingstillgångar som de kan inneha. PTS bedömer att det föreslagna kravet kan föranleda en administrativ engångskostnad för stora tillhandahållare om 6 492 kronor (givet en tidsåtgång om 12 timmar och en lönekostnad om 541 kronor/timme), 4 328 kronor för medelstora tillhandahållare (givet en tidsåtgång om 8 timmar och en lönekostnad om 541 kronor/timme), 2 164 kronor för en liten tillhandahållare (givet en tidsåtgång om 4 timmar och en lönekostnad om 541 kronor/timme) och 1082 kronor för mikroföretag (givet en tidsåtgång om 2 timmar och en lönekostnad om 541 kronor/timme).

Vidare bedömer PTS att det föreslagna kravet medför att uppgifter om informationsbehandlingstillgångar behöver ses över och vid behov revideras. Det utgör en årlig administrativ kostnad som PTS uppskattar till 3 246 kronor givet en tidsåtgång om 6 timmar och en lönekostnad om 541 kronor/timme.

Kravet på att viss dokumentation ska bevaras i fem år kan medföra administrativa årliga kostnader i det fall leverantören i nuläget inte sparar denna information under en så lång tid. PTS bedömer att det i genomsnitt tar två timmar per år att spara ned dokumentationen på valfritt sätt. Med en lönekostnad om 541 kronor/timme uppgår den totala administrativa årliga kostnaden för bevarande av denna dokumentation till 1 082 kronor.

PTS bedömer att kravet inte innebär några övriga kostnader.

I övrigt föreslås följande språkliga och redaktionella ändringar av bestämmelserna. Någon ändring av bestämmelsernas innebörd är dock inte avsedd, varför PTS bedömer att dessa inte kommer att innebära några ekonomiska konsekvenser.

- Kravet om identifiering och dokumentation saknas i PTSFS 2012:4. I förhållande till den föreskriften är således bestämmelsen ny. De uppgifter en tillhandahållare kan vara skyldig att lagra för brottsbekämpande ändamål enligt 9 kap. 19 § nya LEK lagras emellertid i tillgångar som omfattas av definitionen av informationsbehandlingstillgångar. Informationsbehandlings-tillgångar ska identifieras och dokumenteras enligt PTSFS 2014:1. De

tillgångar som regleras i PTSFS 2014:1 omfattas därmed indirekt av krav på identifiering och dokumentation. Ändringen innebär därför inga konsekvenser.
- Det förtydligas att tillgångens eller förbindelsens geografiska placering ska dokumenteras under förutsättning att en sådan finns.
- Det förtydligas att identifiering ska göras före dokumentering.

6.7 Riskanalys

5 kap. i de förslagna föreskrifterna innehåller bestämmelser om riskanalyser. I sådana riskanalyser analyseras risken för att integritets- eller säkerhetsincidenter inträffar. Riskanalyser utgör ett viktigt underlag för att kunna besluta hur risker ska hanteras och vilka säkerhetsåtgärder som ska vidtas.

Bestämmelserna motsvarar första stycket i allmänna råd till 3 § och delvis 5 § PTSFS2012:4, 4 § andra stycket PTSFS 2014:1 samt 5 och 5 a §§ PTSFS 2015:2 med språkliga och redaktionella ändringar samt ett antal materiella ändringar. De materiella ändringarna innebär att riskanalyserna ska omfatta fler säkerhetsaspekter än idag, att det i vissa hänseende införs mer detaljerade krav kring vilka delar riskanalyserna består av och hur riskanalysarbetet ska bedrivas samt att omvärldsbevakning ska ske som en del i riskanalysarbetet.

De föreslagna bestämmelserna om riskanalyser omfattar samtliga tillhandahållare. För tillhandahållare av NI-ICS är bestämmelserna nya. För övriga tillhandahållare – som redan omfattas av de nuvarande föreskrifterna – är det endast de materiella ändringarna som är nyheter i sak. Nättillhandahållare som behandlar uppgifter omfattas inte av PTSFS 2014:1 men omfattas av de föreslagna bestämmelserna. För dessa tillhandahållare är därmed dessutom kravet på riskanalys av informations-behandlingstillgångar nytt.

6.7.1 Beskrivning av bestämmelserna

Vad som ska analyseras

Bestämmelserna i 5 kap. innebär att tillhandahållare ska analysera riskerna för att tillgångar, informationsbehandlingstillgångar och förbindelser – som tillhandahållare ska identifiera och dokumentera enligt 4 kap. 1 § – orsakar eller drabbas av säkerhets- eller integritetsincidenter.

Riskanalyser ska enligt 5 kap. 1 § göras för varje tillgång, informationsbehandlings-tillgång och förbindelse. I allmänna råd till 1 § förtydligas att tillhandahållare kan välja att kategorisera likvärdiga tillgångar, informationsbehandlingstillgångar och förbindelser i syfte att göra en gemensam riskanalys för en viss kategori så länge

detta innebär att samtliga tillgångar, informationsbehandlingstillgångar och förbindelser omfattas av en riskanalys. Det är emellertid av vikt att i det enskilda fallet beakta de eventuella unika förutsättningar och hot som kan föreligga.

När det gäller planerade förändringar ska dock tillhandahållare istället analysera risken för att förändringen kan påverka säkerheten i nät och tjänster.

Enligt PTS är riskanalyser en förutsättning för att kunna bedöma vilka tekniska och organisatoriska åtgärder tillhandahållare behöver vidta. Med hjälp av riskanalyser tydliggörs vilka hot som kan påverka tillhandahållares nät och tjänster samt på vilket sätt, hur ofta det skulle kunna inträffa och vilka konsekvenser som kan uppstå om det inträffar. Detta utgör sedan ett underlag för värdering av riskerna för dessa hot samt beslut hur riskerna ska hanteras och vilka åtgärder som ska vidtas. Riskanalysen ligger således till grund för och påverkar valet av säkerhetsåtgärder. Genom analyserna kan åtgärderna anpassas efter riskerna och det säkerställs därmed att så korrekta säkerhetsåtgärder som möjligt införs. På detta sätt säkerställs även att resurser koncentreras till områden där de gör mest nytta. Riskanalyser minskar därmed risken för att incidenter inträffar samt gör att tillhandahållare har en god beredskap att hantera och begränsa konsekvenserna av de incidenter som ändå inträffar.

När analyser ska göras

Riskanalyser av tillgångar, informationsbehandlingstillgångar och förbindelser ska enligt 5 kap. 2 § genomföras minst en gång per år. Utöver det ska riskanalyser genomföras i samband med att rapporteringspliktiga säkerhetsincidenter har inträffat och efter att tidigare okända hot som är relevanta för riskanalysen identifierats.

Riskanalyser ska dessutom genomföras inför planerade förändringar samt inför upphandling av tillgångar, informationsbehandlingstillgångar, förbindelser och uppdragstagare.

Hoten och förutsättningarna för verksamheten är under ständig förändring. Dessutom kan förändringar i samhället påverka beroendet av nät och tjänster och därmed de möjliga konsekvenserna i händelse av att ett hot förverkligas.

För att kunna upprätthålla en ändamålsenlig säkerhetsnivå över tid och anpassa säkerhetsåtgärderna allt eftersom behovet förändras behöver riskanalysarbetet bedrivas med kontinuitet samt kontrolleras och uppdateras regelbundet, vilket är bakgrunden till att tillhandahållare åtminstone årligen ska genomföra analyserna. Att riskanalyser ska genomföras i samband med att säkerhetsincidenter av betydande omfattning har inträffat syftar till att analysera om behovet av säkerhetsåtgärder är förändrat med anledning av det inträffade, så att liknande incidenter inte inträffar i

framtiden. Det kan t.ex. vara så att en incident gör att nya hot uppdagas eller att tidigare gjorda bedömningar behöver ses över. I en riskanalys kan det t.ex. ha gjorts en bedömning att det är helt osannolikt att ett visst hot skulle realiseras. Om det hotet trots allt inträffar behöver sannolikhetsbedömningen justeras eftersom hotet har inträffat och det kan inträffa igen. Det kan dessutom vara så att sannolikhets-bedömningen behöver justeras även i andra riskanalyser avseende liknande tillgångar, informationsbehandlingstillgångar eller förbindelser till följd av den förändrade hotbilden. Vidare kan hot, som tidigare inte varit kända för tillhandahållare, innebära att riskanalyser behöver genomföras. Av bestämmelsen framgår att information om sådana hot kan förmedlas av PTS. PTS ser att det kan finnas eller uppstå hot mot säkerheten som myndigheten – men inte nödvändigtvis tillhandahållare – får kännedom om. För att säkerställa att dessa hot beaktas av tillhandahållare anges därmed i bestämmelsen att även denna typ av okända hot ska analyseras. På vilket sätt sådan information förmedlas till tillhandahållare regleras inte utan får avgöras i det enskilda fallet.

Hur analyser ska göras

Enligt 5 kap. 3 § ska tillhandahållare identifiera och analysera relevanta hot mot respektive tillgång, informationsbehandlingstillgång och förbindelse. Riskanalyser inför planerade förändringar ska emellertid istället innefatta en identifiering och analys av relevanta hot mot säkerheten i tillgångar och förbindelser med anledning av den planerade förändringen.

Tillhandahållare ska således genom att identifiera och analysera hot, fastställa möjliga händelser som skulle kunna innebära att en säkerhets- eller integritetsincident inträffar och få insikt i hur, var och varför detta skulle kunna bli verklighet.

Fokus för analyserna är alltså risken för säkerhets- eller integritetsincidenter. Analyserna ska således inkludera perspektivet från dem som är beroende av näten och tjänsterna eller vars uppgifter behandlas, och inte t.ex. risker för tillhandahållares verksamhet i sig.

I 1 kap. 7 § nya LEK definieras integritetsincidenter som händelser som leder till oavsiktlig eller otillåten utplåning, förlust eller ändring eller otillåtet avslöjande av eller otillåten åtkomst till behandlade uppgifter. Säkerhetsincidenter definieras enligt samma bestämmelse som händelser med en faktisk negativ inverkan på tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos nät eller tjänster, hos lagrade, överförda eller behandlade uppgifter eller hos de närliggande tjänster som erbjuds genom eller är tillgängliga via dessa nät eller tjänster, eller på förmågan att motstå sådana händelser. Det förtydligas i 8 kap. 1 § nya LEK att åtgärder särskilt

ska vidtas för att förebygga och minimera incidenters påverkan på användare samt på andra nät och tjänster.

Hot kan ha många olika former. Hot kan vara både inom och utanför verksamhetens kontroll, ha ett naturligt eller mänskligt ursprung, vara oavsiktliga eller avsiktliga, samt komma inifrån organisationen eller utifrån.

I allmänna råd till 3 § anges att tillhandahållare åtminstone bör analysera organisatoriska, logiska och fysiska hot. Organisatoriska hot är t.ex. mänskliga misstag, bristfälliga processer, och personalbortfall. Fysiska hot är t.ex. ras, översvämning till följd av läckage från en huvudvattenledning, brist i vattenförsörjning, kabelbrott, stöld och strömavbrott. Logiska hot är t.ex. att en databas blir korrupt, konfigurationsfel, överbelastningsattacker, logiska intrång och kända svagheter i programvara eller i protokoll såsom *Border Gateway Protocol* (BGP).

Det anges vilka organisatoriska, logiska respektive fysiska hot som alltid bör analyseras. Flera av dessa hot motsvarar sådant som även anges i EU:s verktygslåda för 5G-säkerhet.[32] Uppräkningen motsvarar hot som är ständigt närvarande och kan få stor påverkan på nät, tjänster och uppgifter. Dessa hot utgör – efter en riskbedömning – nästan alltid en risk som tillhandahållare därmed behöver hantera, vilket följer av bestämmelserna om riskhantering och åtgärder efter riskbedömning. Dessa bestämmelser anger dock endast *att* åtgärder behöver vidtas och det måste därmed i varje enskilt fall bedömas *vilka* åtgärder som är motiverade att vidta för att hantera en viss risk. Tillhandahållares riskanalys ska då användas som grund för valet av åtgärd. Riskbedömningen ligger därmed till grund för beslut om säkerhetsåtgärder som tillförsäkrar att varje tillgång, informationsbehandlingstillgång och förbindelse – eller kategori av sådana – är skyddade på sätt som är anpassade efter omständigheterna i det enskilda fallet. Riskanalyserna kan även användas som grund för val av åtgärder enligt övriga bestämmelser i föreskriften.

Utöver dessa uppräknade hot – som alltså nästan alltid är att se som relevanta – krävs det att tillhandahållare gör en egen bedömning för att identifiera ytterligare relevanta hot. I detta ligger att tillhandahållare inte kan ignorera uppenbara hot mot säkerheten, som t.ex. hot som tidigare realiserats och lett till en incident för en viss tillgång, informationsbehandlingstillgång eller förbindelse. Andra hot som kan vara relevanta – och som även omnämns i EU:s verktygslåda för 5G-säkerhet – är risker vid utformning, uppbyggnad och drift av nätverk, låg säkerhetsnivå för produkter och tjänster samt risker kopplade till användningen av högriskleverantörer.[33]

[32] Se bl.a. s. 5 i Cybersecurity of 5G networks- EU Toolbox of risk mitigating measures
[33] Se bl.a. s. 5 i Cybersecurity of 5G networks- EU Toolbox of risk mitigating measures

I allmänna råd till 3 § anges vidare att riskanalyserna bör innehålla en beskrivning av hur tillgångarna, informationsbehandlingstillgångarna eller förbindelserna kan påverkas i samband med att identifierade hot realiseras och hur detta kan påverka nät och tjänster.

Utöver identifieringen av relevanta hot ska riskanalyserna omfatta en bedömning av konsekvenserna som skulle kunna uppstå om ett identifierat hot realiseras, dvs. en bedömning av skadorna som uppstår om hotet blir verklighet. Konsekvensbedömningar kan beskrivas t.ex. genom användningen av olika förutbestämda begrepp indelade i olika nivåer såsom ”försumbar”, ”lindrig”, ”måttlig”, ”allvarlig” och ”katastrofal”, som är enhetliga och jämförbara över tid.

Riskanalyserna ska även omfatta en bedömning av sannolikheten för att ett identifierat hot inträffar. Sannolikhetsbedömningar kan beskrivas t.ex. genom användningen av olika förutbestämda begrepp indelade i olika nivåer såsom ”mycket sällsynt”, ”tämligen sällsynt”, ”regelbundet” och ”ofta”, som är enhetliga och jämförbara över tid.

Utifrån konsekvens- och sannolikhetsbedömningarna ska riskanalysen sedan omfatta en sammanvägd bedömning, dvs. en bedömning av sannolikheten för att ett hot inträffar och konsekvensen det kan medföra om ett hot inträffar. I den sammanvägda bedömningen kalkylerar tillhandahållare riskvärden för de olika hoten, vilket därmed anger riskens storlek. Riskvärdena för olika hot kan beskrivas t.ex. genom användningen av olika förutbestämda begrepp indelade i olika nivåer såsom ”betydande” och ”lindrig” eller genom användning av olika risktal, som är enhetliga och jämförbara över tid.

Vid genomförandet av riskanalyser ska tillhandahållare enligt 5 kap. 4 § beakta erfarenheter från tidigare inträffade säkerhets- och integritetsincidenter, allmänt uppmärksammade säkerhets- och integritetsincidenter och aktuella omvärldsföreteelser som är relevanta för att upprätthålla säkerheten i tillhandahållna nät och tjänster.

Syftet är att säkerställa att tillhandahållare beaktar sådana händelser som potentiellt kan få en påverkan på upprätthållandet av säkerheten och integriteten hos nät, tjänster och uppgifter. Ett pågående omvärldbevakningsarbete är enligt PTS av stor vikt för att tillse att nya och aktuella hot identifieras och omhändertas i riskanalysarbetet. Det är även av vikt att beakta erfarenheter från inträffade incidenter. När en incident är hanterad och åtgärdad är det enligt PTS viktigt att organisationen snabbt identifierar och drar lärdomar från genomförda aktiviteter och handlingar samt att slutsatser gås igenom och tas hänsyn till. Om detta inte görs kommer mycket av kunskapen och erfarenheten från hanterade incidenter att försvinna och det finns en risk att samma incident kan inträffa igen.

Vid genomförande av riskanalyser ska tillhandahållare vidare tillämpa processer som utgår från etablerad standard på området. Exempel på etablerade standarder är SS-ISO/IEC 27005 *Riskhantering för informationssäkerhet*, SS-EN 33010 *Riskhantering – Metoder för riskbedömning*, SS-ISO 31000 *Riskhantering vägledning* samt SS-ISO/IEC 27036 del 1 – 3 *Informationssäkerhet vid leverantörsrelationer*.

Att tillhandahållare ska tillämpa processer som utgår från etablerad standard syftar till att ge tillhandahållare ett stöd i arbetet. Viktigt att poängtera är dock att etablerade standarder innehållsmässigt fokuserar på risker för tillhandahållares verksamhet i sig medan kraven i föreskriften istället fokuserar på risker utifrån ett användarperspektiv. Standarder är således ett stöd för själva arbetsprocessen med riskanalyser men innehållet behöver anpassas efter bestämmelserna i de föreslagna föreskrifterna för att säkerställa en korrekt efterlevnad.

Tillhandahållare ska även ha en plan för vid vilka tidpunkter och i vilka situationer de kommer att genomföra riskanalyser. Flera tidpunkter och situationer följer direkt av bestämmelsen. Enligt PTS är det av vikt att tillhandahållare har en plan för när riskanalyser ska göras och de närmare detaljerna kring detta arbete.

Av bestämmelserna om övergripande säkerhetsarbete i 3 kap. följer att processen och planen ska upprättas, dokumenteras och revideras vid behov samt att tillhandahållare ska säkerställa att de anställda och uppdragstagare som berörs av dem har kunskap om och tillämpar dem.

Tillhandahållare ska slutligen dokumentera genomförda riskanalyser vilket därmed även inkluderar de bedömningar som har gjorts. Kravet på dokumentation utgör en förutsättning för en systematisk uppföljning av säkerhetsarbetet och kontroll av vilka riskbedömningar som gjorts för olika delar av verksamheten.

6.7.2 Föreslagna ändringar och dess konsekvenser

Tillhandahållare av NI-ICS

För tillhandahållare av NI-ICS är de föreslagna bestämmelser om riskanalyser nya. I viss mån kan det emellertid antas att sådana tillhandahållare redan arbetar riskbaserat, i vart fall vad gäller större sådana tillhandahållare

PTS bedömer att de administrativa engångskostnaderna består av att tillhandahållare behöver upprätta en plan eller modell för hur riskanalyser ska genomföras. I den uppgiften ingår att välja metod för riskanalys. Riskanalyser ska också genomföras för samtliga tillgångar, informationsbehandlingstillgångar och förbindelser. Dessa engångskostnader omfattar även de delar av nästkommande bestämmelser, se vidare avsnitt 6.8, som avser beslut hur varje risk ska hanteras samt motivering och dokumentation av detta. Engångskostnaderna för genomförande av riskanalyserna

bedöms som större än de årliga kostnaderna, mot bakgrund av att många befintliga riskanalyser under kommande år kan kontrolleras och revideras utan att göras om från grunden. PTS uppskattar att de administrativa engångskostnaderna uppgår till 151 480 kronor, givet en tidsåtgång om 280 timmar och en lönekostnad om 541 kronor/timme.

PTS bedömer vidare att de administrativa årliga kostnaderna avser arbetet att årligen, samt vid de ytterligare situationer som framgår av bestämmelserna, genomföra riskanalyser. Det omfattar även de delar av nästkommande bestämmelser, se vidare avsnitt 6.8, som avser beslut om hur varje risk ska hanteras samt motivering och dokumentation av detta. PTS uppskattar tidsåtgången till totalt 128 timmar årligen. Med en lönekostnad om 541 kronor/timme uppgår de administrativa årliga kostnaderna till 69 248 kronor.

PTS bedömer att de övriga kostnaderna (årliga) som är förknippade med bestämmelserna är hänförliga till personalkostnader. Dessa kostnader kan utgöras av kostnader för eventuell utbildning för de som ska delta i arbetet med att genomföra riskanalyser. PTS uppskattar tidsåtgången för det till två heldagar (16 timmar) för två personer, beroende på verksamhetens art och omfattning, dvs. totalt 32 timmar. Med en lönekostnad om 541 kronor/timme innebär det att de övriga kostnaderna uppgår till 17 312 kronor.

Övriga tillhandahållare

Samtliga tillhandahållare förutom tillhandahållare av NI-ICS omfattas redan av bestämmelser om riskanalyser, med undantag för nättillhandahållare som inte omfattas av PTSFS 2014:1 (och därmed inte bestämmelserna om riskanalyser för informationsbehandlingstillgångar). För att säkerställa att behandlade uppgifter skyddas är det enligt PTS av vikt att även dessa tillhandahållare omfattas av bestämmelserna.

Som ovan angetts motsvarar de föreslagna bestämmelserna första stycket i allmänna råd till 3 § och delvis 5 § PTSFS 2012:4, 4 § andra stycket PTSFS 2014:1 samt 5 och 5 a §§ PTSFS 2015:2 med språkliga och redaktionella ändringar samt med de materiella ändringarna gällande riskanalysernas omfattning och hur riskanalyserna ska genomföras.

Bestämmelserna om riskanalyser har utformats med utgångspunkt i hur kraven är formulerade i PTSFS 2015:2 med tilläggen att riskanalyser ska göras för att säkerställa både säkerhet och integritet samt att omvärldsbevakning ska ske. I förhållande till PTSFS 2012:4 omformuleras kravet från allmänna råd om att genomföra riskanalyser. I förhållande till PTSFS 2012:4 och PTSFS 2014:1 förtydligas det dessutom vilka

moment som riskanalyserna åtminstone ska innehålla, när de ska göras, vilka hot som bör analyseras samt att en process och en plan för arbetet ska finnas.

Bestämmelserna innebär att tillhandahållare inom ramen för sitt riskanalysarbete behöver säkerställa att samtliga säkerhetsaspekter beaktas, dvs. att respektive tillgång, informationsbehandlingstillgång och förbindelse analyseras utifrån tillgänglighets-, autenticitets-, riktighets-, konfidentialitets- och integritetsperspektiv. Nättillhandahållare kan i tillägg till det behöva genomföra fler riskanalyser, i och med att bestämmelserna innebär att dessa behöver analysera även informations-behandlingstillgångar. Det innebär att riskanalyserna som tillhandahållare behöver göras utökas något i omfattning och i vissa fall i antal. PTS bedömning är dock att tillhandahållare i viss mån redan gör detta som en del av sitt ordinarie säkerhets-arbete, men bestämmelserna kan ändå innebära vissa konsekvenser.

PTS bedömer att de administrativa engångskostnaderna avser arbetet att revidera riskanalyser och processen för arbetet samt i förekommande fall genomförandet av nya riskanalyser. Det inkluderar även dokumentation av analyser och process. PTS uppskattar att dessa administrativa kostnader uppgår till 69 248 kronor för stora företag (givet en tidsåtgång om 128 timmar och en lönekostnad om 541 kronor), 34 624 kronor för medelstora företag (givet en tidsåtgång om 64 timmar och en lönekostnad om 541 kronor), 17 312 kronor för små företag (givet en tidsåtgång om 32 timmar och en lönekostnad om 541 kronor) samt 8 656 kronor för mikroföretag (givet en tidsåtgång om 16 timmar och en lönekostnad om 541 kronor).

PTS bedömer vidare att de administrativa årliga kostnaderna avser arbetet med att genomföra nya riskanalyser, revidering av befintliga analyser och i förekommande fall revidering av processen för arbetet. Det inkluderar även dokumentation av analyser och process. PTS uppskattar att dessa administrativa årliga kostnader uppgår till 17 312 kronor för stora företag (givet en tidsåtgång om 32 timmar och en lönekostnad om 541 kronor), 8 656 kronor för medelstora företag (givet en tidsåtgång om 16 timmar och en lönekostnad om 541 kronor), 4 328 kronor för små företag (givet en tidsåtgång om 8 timmar och en lönekostnad om 541 kronor) samt 2 164 kronor för mikroföretag (givet en tidsåtgång om 4 timmar och en lönekostnad om 541 kronor).

Kravet på att beakta omvärldsföreteelser i riskanalysen är en nyhet för alla tillhanda-hållare. PTS bedömning är att omvärldsbevakning i viss utsträckning förekommer inom de delar av tillhandahållarnas organisationer som ansvarar för riskanalysen. Dock kan kravet att inkludera erfarenheter från denna omvärldsbevakning i riskanalysarbetet innebära ett justerat arbetssätt som innebär konsekvenser.

PTS bedömer att den administrativa engångskostnaden avser arbetet med att revidera processen för riskanalysarbetet. PTS uppskattar att kostnaderna för detta uppgår till 34 624 kronor för stora företag (givet en tidsåtgång om 64 timmar och en

lönekostnad om 541 kronor), 17 312 kronor för medelstora företag (givet en tidsåtgång om 32 timmar och en lönekostnad om 541 kronor), 4 328 kronor för små företag (givet en tidsåtgång om 8 timmar och en lönekostnad om 541 kronor) samt 2 164 kronor för mikroföretag (givet en tidsåtgång om 4 timmar och en lönekostnad om 541 kronor).

PTS bedömer vidare att de administrativa årliga kostnaderna avser nät- och tjänstetillhandahållares arbete att omvärldsbevaka inom ramen för arbetet med specifika riskanalyser. PTS uppskattar att de administrativa årliga kostnaderna för detta uppgår till 138 496 kronor för stora företag (givet en tidsåtgång om 256 timmar och en lönekostnad om 541 kronor), 69 248 kronor för medelstora företag (givet en tidsåtgång om 128 timmar och en lönekostnad om 541 kronor), 34 624 kronor för små företag (givet en tidsåtgång om 64 timmar och en lönekostnad om 541 kronor) samt 17 312 kronor för mikroföretag (givet en tidsåtgång om 32 timmar och en lönekostnad om 541 kronor).

I övrigt föreslås följande språkliga och redaktionella ändringar av bestämmelserna om riskanalyser. Någon ändring av bestämmelserna innebörd är dock inte avsedd varför PTS bedömer att dessa inte kommer att innebära några ekonomiska konsekvenser.

- I förhållande till PTSFS 2012:4 omformuleras bestämmelserna från ett krav att analyserna ska göras ”för den egna verksamheten” till att de nu istället ska göras utifrån ”tillgångar, informationsbehandlingstillgångar och förbindelser”. PTS anser att samma sak avses.
- Nya allmänna råd införs som förtydligar – men vilket sedan tidigare varit underförstått – att det är möjligt att göra en gemensam riskanalys för likvärdiga tillgångar, informationsbehandlingstillgångar och förbindelser.
- Istället för att det i bestämmelsen anges vilka hot som alltid är relevanta anges det nu istället i allmänna råd till bestämmelserna.

6.8 Hantering av risker och åtgärder efter riskbedömning

6 kap. i de förslagna föreskrifterna innehåller bestämmelser om riskhantering och åtgärder efter riskbedömning. Bestämmelserna innebär att tillhandahållare ska – utifrån de riskbedömningar som gjorts i enlighet med 5 kap. – besluta hur riskerna ska hanteras. Därefter ska tillhandahållare vidta åtgärder för att hantera riskerna.

Bestämmelserna motsvarar delvis 3 och 5 §§ PTSFS 2012:4, 4 § tredje stycket, allmänna råd till 4 § och 8 § andra och tredje styckena PTSFS 2014:1 samt 9 – 12 §§ PTSFS 2015:2 med språkliga och redaktionella ändringar samt ett antal materiella ändringar. De materiella ändringarna innebär att åtgärder behöver vidtas för att säkerställa samtliga säkerhetsaspekter (inte bara driftsäkerhet respektive integritet). Det införs även krav på att tillhandahållare ska dokumentera beslut avseende

riskhantering. Dessutom införs det vid planerade förändringar krav på härdning och verifieringar av förändringar efter att de har genomförts.

De föreslagna bestämmelserna om riskhantering och åtgärder efter riskbedömning omfattar samtliga tillhandahållare. För tillhandahållare av NI-ICS är bestämmelserna nya. För övriga tillhandahållare – som redan omfattas av nuvarande föreskrifter – är det endast utökningen till samtliga säkerhetsaspekter samt tilläggen avseende dokumentationen av riskhantering, härdning och verifiering av förändringar som innebär en ändring i sak. Nättillhandahållare som behandlar uppgifter omfattas inte av PTSFS 2014:1 men omfattas av de föreslagna bestämmelserna. För dessa tillhandahållare är därmed dessutom kraven i förhållande till informations-behandlingstillgångar nya.

6.8.1 Beskrivning av bestämmelserna

Riskhantering

Enligt 6 kap. 1 § ska tillhandahållare utifrån riskbedömningarna som gjorts i enlighet med 5 kap. om riskanalyser besluta hur respektive risk ska hanteras. Tillhandahållare kan välja att acceptera, reducera eller undvika riskerna. I allmänna råd till 1 § anges att tillhandahållare alltid bör eftersträva att reducera risker framför att acceptera dem. Tillhandahållare bör endast acceptera risker om säkerheten i nät och tjänster i stort kan upprätthållas trots att hotet förverkligas eller incidenten inträffar.

Beslut om hur riskerna ska hanteras ska dokumenteras. Beslut om att acceptera en risk ska även motiveras. Att godta eller bibehålla en risk utan vidare åtgärder kräver således ett välgrundat beslut som syftar till att riskacceptans – precis som beslut att åtgärda risker – ska utgöra en aktiv och genomtänkt åtgärd.

Åtgärder efter riskbedömning

Enligt 6 kap. 2 § ska tillhandahållare vidta åtgärder för att hantera de risker som ska undvikas eller reduceras. Sådana förebyggande säkerhetsåtgärder syftar till att minska risken för att säkerhets- och integritetsincidenter inträffar samt begränsa konsekvenserna om dessa ändå skulle inträffa. Om förebyggande säkerhetsåtgärder inte skulle vidtas finns, enligt PTS, en risk att säkerhetsarbetet blir alltför reaktivt, dvs. genom att åtgärder endast vidtas efter det att en incident inträffat. Enligt PTS är det därför nödvändigt att säkerhetsarbetet bedrivs proaktivt, så att hot så långt som det är rimligt hanteras innan en säkerhets- eller integritetsincident realiserats.

Bestämmelsen anger *att* säkerhetsåtgärder ska vidtas när riskanalysen visar på risker som ska undvikas eller reduceras. *Vilka* säkerhetsåtgärder som är lämpliga att vidta anges dock inte. Risker i tillhandahållares verksamheter kan variera stort och enligt PTS är det därför inte motiverat att myndigheten i dessa fall anger vad som är

motiverade säkerhetsåtgärder att vidta. Istället anges endast vad som ska beaktas vid val av åtgärd.

Åtgärderna ska vidtas på en nivå som är anpassad till den risk som föreligger, med beaktande av tillgänglig teknik och kostnaderna för åtgärderna. En tillhandahållare är således inte skyldig att t.ex. vidta åtgärder som kostar oproportionerligt mycket. Detta gäller dock inte för sådana uppgifter som ska lagras för brottsbekämpande ändamål enligt 9 kap. 19 § nya LEK. Tillhandahållare ska för sådana uppgifter vidta åtgärder i enlighet med vad som väntas anges i den kommande förordningen till nya LEK (som motsvarar nuvarande 37 § förordning (2003:396) om elektronisk kommunikation). Den bestämmelsen lämnar inte något utrymme att bestämma säkerhetsnivån genom en avvägning mellan teknik, kostnader och risken för integritetsintrång. Istället måste åtgärder vidtas som säkerställer att uppgifterna skyddas.

I allmänna råd till 2 § anges att tillhandahållares åtgärder bör följa etablerad standard, normer, praxis och säkerhetsvägledningar. Syftet med det är att säkerställa att tillhandahållare vidtar adekvata åtgärder. Att följa sådana standarder m.m. är något som dessutom särskilt anges i EU:s verktygslåda för 5G-säkerhet som viktiga åtgärder.[34] Med etablerad standard, normer, praxis och säkerhetsvägledningar avses t.ex. sådana som är framtagna av ISO och organisationen GSM Association. GSM Association har tagit fram stöd inom flera olika områden bl.a. gällande skydd av signaleringstrafik (se t.ex. GSMA FS.11: *SS7 Monitoring*, GSMA FS.07: *SS7 filtering*, GSMA FS.19: *Diameter interconnect security* och GSMA IR.82: *Security SS7 implementation on SS7 network guidelines*) och skydd av röstbrevlådor (GSMA *Voicemail Security Guidelines*).

De åtgärder tillhandahållare behöver vidta för att hantera risker är av många olika slag. För att ge några exempel på åtgärder som kan behöva vidtas kan följande nämnas.

Åtgärder för att hantera risker för intrång, sabotage och yttre påverkan kan t.ex. vara installation av inbrottslarm, låsta dörrar och skyddsstaket samt upprättande av utrustning för intrångsdetektering och filtrering av oönskad trafik. Åtgärder för att hantera risker för miljörelaterade hot kan t.ex. vara att säkerställa att anläggningar nära områden som ofta drabbas av översvämningar, jordskred eller brand ges särskilt skydd eller placeras någon annanstans, samt att säkerställa att nya och befintliga anläggningar har erforderlig avfuktningsutrustning, ventilationssystem och utrustning med tillräcklig kylförmåga. Åtgärder för att hantera risker som identifierats

[34] Se s. 23 i Cybersecurity of 5G networks- EU Toolbox of risk mitigating measures, TM01 *Ensuring the application of baseline security requirements.*

vid riskanalys inför upphandling kan vara t.ex. byte av uppdragstagare eller tillverkare. Ytterligare relevanta åtgärder att vidta anges i EU:s verktygslåda för 5G-säkerhet.[35]

Det är enligt PTS inte möjligt att på förhand ange vilka åtgärder som är motiverade att vidta. Valet av åtgärd beror på vilken risk och vilka förutsättningar som gäller i det enskilda fallet. Ibland kan en viss åtgärd vara tillräcklig för att hantera en risk och ibland krävs flera åtgärder för att hantera samma risk.

Tillhandahållarnas bedömningar vid val av åtgärder ska enligt 6 kap. 3 § dokumenteras samt följas upp årligen och vid behov. I ett långsiktigt, kontinuerligt och systematiskt säkerhetsarbete är det enligt PTS en förutsättning att vidtagna åtgärder följs upp och att bedömningarna och valet av åtgärder utvärderas. Syftet är att säkerställa om adekvata åtgärder vidtagits eller om det finns ett behov av nya eller förbättrade säkerhetsåtgärder för att hantera en viss risk.

I tillägg till vad som ovan angetts måste, enligt 6 kap. 4 §, vissa åtgärder vidtas när det föreligger risker för att planerade förändringar kan orsaka rapporteringspliktiga säkerhetsincidenter.

Planerade förändringar i nät och tjänster är något som tillhandahållare genomför dagligen och är en förutsättning för att upprätthålla nätens och tjänsternas kvalitet och säkerhet. Fel i samband med sådana förändringar är dock enligt PTS erfarenhet en vanlig orsak till säkerhetsincidenter. Det kan t.ex. handla om mänskliga misstag, programvarufel eller att förändringen eller återställandet tar längre tid än planerat och inte klaras av under servicefönstret. Ett fel drabbar normalt en enskild tillhandahållare eller accessteknik men vissa enskilda fel kan orsaka omfattande säkerhetsincidenter om de t.ex. uppstår i kommunikationsnät med regional och nationell påverkan eller om det begränsar möjligheten till nödkommunikation. Dagens nät är dessutom mycket komplexa varför felavhjälpning kan vara komplicerat och generera följdfel. Det finns därför enligt PTS ett stort behov av att säkerställa att tillhandahållare arbetar förebyggande för att motverka dessa fel i största möjliga mån.

För att säkerställa att förändringar blir lyckade och inte orsakar säkerhetsincidenter ska tillhandahållare därför genomföra tester och härdning samt ta fram planer för att hantera eventuella säkerhetsincidenter genom att vid behov kunna återställa näten och tjänsterna till tidigare fungerande läge före förändringen.

Av bestämmelserna om övergripande säkerhetsarbete i 3 kap. följer att planerna ska upprättas, dokumenteras och revideras vid behov samt att tillhandahållare ska säkerställa att de anställda och uppdragstagare som berörs av dem har kunskap om och tillämpar dem.

[35] Se bl.a. s. 5 i Cybersecurity of 5G networks- EU Toolbox of risk mitigating measures

Härdning är ett moment som genomförs före driftsättning. Momentet innebär att ett it-system konfigureras utifrån dess bestämda funktion. I detta ingår bl.a. att det som inte behövs för tillgångens bestämda funktion tas bort, stängs av eller åtkomstbegränsas. Även ändring av t.ex. standardlösenord och justering av krypteringsparametrar ingår. Syftet är att minska antalet potentiella sårbarheter och attackvägar genom att begränsa en tillgångs funktionalitet till att endast kunna utföra det den är avsedd för och ingenting annat.

Tester ska utföras inför förändringen och efter förändringen ska tillhandahållare verifiera att förändringen inte påverkat säkerheten negativt. Att tester utförs innan ändringar genomförs i produktionsmiljö och börjar tillämpas är viktigt för att minska risken för säkerhetsincidenter. Det är dock minst lika viktigt att tester även utförs efter att ändringen är genomförd. Många planerade förändringar görs t.ex. manuellt och i många på varandra efterföljande steg vilket innebär att det finns en betydande risk att fel görs av misstag trots att den som utför ändringen både har övat och testat innan. Därför kan det vara motiverat att åtminstone identifiera kärnfunktioner och säkerställa att dessa fungerar även efter den aktuella ändringen är gjord. Det kan göras på flera sätt t.ex. genom att användarfall testas på nytt i produktionsmiljön eller att tillhandahållare kontrollerar med hjälp av loggar att kärnfunktioner fungerar.

Det ställs i bestämmelserna inte något krav på formen för härdningen, testerna eller återställandeplanerna, men dessa ska vara utformade så att de är anpassade efter förändringens art och omfattning. Det blir således tillhandahållares riskanalys för förändringen som avgör om härdning, test och återställandeplan behövs, samt hur omfattande dessa ska vara.

Tillhandahållare ska vid genomförande av planerade förändringar tillämpa en process för förändringshantering som utgår från etablerad standard på området. Exempel på etablerad standard är *Information Technology Infrastructure Library* (ITIL).

Av bestämmelserna om övergripande säkerhetsarbete i 3 kap. följer att processen ska upprättas, dokumenteras och revideras vid behov samt att tillhandahållare ska säkerställa att de anställda och uppdragstagare som berörs av den har kunskap om och tillämpar dem. Av bestämmelserna framgår även att testerna ska dokumenteras.

6.8.2 Föreslagna ändringar och dess konsekvenser

Tillhandahållare av NI-ICS

För tillhandahållare av NI-ICS är de föreslagna bestämmelserna om riskhantering och åtgärder efter riskbedömning i 6 kap. nya.

Riskhantering

Tillhandahållare ska besluta hur varje risk ska hanteras, samt motivera och dokumentera detta. Tidsåtgången för detta är inkluderat i uppskattningen av tidsåtgång för riskanalysarbetet, se avsnitt 6.7.2.

Åtgärder efter riskbedömning, förutom i samband med planerade förändringar

Tillhandahållare ska vidta de åtgärder som är nödvändiga för att hantera de risker som ska undvikas eller reduceras. Åtgärderna ska vidtas på en nivå som är anpassad till risken. I det ska tillhandahållare beakta den senaste tekniska utvecklingen. Detta innebär att tillhandahållare måste hålla sig uppdaterade om de tekniska lösningar som finns på marknaden då teknisk utveckling kan medföra att behovet av åtgärder förändras.

För tillhandahållare av NI-ICS, som till största delen är molnbaserade tjänstetillhandahållare som saknar fysisk infrastruktur, innebär åtgärdskraven i stort sett det som omfattas av ett grundläggande systematiskt säkerhetsarbete. Då kan frågan om kostnad formuleras som en fråga om vilken mognad dessa tillhandahållare har i sitt säkerhetsarbete. Storleken på dessa varierar från mindre aktörer som enbart tillhandahåller själva kommunikationstjänsten, till mycket stora aktörer på den globala tech-marknaden, som har en eller flera kommunikationstjänster som en mindre del av sin verksamhet. De större aktörerna kan i många fall anses vara ledande inom organisatoriskt och tekniskt it-säkerhetsarbete av den typ som avses här. Även om de mindre aktörerna inte har samma resurser att avvara för det organisatoriska säkerhetsarbetet som de stora aktörerna så är många av de tekniska säkerhetsåtgärderna något som hanteras av de etablerade molntjänstleverantörer som de mindre tillhandahållarna anlitar. Ansvaret för säkerheten kan dock inte avtalas bort vilket innebär att de som anlitar molntjänster för att tillhandahålla en tjänst måste försäkra sig om att leverantören av molntjänster håller en nivå på säkerheten som medger att tillhandahållare kan uppfylla alla krav, vilket innebär kostnader. En stor säkerhetsmässig utmaning för en mindre tillhandahållare som är helt molnbaserad kan även vara säker utveckling och underhåll av programvaran för tjänsten med tillhörande appar. Dessa tillhandahållare kan drabbas av andra säkerhetsproblem som t.ex. BGP-relaterade routingfel eller överbelastningsattacker, även om det är något som normalt hanteras av de större molnleverantörerna utan instruktioner från kunderna, dvs. de mindre tillhandahållare som använder molntjänsten.

Beroende på vilka hot som vid var tid föreligger och nivån av skydd tillhandahållare har idag, kan bestämmelserna innebära allt från små till mycket stora investeringar i säkerhetsåtgärder. PTS kan således inte kvantifiera eller uppskatta kostnaderna fullt ut mot bakgrund av att det inte är möjligt att i förväg veta vilka investeringar som respektive tillhandahållare kommer att behöva göra.

Särskilt om planerade förändringar

I likhet med diskussionen ovan, om aktörernas säkerhetsåtgärder, så bedömer PTS att de tillhandahållare som är stora globala organisationer redan har etablerade processer och rutiner för förändringsarbete, testning och härdning. För de mindre tillhandahållare som inte har ett etablerat förändringsarbete finns det särskilda risker för säkerheten vid t.ex. utveckling och uppdatering av mjukvara. Slarv, buggar eller bristfälliga återställningsrutiner kan orsaka både incidenter i form av störningar och avbrott samt förlust av skyddsvärda uppgifter som i sin tur medför stora kostnader för tillhandahållare. Att införa ett systematiskt förändringsarbete i syfte att minska riskerna med sådana situationer bör endast i undantagsfall innebära större årliga kostnader på sikt än vad situationerna i sig skulle ha orsakat tillhandahållare, men att arbeta enligt en etablerad förändringsprocess innebär ändå en tidsåtgång. PTS uppskattar att de administrativa årliga kostnaderna för detta uppgår till 17 312 kronor (givet en tidsåtgång om 32 timmar och en lönekostnad om 541 kronor). Inledningsvis kan ett införande av ett förändringsarbete innebära en engångskostnad i form av upprättande av planer och processer för arbetet, samt vissa övriga kostnader för utbildning av personal. PTS bedömer att denna administrativa engångskostnad uppgår till 6492 kronor, givet en tidsåtgång om 12 timmar och en lönekostnad/timme om 541 kronor. PTS bedömer att den övriga engångskostnaden för utbildning uppgår till 8 656 kronor, givet en utbildningsinsats om 4 timmar för fyra personer (dvs. sammanlagt 16 timmar) och en lönekostnad om 541 kronor/timme.

Övriga tillhandahållare

Övriga tillhandahållare, dvs. samtliga tillhandahållare förutom tillhandahållare av NI-ICS, omfattas redan av bestämmelser om riskhantering och åtgärder efter riskbedömning, med undantag för nättillhandahållare som inte omfattas av PTSFS 2014:1 (och därmed avseende informationsbehandlingstillgångar). För att säkerställa att behandlade uppgifter skyddas är det enligt PTS av vikt att även dessa tillhandahållare omfattas av bestämmelserna. Som ovan angetts motsvarar de föreslagna bestämmelserna delvis 3 och 5 §§ PTSFS 2012:4, 4 § tredje stycket, allmänna råd till 4 § och 8 § andra och tredje styckena PTSFS 2014:1 samt 9 – 12 §§ PTSFS 2015:2 med vissa språkliga och redaktionella ändringar samt med de materiella ändringarna att kravet nu omfattar samtliga säkerhetsaspekter, att det införs krav på dokumentation avseende riskhantering samt att det införs krav på härdning och verifiering av förändringar efter att de har genomförts.

Riskhantering

Tillhandahållare ska besluta hur varje risk ska hanteras, samt motivera och dokumentera detta. Tidsåtgången för detta är inkluderat i uppskattningen av tidsåtgång för riskanalysarbetet, se avsnitt 6.7.2

Åtgärder efter riskbedömning, förutom i samband med planerade förändringar

Det förändrade kravet på riskanalys innebär att tillhandahållarna behöver beakta fler säkerhetsaspekter (konfidentialitet, autenticitet och riktighet) utöver tillgänglighet. Tillhandahållare av nät kommer även behöva inkludera informationsbehandlings-tillgångar. Det innebär att fler säkerhetsåtgärder kommer att identifieras som lämpliga för att bemöta de risker som framkommit i riskanalysen. Bestämmelserna kan innebära allt från små till mycket stora investeringar i säkerhetsåtgärder. PTS kan således inte kvantifiera eller uppskatta kostnaderna fullt ut mot bakgrund av att det inte är möjligt att i förväg veta vilka investeringar som respektive tillhandahållare kommer att behöva göra.

Kravet ändras inte i sak och kommer därför inte innebära några ytterligare kostnader, förutom för den som tillhandahåller enbart nät som tidigare inte har behövt analysera riskerna för annat än tillgänglighet. Beroende på utfallet i riskanalysen kan tillhandahållarna behöva införa ytterligare åtgärder. Inte heller här går det att veta vilka åtgärder som kan vara nödvändiga, men PTS gör följande bedömning. Även om risken för bristande konfidentialitet ska analyseras för nätets tillgångar i stort, kommer föremålen för den utökade riskanalysen främst vara ett fåtal informations-behandlingstillgångar, där uppgifter om t.ex. slutanvändare kan finnas. I de fall en nättillhandahållare har sådana tillgångar överhuvudtaget, kommer det vara sådana som tidigare omfattats av säkerhetskrav som följer av EU:s dataskyddsförordning. PTS har inga uppgifter om, eller anledning att befara, att säkerhetsåtgärder skulle saknas för dessa tillhandahållares informationsbehandlingstillgångar i sådan utsträckning att bestämmelsen skulle medföra påtagligt ökade kostnader.

Särskilt om planerade förändringar

Bestämmelsen om förändringsarbete omfattar i det tidigare regelverket enbart driftsäkerhet, dvs. tillgänglighet. I den föreslagna bestämmelsen omfattas även konfidentialitet, riktighet och autenticitet, vilket kan innebära att förändringsarbetet behöver utökas så att risker förknippade med dessa säkerhetsaspekter analyseras inför förändringar.

När det gäller bestämmelsen om härdning så är det kravet nytt. För aktörer med någorlunda fungerande säkerhetsarbete finns redan härdning med som ett moment inför driftsättning. Den tillkommande kostnaden för kravet är därmed avhängigt hur väl tillhandahållare redan idag följer upp säkerheten i tillgångarna i samband med förändringar.

Bestämmelsen om verifiering innebär att en tillhandahållare på lämpligt sätt måste kontrollera att en tjänst eller funktion fungerar som avsett efter att en planerad förändring genomförts (funktionskontroll). Metoden kommer att variera beroende på

vilken typ av tjänst och planerad förändring det rör sig om. PTS bedömer att tillhandahållare redan idag genomför viss verifiering av tjänstens funktionalitet efter att förändringar gjorts, men anser ändå att bestämmelsen kan medföra kostnader.

Med tanke på att kravet om verifiering är formulerat som en del av förändrings-processen kommer större delen av momenten att utgöras av olika kontroller för att verifiera att tillgången fortfarande håller den förväntade säkerhetsnivån efter att förändringen genomförts. Denna utökning av förändringsarbetet, vilket även inkluderar framtagande av checklistor m.m. medför konsekvenser.

PTS bedömer att de administrativa engångskostnaderna avser revidering av förändringsprocessen för att inkludera de nya momenten enligt ovan. PTS uppskattar att de administrativa engångskostnaderna för detta uppgår till 43 280 kronor för stora företag (givet en tidsåtgång om 80 timmar och en lönekostnad om 541 kronor), 15 148 kronor för medelstora företag (givet en tidsåtgång om 28 timmar och en lönekostnad om 541 kronor), 7 574 kronor för små företag (givet en tidsåtgång om 14 timmar och en lönekostnad om 541 kronor) samt 3 787 kronor för mikroföretag (givet en tidsåtgång om 7 timmar och en lönekostnad om 541 kronor).

PTS bedömer vidare att de administrativa årliga kostnaderna avser det mer omfattande arbetet inför en planerad förändring, inklusive moment hänförliga till härdning och verifiering. PTS uppskattar att de administrativa årliga kostnaderna för detta uppgår till 69 248 kronor för stora företag (givet en tidsåtgång om 128 timmar och en lönekostnad om 541 kronor), 25 968 kronor för medelstora företag (givet en tidsåtgång om 48 timmar och en lönekostnad om 541 kronor), 12 984 kronor för små företag (givet en tidsåtgång om 24 timmar och en lönekostnad om 541 kronor) samt 6 492 kronor för mikroföretag (givet en tidsåtgång om 12 timmar och en lönekostnad om 541 kronor).

I övrigt föreslås följande språkliga och redaktionella ändringar av bestämmelserna om riskhantering och åtgärder efter riskbedömning. Någon ändring av bestämmelserna innebörd är dock inte avsedd varför PTS bedömer att dessa inte kommer att innebära några ekonomiska konsekvenser.

- I förhållande till nuvarande föreskrifter har bestämmelserna fått en ny struktur i syfte att underlätta förståelsen av regleringen.
- Det förtydligas att riskhantering – vilket tidigare varit underförstått – är ett eget moment som föregår beslut om åtgärder samt att risker endast bör accepteras om säkerheten kan upprätthållas.

6.9 Åtgärder avseende åtkomst och behörighet

7 kap. 1 § i de förslagna föreskrifterna innehåller en bestämmelse om åtgärder avseende åtkomst och behörighet. Bestämmelsen handlar om vem som har rätt att få åtkomst till nät, tjänster och uppgifter samt att förhindra att obehöriga får sådan åtkomst.

Bestämmelsen motsvarar tredje stycket i allmänna råd till 3 §, 4 §, andra, tredje och fjärde styckena i allmänna råd till 4 § samt delvis 5 § PTSFS 2012:4, 5, 6 och delvis 8 §§ andra och tredje styckena PTSFS 2014:1 samt 13 § PTSFS 2015:2 med språkliga och redaktionella ändringar samt en materiell ändring. Den materiella ändringen innebär att tillhandahållare ska ha system för hantering och kontroll av identiteter och behörigheter inte bara gällande åtkomst till behandlade uppgifter (som gäller enligt nuvarande föreskrifter) utan även gällande åtkomst till tillgångar.

Den föreslagna bestämmelsen om åtkomst och behörighet omfattar samtliga tillhandahållare. För tillhandahållare av NI-ICS är bestämmelsen ny. För övriga tillhandahållare, som redan omfattas av nuvarande föreskrifter, är det endast tillägget gällande system för hantering och kontroll av identiteter och behörigheter som innebär en ändring i sak. Nättillhandahållare som behandlar uppgifter omfattas dock inte av PTSFS 2014:1, men omfattas av den nu föreslagna bestämmelsen. För dessa tillhandahållare är därmed bestämmelsen om åtkomst till behandlade uppgifter i sin helhet ny.

6.9.1 Beskrivning av bestämmelserna

Enligt 7 kap. 1 § ska tillhandahållare medge åtkomst till tillgångar och behandlade uppgifter endast till den som tilldelas behörighet till dessa. Endast den som behöver det för att kunna utföra sina arbetsuppgifter får tilldelas behörighet. Kravet gällande behörigheter gäller såväl för uppdragstagare som för tillhandahållares egna anställda.

Bestämmelsen om åtkomst till behandlade uppgifter omfattar samtliga uppgifter som en tillhandahållare får eller ska behandla. Det inkluderar således även de uppgifter som tillhandahållare kan vara skyldiga att lagra för brottsbekämpande ändamål enligt 9 kap. 19 § nya LEK.

Tillhandahållare ska säkerställa att åtkomst endast ges till den som har upplysts om tystnadsplikten i de fall 9 kap. 31 och 32 §§ nya LEK är tillämpliga. Bestämmelserna om tystnadsplikt gäller samtliga tillhandahållare förutom tillhandahållare av NI-ICS.

I allmänna råd till 1 § anges dessutom att den som kommer i kontakt med behandlade uppgifter regelbundet bör få utbildning och information om när och hur behandlade uppgifter får hanteras, tecken på att en integritetsincident har inträffat och tänkbara konsekvenser av en inträffad integritetsincident för abonnenter och användare.

Det är enligt PTS viktigt att de som har behov av behandlade uppgifter i sitt arbete har upplysts om den tystnadsplikt som gäller och har tillräcklig kunskap om hur behandlade uppgifter får hanteras så att skyddet för sådana skyddsvärda uppgifter kan upprätthållas och incidenter förhindras, och i de fall de ändå inträffar, identifieras.

I allmänna råd till 1 § anges även att tilldelade behörigheter bör vara begränsade i tid och omfattning, särskilt för tillfälliga uppdragstagare. Tilldelade behörigheter bör därför tas bort (återkallas) efter utfört uppdrag. Syftet med att tillämpa en sådan strikt åtkomstkontroll är för att på ett adekvat sätt hantera risker som kan uppstå när t.ex. en uppdragstagare ansluten via fjärranslutning tillfälligt får åtkomst för att genomföra en felsökning eller en planerad ändring i ett system. Att vidta åtgärder för att minimera åtkomst för tillfälliga uppdragstagare, framför allt från högriskleverantörer, via fjärranslutning är något som dessutom särskilt anges i EU:s verktygslåda för 5G-säkerhet som viktiga åtgärder.

Bestämmelsen om åtgärder avseende åtkomst och behörighet syftar till att förhindra att obehöriga får åtkomst till nät, tjänster och uppgifter. Att kontrollera och begränsa vem (eller vad) som får åtkomst till vad är enligt PTS en förutsättning för att hantera risker för säkerhets- och integritetsincidenter. Att någon obehörig får åtkomst kan i sig utgöra en säkerhets- och integritetsincident. En obehörig kan även genom sitt agerande orsaka ytterligare säkerhets- eller integritetsincidenter, t.ex. genom skadegörelse.

Att säkerställa att åtkomst endast ges till den som är behörig gäller både inom den egna verksamheten och gentemot utomstående. Det innebär alltså att tillhandahållare ska säkerställa att anställda och uppdragstagares åtkomst och behörigheter begränsas till vad som är nödvändigt för att de ska kunna utföra sitt arbete, samt att när någon inte längre har ett behov av en viss tilldelad behörighet ska den behörigheten omedelbart återkallas. Det innebär även att utomstående helt hindras från att få åtkomst till tillgångar och behandlade uppgifter. På så sätt minskar risken för att t.ex. anställda och uppdragstagare får tillgång till sådant som de inte är behöriga att få åtkomst till, vilket i sig utgör en incident. Det minskar även risken för att en anställd med alltför omfattande rättigheter i ett system råkar genomföra en felaktig ändring som ett resultat av felklick, att tillgångar saboteras, eller att angripare får åtkomst till hela it-miljön genom att lyckas ta över en anställds konto vars behörighet inte har begränsats.

Bestämmelsen uppställer inga krav på *hur* bestämmelsen ska efterlevas, utan det är upp till tillhandahållare att själv avgöra vilka åtgärder som behövs för att säkerställa att bestämmelsen efterlevs.

Fysisk åtkomst kan begränsas exempelvis genom skalskydd, lås och olika tillträdes-/behörighetskontroller till anläggningar. Fysisk åtkomst till anläggningar med tillgångar

ska endast ges till dem som behöver det för sitt arbete. Logisk åtkomst kan hanteras och begränsas genom införande av diverse tekniska begränsningar på olika nivåer, t.ex. genom upprättandet av unika identiteter (användarkonton) med tilldelade anpassade behörigheter beroende av behörighetsbehov hos såväl anställda som uppdragstagare samt genom tillämpning av lämpliga autentiseringsförfaranden (identifiering och legitimering av legitima användare i system och tjänster).

Behörigheter kan vara knutna till enskilda anställda, enskilda uppdragstagare och grupper. Behörigheter kan även vara rollbaserade. Tillhandahållare kan använda sig av olika typer av behörigheter. Vissa behörigheter kan tilldelas samtliga användare i ett visst system. Andra behörigheter kan ges till en begränsad grupp av användare eller tilldelas först efter ansökan.

Bestämmelserna innebär vidare att tillhandahållare ska tillämpa en process för tilldelning, ändring och uppföljning av tilldelade behörigheter. En förutsättning för en sådan process är enligt PTS att man ska tillämpa principen om att det behövs fler än en person/roll för att besluta om behörigheter respektive för att tilldela, justera, återkalla behörigheter (*the segregation of duties principle)*. Det innebär t.ex. att säkerställa att den som begär en utökning av en behörighet inte också är den som ska godkänna en sådan begäran.

Av bestämmelserna om övergripande säkerhetsarbete i 3 kap. följer att processen ska upprättas, dokumenteras och revideras vid behov samt att tillhandahållare ska säkerställa att de anställda och uppdragstagare som berörs av den har kunskap om och tillämpar den.

Vidare innebär bestämmelsen att de behörigheter som tilldelas ska dokumenteras samt följas upp årligen och vid behov, t.ex. vid personal- eller organisations-förändringar. Dokumentation av tilldelade behörigheter utgör enligt PTS en förutsättning för ett systematisk och långsiktigt säkerhetsarbete. Det är även en förutsättning för uppföljning och kontroll av vilka behörigheter som tilldelats för olika delar av verksamheten.

Bestämmelserna reglerar inte vilken form som dokumentationen ska ha. Dokumentation av behörigheter kan således göras genom mer avancerade identitets- eller åtkomstsystem likväl som i en fysisk förteckning.

Slutligen innebär bestämmelserna att tillhandahållare även ska ha system för hantering och kontroll av identiteter och behörigheter. Sådana system säkerställer att åtkomst endast medges i enlighet med tilldelade behörigheter och omfattar bl.a. att unika identiteter skapas, behörigheter tilldelas administrativt, användare loggar in och enbart kan göra det som behörigheterna tillåter i systemet. En tillhandahållare kan uppfylla regleringen genom ett ensamt system eller med flera olika system som

samverkar kring hantering av identiteter, hantering av behörigheter, kontroll av inloggningsuppgifter och kontroll (*enforcement*) av behörigheterna.

6.9.2 Föreslagna ändringar och dess konsekvenser

Tillhandahållare av NI-ICS

För tillhandahållare av NI-ICS är de föreslagna bestämmelserna om åtgärder avseende åtkomst och behörighet i 7 kap. nya.

PTS bedömning är emellertid att tillhandahållare av NI-ICS redan har vidtagit åtgärder för att begränsa fysisk och logisk åtkomst till behandlade uppgifter och tillgångar.

I det fall tillhandahållare av NI-ICS behöver komplettera sina processer och rutiner avseende åtkomst- och behörighetshantering för att säkerställa överensstämmelse med föreskrivna krav uppskattar PTS att ett sådant arbete uppgår till ca 30 timmar. Med en lönekostnad om 541 kronor/timme medför arbetet en administrativ engångskostnad om 16 230 kronor.

De administrativa årliga kostnaderna för bestämmelserna avser fortsatta bedömningar av vilka behörigheter som ska tilldelas, samt ändringar och uppföljningar av tilldelade behörigheter och dokumentation av behörigheter enligt kravet. PTS bedömer att detta arbete utgör en årlig administrativ kostnad som uppgår till 27 050 kronor, givet en tidsåtgång om 50 timmar och en lönekostnad om 541 kronor/timme.

PTS bedömer att övriga engångskostnader som är förknippade med bestämmelserna är hänförliga till personalkostnader, främst kostnader för eventuell utbildning av personal avseende processer och rutiner för åtkomst och behörighet. I det fall tillhandahållare genomför en utbildning på 2 timmar per utbildningstillfälle med 5 medarbetare, två gånger medför det en total kostnad om 10 820 kronor (givet en tidsåtgång om 20 timmar och en lönekostnad om 541 kronor/timme).

Övriga tillhandahållare

Övriga tillhandahållare, dvs. samtliga tillhandahållare förutom tillhandahållare av NI-ICS, omfattas redan av bestämmelser om åtgärder avseende åtkomst och behörighet, med undantag för nättillhandahållare som inte omfattas av PTSFS 2014:1 (och därmed inte bestämmelserna avseende åtkomst och behörighet till behandlade uppgifter). För att säkerställa att behandlade uppgifter skyddas är det enligt PTS av vikt att även dessa tillhandahållare omfattas av bestämmelserna. Som ovan angetts motsvarar de föreslagna bestämmelserna tredje stycket i allmänna råd till 3 §, 4 §, andra, tredje och fjärde styckena i allmänna råd till 4 § samt delvis 5 § PTSFS 2012:4, 5, 6 och delvis 8 §§ andra och tredje styckena PTSFS 2014:1 samt 13 § PTSFS 2015:2

med språkliga och redaktionella ändringar samt med den materiella ändringen att det införs krav på system för hantering och kontroll av identiteter och behörigheter även gällande åtkomst till tillgångar.

När det gäller kostnader som föranleds av förslaget på bestämmelse är storleken på kostnaderna beroende på vilken nivå av skydd som tillhandahållarna har idag.

PTS bedömer att kravet på system för hantering av kontroll av identiteter och behörigheter inte föranleder några kostnader mot bakgrund av att samtliga tillhandahållare bedöms ha detta idag.

PTS bedömer däremot att bestämmelserna medför konsekvenser för nättillhandahållare, när det gäller åtkomst och behörighet till behandlade uppgifter. Dessa tillhandahållare kan behöva komplettera sina processer och rutiner avseende åtkomst- och behörighetshantering, liksom vid behov vidta lämpliga tekniska åtgärder för att säkerställa åtkomst och behörighet till dem som behöver det för att utföra sina uppgifter. PTS bedömer att de administrativa engångskostnaderna för detta uppgår till 8 656 kronor för stora företag (givet en tidsåtgång om 16 timmar och en lönekostnad om 541 kronor/timme), 4 328 kronor för medelstora företag (givet en tidsåtgång om 8 timmar och en lönekostnad om 541 kronor/timme), 2 164 kronor för små företag (givet en tidsåtgång om 4 timmar och en lönekostnad om 541 kronor/timme) samt 1 082 kronor för mikroföretag (givet en tidsåtgång om 2 timmar och en lönekostnad om 541 kronor/timme).

PTS bedömer att de administrativa årliga kostnaderna avser arbete med att gå igenom behörigheter och vid behov justera behörigheter (tilldelning, återkallelse, övriga justeringar i tid eller omfattning) och ev. årlig uppdatering av dokumentation enligt kravet. PTS bedömer att de administrativa årliga kostnaderna för detta uppgår till 8 656 kronor för stora företag (givet en tidsåtgång om 16 timmar och en lönekostnad om 541 kronor), 4 328 kronor för medelstora företag (givet en tidsåtgång om 8 timmar och en lönekostnad om 541 kronor), 2 164 kronor för små företag (givet en tidsåtgång om 4 timmar och en lönekostnad om 541 kronor) samt 1 082 kronor för mikroföretag (givet en tidsåtgång om 2 timmar och en lönekostnad om 541 kronor).

Utbildning av personal med anledning av de föreslagna bestämmelserna är en övrig årlig kostnad som kan uppstå. PTS uppskattar den till 21 640 kronor för stora företag (givet en tidsåtgång om 40 timmar och en lönekostnad om 541 kronor), 21 640 kronor för medelstora företag (givet en tidsåtgång om 40 timmar och en lönekostnad om 541 kronor), 1 082 kronor för små företag (givet en tidsåtgång om 2 timmar och en lönekostnad om 541 kronor), 271 kronor för mikroföretag (givet en tidsåtgång om 0,5 timmar och en lönekostnad om 541 kronor).

En ytterligare kostnad som skulle kunna uppstå är en investeringskostnad i form av licenser för programvara som PTS uppskattar till 60 000 kronor för stora företag och 30 000 kronor för medelstora företag med en avskrivningstid på 5 år. Givet avskrivningstiden på 5 år och en diskonteringsränta på 4,44 % ger det en årlig annuitetsberäknad kostnad för stora företag på 13 644 kronor/år och 6 822 kronor/år för medelstora företag.

I övrigt föreslås språkliga och redaktionella ändringar av bestämmelserna om åtgärder avseende åtkomst och behörighet. Utöver några mindre språkliga och redaktionella ändringar är det framför allt följande språkliga och redaktionella ändringar som görs. Någon ändring av bestämmelserna innebörd är dock inte avsedd varför PTS bedömer att dessa inte kommer att innebära några ekonomiska konsekvenser.

- I syfte att förtydliga bestämmelserna byts begreppet ”system för identitets- och åtkomsthantering” ut mot ”system för hantering och kontroll av identiteter och behörigheter”. Det senare begreppet är enligt PTS mer vedertaget och är lämpligare för att tydliggöra att det alltså handlar om system som inte bara avser administrativa delar (skapa unika identiteter och tilldela behörigheter) utan även inkluderar inloggningskontroll och kontroll (*enforcement*) av behörigheterna.
- Det förtydligas i nya allmänna råd – vilket tidigare varit underförstått – att behörigheter bör vara begränsade både i tid och omfattning.
- I förhållande till PTSFS 2012:4 omformuleras bestämmelserna från ett krav på att det ska finnas rutiner som säkerställer att endast personal med särskild behörighet har tillgång till uppgifterna och allmänna råd som anger vilka säkerhetsåtgärder som bör vidtas gentemot personalen. PTS bedömer att de föreslagna bestämmelserna uppnår samma sak i kombination med de bestämmelser som finns i säkerhetsskyddslagstiftningen om säkerhetsprövning av personal.

6.10 Säkerhetskopiering m.m.

8 kap. i de förslagna föreskrifterna innehåller bestämmelser om säkerhetskopiering m.m. Bestämmelserna handlar om att skydda uppgifter som varaktigt lagras och uppgifter som lagras för brottsbekämpande ändamål genom att säkerställa att uppgifterna på något sätt kopieras så att originalet kan återskapas om det t.ex. skadas eller försvinner.

Bestämmelserna motsvarar 7 § PTSFS 2012:4 och 8 § första stycket PTSFS 2014:1 med språkliga och redaktionella ändringar.

De föreslagna bestämmelserna om varaktigt lagrade uppgifter i 8 kap. omfattar samtliga tillhandahållare. De föreslagna bestämmelserna om uppgifter som lagras för brottsbekämpande ändamål omfattar samtliga tillhandahållare förutom tillhandahållare av NI-ICS (tillhandahållare av NI-ICS är inte skyldiga att lagra sådana uppgifter).

För tillhandahållare av NI-ICS är bestämmelserna om varaktigt lagrade uppgifter nya. För övriga tillhandahållare, som redan omfattas av nuvarande föreskrifter, innebär förslaget ingen ändring i sak. Nättillhandahållare som behandlar uppgifter, omfattas dock inte av PTSFS 2014:1, men omfattas av de föreslagna bestämmelserna. För dessa tillhandahållare är därmed bestämmelserna om varaktigt lagrade uppgifter nya.

6.10.1 Beskrivning av bestämmelserna

Enligt 8 kap. 1 § ska tillhandahållare vidta åtgärder för att säkerställa att behandlade uppgifter som varaktigt lagras skyddas mot oavsiktlig eller otillåten utplåning eller förlust. I allmänna råd till 1 § anges att det bör ske genom säkerhetskopiering och att återläsning av säkerhetskopior bör verifieras åtminstone årligen.

Uppgifter som inte omfattas av bestämmelserna, och som alltså inte är att anse som varaktigt lagrade, är t.ex. uppgifter som temporärt mellanlagras i samband med överföringen av kommunikationen (s.k. cachade uppgifter).

Bestämmelserna innebär vidare enligt 2 § att uppgifter som ska lagras för brottsbekämpande ändamål i enlighet med 9 kap. 19 § nya LEK ska skyddas mot oavsiktlig eller otillåten utplåning samt oavsiktlig förlust eller ändring genom lagring på minst två fysiskt åtskilda platser. Detsamma gäller loggen avseende åtkomst till uppgifter som ska lagras för brottsbekämpande ändamål (för en mer utförlig beskrivning av loggen se avsnitt 6.11).

I allmänna råd till 2 § förtydligas att lagring på minst två fysiskt åtskilda platser kan uppnås genom redundant lagring, säkerhetskopiering eller liknande.

Vidare stadgar 8 kap. 2 § att säkerhetskopiorna eller motsvarande ska omfattas av samma skydd och utplånas samtidigt som de uppgifter som lagras för brottsbekämpande ändamål.

Utplåning och förlust av de uppgifter som omfattas av bestämmelserna om säkerhetskopiering m.m. kan medföra skada för såväl tillhandahållare som berörda användare och abonnenter. Det är således enligt PTS av vikt att uppgifterna skyddas. Genom att säkerhetskopiera eller vidta motsvarande åtgärder kan uppgifter som på något sätt gått förlorade återställas.

PTS anser vidare att det i ett kontinuerligt, systematiskt och långsiktigt säkerhetsarbete är motiverat att åtminstone årligen, och därtill vid behov, verifiera att uppgifterna som säkerhetskopieras kan återskapas.

6.10.2 Föreslagna ändringar och dess konsekvenser

Tillhandahållare av NI-ICS

Tillhandahållare av NI-ICS omfattas av bestämmelsen om säkerhetskopiering för varaktigt lagrade uppgifter i 8 kap. 1 §. Dessa tillhandahållare omfattas dock inte av 2 § då dessa tillhandahållare inte omfattas av skyldigheten att skydda sådana uppgifter som regleras där enligt 8 kap. 5 § nya LEK.

PTS bedömer att tillhandahållare av NI-ICS, i sitt nyttjande av molnbaserad infrastruktur, redan har lagringslösningar som skyddar uppgifter mot utplåning på grund av fysiska hot och hårdvarufel. Att ha redundant lagring är däremot inte samma sak som säkerhetskopiering. Att skydda sig mot logiska hot, som t.ex. *ransomware*-angrepp (där uppgifterna krypteras av en utpressare) eller oavsiktliga raderingar, kräver att tillhandahållare har flera tidigare versioner av data sparade i form av säkerhetskopior. Även om det sannolikt inte saknas sådana lösningar idag hos dessa tillhandahållare så kan bestämmelsen innebära konsekvenser.

PTS bedömer att de administrativa engångskostnaderna avser upprättande eller revidering av rutiner samt av arbetet med upprättande av säkerhetskopiering. PTS uppskattar att de administrativa engångskostnaderna för detta uppgår till 12 984 kronor, givet en tidsåtgång om 24 timmar och en lönekostnad om 541 kronor. PTS bedömer vidare att de administrativa årliga kostnaderna avser löpande säkerhetskopiering och verifiering (återläsning). PTS uppskattar att de administrativa årliga kostnaderna för detta uppgår till 8 656 kronor, givet en tidsåtgång om 16 timmar och en lönekostnad om 541 kronor.

Övriga tillhandahållare

Övriga tillhandahållare, dvs. samtliga tillhandahållare förutom tillhandahållare av NI-ICS, omfattas redan av bestämmelser om säkerhetskopiering m.m., med undantag för nättillhandahållare som inte omfattas av PTSFS 2014:1 (och därmed inte bestämmelserna om säkerhetskopiering för varaktigt lagrade uppgifter). För att säkerställa att behandlade uppgifter skyddas är det enligt PTS av vikt att även dessa tillhandahållare omfattas av bestämmelserna. Som ovan angetts motsvarar de föreslagna bestämmelserna 7 § PTSFS 2012:4 och 8 § första stycket PTSFS 2014:1 med språkliga och redaktionella ändringar.

Utöver några mindre språkliga och redaktionella ändringar är det framför allt följande ändringar som görs.

- I förhållande till PTSFS 2014:1 omformuleras syftet med bestämmelsen från ”skydd mot oavsiktlig eller otillåten utplåning eller förlust” till ”skydd mot förlust och förvanskning”.
- I förhållande till PTSFS 2012:4 omformuleras bestämmelserna från ett krav om att säkerhetskopiering ska vidtas till att nu stadga att lagring ska ske på minst två fysiskt åtskilda platser. PTS anser att syftet med bestämmelsen ska behållas men att den tekniska utvecklingen har gjort att det inte längre är motiverat att endast kräva säkerhetskopiering utan skydd kan uppnås även genom andra tekniker. Genom den tekniska utvecklingen gällande redundant lagring är det heller inte längre motiverat att behålla det allmänna rådet till 7 § PTSFS 2012:4 om kontroll av säkerhetskopior. Någon ändring av bestämmelserna innebörd är dock inte avsedd varför PTS bedömer att dessa inte kommer att innebära några ekonomiska konsekvenser.

Som ovan angetts omfattas tillhandahållare av tjänster redan av bestämmelserna om säkerhetskopiering m.m. För dessa tillhandahållare tillkommer således inga kostnader. För nättillhandahållare är emellertid bestämmelserna nya. PTS bedömer att dessa tillhandahållare endast har ett fåtal tillgångar som träffas av denna regel. Sannolikt har dessa tillhandahållare någon form av arbete med säkerhetskopiering redan idag som kan behöva utökas något.

PTS bedömer att de administrativa engångskostnaderna avser upprättande eller revidering av rutiner samt av upprättande och eller anpassningar av säkerhetskopiering i enlighet med föreslaget krav. PTS uppskattar att de administrativa engångskostnaderna för detta uppgår till 17 312 kronor för stora företag (givet en tidsåtgång om 32 timmar och en lönekostnad om 541 kronor), 10 820 kronor för medelstora företag (givet en tidsåtgång om 20 timmar och en lönekostnad om 541 kronor), 5 410 kronor för små företag (givet en tidsåtgång om 10 timmar och en lönekostnad om 541 kronor) samt 1 082 kronor för mikroföretag (givet en tidsåtgång om 2 timmar och en lönekostnad om 541 kronor/timme).

PTS bedömer att de administrativa årliga kostnaderna avser löpande säkerhetskopiering och verifiering (återläsning). PTS uppskattar att de administrativa årliga kostnaderna för detta uppgår till 8 656 kronor för stora företag (givet en tidsåtgång om 16 timmar och en lönekostnad om 541 kronor), 4 328 kronor för medelstora företag (givet en tidsåtgång om 8 timmar och en lönekostnad om 541 kronor), 2 164 kronor för små företag (givet en tidsåtgång om 4 timmar och en lönekostnad om 541 kronor) samt 1 082 kronor för mikroföretag (givet en tidsåtgång om 2 timmar och en lönekostnad om 541 kronor/månad).

6.11 Loggning

9 kap. i de förslagna föreskrifterna innehåller bestämmelser om loggning. Bestämmelserna motsvarar 6 § första och andra styckena PTSFS 2012:4 samt 7 § PTSFS 2014:1 med språkliga och redaktionella ändringar samt ett antal materiella ändringar. De materiella ändringarna innebär att det införs ett nytt krav på att logga systemhändelser. Det införs även nya allmänna råd som anger att automatisk övervakning av loggar bör ske.

Loggning handlar om registrering av genomförda aktiviteter i tillhandahållares elektroniska kommunikationsnät och -tjänster inklusive system och tjänster för behandlade uppgifter i syfte att säkerhets- och integritetsincidenter ska upptäckas så tidigt som möjligt, och i vissa fall förhindras, samt kunna utredas. Loggar är viktiga för att kunna utreda vad som har inträffat efter en inträffad händelse. Självfallet ska krav enligt EU:s dataskyddsförordning efterlevas vid upprättande och genomförande av loggning och endast nödvändiga personuppgifter ska loggas. Enligt dataskydds-förordningens grundläggande principer vid personuppgiftsbehandling råder uppgifts-minimering samt lagringsminimering.

De föreslagna bestämmelserna om loggning omfattar samtliga tillhandahållare, förutom de delar som rör uppgifter som lagras för brottsbekämpande ändamål, som omfattar samtliga tillhandahållare förutom tillhandahållare av NI-ICS. För tillhanda-hållare av NI-ICS är de tillämpliga bestämmelserna nya. För övriga tillhandahållare, som redan omfattas av nuvarande föreskrifter, är det endast tilläggen gällande systemhändelser och automatisk övervakning som innebär en ändring i sak. Nättillhandahållare som behandlar uppgifter, omfattas dock inte av PTSFS 2014:1, men omfattas av de föreslagna bestämmelserna. För dessa tillhandahållare är därmed dessutom bestämmelserna avseende behandlade uppgifter nya.

6.11.1 Beskrivning av bestämmelserna

Med loggning avses ett regelbundet insamlande och bevarande av elektroniska spår som innehåller information om olika aktiviteter som sker i tillhandahållares nät och tjänster. Informationen dokumenteras elektroniskt, i t.ex. en databas, och blir därmed tillgänglig för läsning för behöriga.

Loggarna ger en översikt över normaltillståndet, vilket gör att avvikelser på så sätt kan upptäckas. Loggar kan även bidra till att identifiera en incidents karaktär och omfattning samt ger en tidslinje för det inträffade. Dessutom kan loggar användas för att ta reda på vem som har fått åtkomst till vilka tillgångar och informations-behandlingstillgångar och när. Kännedom om att sådan loggning sker kan även ha en preventiv effekt, vilket kan medföra att färre säkerhets- och integritetsincidenter inträffar. Loggarna är enligt PTS en förutsättning för att upptäcka, utreda och minska

konsekvenserna av incidenter. Annars skulle händelser kunna passera oupptäckta och det skulle inte vara möjligt att i efterhand utreda dem.

Enligt 9 kap. 1 § ska tillhandahållare logga all läsning, kopiering, ändring och utplåning av behandlade uppgifter samt åtkomst till de system där uppgifterna finns. Det innebär att loggningen således även ska omfatta systemadministrativ åtkomst till berörda system, till exempel datorer, servrar och nätelement.

Tillhandahållare ska vidare enligt 9 kap. 2 § logga systemhändelser relevanta för att kunna utreda säkerhetsincidenter. En systemhändelse kan röra allt från externa händelser med avseende på säkerheten eller integriteten såsom intrångsförsök eller faktiska intrång i olika tillgångar hos tillhandahållare samt överbelastningsattacker liksom uppgifter om att tjänster och tillgångar på det interna nätet håller på att bli otillgängliga eller otillåtna slagningar av behandlade uppgifter internt. Exempel på systemhändelser kan alltså handla om ”Otillåtet uppkopplingsförsök mot port 445 från IP-adress 192.168.1.23 stoppades” eller ”Slut på portar i telefonväxel” eller ”Minnet i routern utnyttjat till 90%!”.

I allmänna råd till 1 och 2 §§ anges att tillhandahållare bör tillämpa automatisk övervakning av loggar, i syfte att snabbt upptäcka onormala användarmönster, händelser eller serier av händelser. En sådan övervakning innebär således att tillhandahållare mer eller mindre i realtid kan övervaka loggar, vilket kompletterar den kontroll av loggar som också regleras i bestämmelsen. Övervakningen är enligt PTS motiverad för att hantera risken för säkerhets- och integritetsincidenter. Loggar avseende åtkomst till uppgifter som lagras för brottsbekämpande ändamål omfattas inte av det föreslagna allmänna rådet om automatisk övervakning.

Enligt 9 kap. 1 § ska, när det gäller loggar avseende behandlade uppgifter och åtkomst till system där uppgifterna finns, loggning ske på ett sådant sätt att det går att se vem som har vidtagit vilken åtgärd med vilka uppgifter och vid vilken tidpunkt. Vidare ska dessa loggar kontrolleras systematiskt och återkommande samt vid misstanke om att en integritetsincident har inträffat. Regelbunden uppföljning av loggarna utgör enligt PTS en viktig del i ett systematiskt, kontinuerligt och långsiktigt säkerhetsarbete. Avsaknad av systematisk och återkommande uppföljning förtar mycket av värdet av loggningen och minskar möjligheterna att upptäcka de integritetsincidenter som inträffar i verksamheten. Genomförda kontroller av loggar ska dokumenteras. Tillhandahållare ska ha rutiner för kontroll av loggarna. Av bestämmelserna om övergripande säkerhetsarbete i 3 kap. följer att rutinerna ska upprättas, dokumenteras och revideras vid behov samt att tillhandahållare ska säkerställa att de anställda och uppdragstagare som berörs av dem har kunskap om och tillämpar dem.

Bestämmelserna om loggar avseende behandlade uppgifter och åtkomst till system där uppgifterna finns omfattar samtliga uppgifter som en tillhandahållare får eller ska behandla. Det inkluderar således även de uppgifter som tillhandahållare kan vara skyldiga att lagra för brottsbekämpande ändamål enligt 9 kap. 19 § nya LEK. När det gäller sådana uppgifter ska tillhandahållare utöver vad som följer av tidigare delar av bestämmelserna även, enligt 9 kap. 3 §, säkerställa att den som har haft tillgång till uppgifterna inte ges tillgång till loggen avseende åtkomst till uppgifterna. Loggen kommer att innehålla känsliga uppgifter eftersom den innehåller information om vilka uppgifter som efterfrågats och lämnats ut för brottsbekämpande ändamål. PTS bedömer mot denna bakgrund att loggen kommer att innehålla uppgifter som är särskilt skyddsvärda bl.a. med hänsyn till skyddet av den personliga integriteten för de individer vars uppgifter kan komma att ingå i loggen. Tillhandahållare ska vidare, enligt 9 kap. 4 §, utöver övriga bestämmelser om kontroll av loggar, innan uppgifterna utplånas, utföra en systematisk kontroll av loggen avseende åtkomst till uppgifterna. Efter kontrollen, och i samband med att uppgifterna utplånas, ska även loggarna utplånas.

Av bestämmelserna om kryptering i 10 kap. följer att loggen avseende åtkomst till uppgifter som lagras för brottsbekämpande ändamål ska skyddas genom kryptering under lagring och överföring. Bestämmelsen stadgar att kryptering ska ske med en allmänt erkänd krypteringsmetod med tillräcklig nyckellängd och att krypterings-nycklar ska hanteras på ett säkert sätt.

Av bestämmelsen om säkerhetskopiering m.m. i 8 kap. följer att loggen avseende åtkomst till uppgifter som lagras för brottsbekämpande ändamål ska skyddas mot oavsiktlig eller otillåten utplåning, förlust och ändring.

6.11.2 Föreslagna ändringar och dess konsekvenser

Tillhandahållare av NI-ICS

För tillhandahållare av NI-ICS är de föreslagna bestämmelserna om loggning i 9 kap. nya. Dessa tillhandahållare omfattas dock inte av de delar av bestämmelserna som gäller skydd av uppgifter som lagras för brottsbekämpande ändamål då dessa tillhandahållare inte omfattas av skyldigheten att skydda sådana uppgifter enligt 8 kap. 5 § nya LEK.

PTS bedömer att de administrativa engångskostnaderna kan avse identifiering av vad som ska loggas, upprättande eller anpassningar av befintliga loggar (exempelvis av fler uppgifter eller system) samt upprättande eller anpassningar av sedan tidigare framtagna rutiner för kontroll, skydd och radering av loggar (*retention policy*) i de fall sådana rutiner saknas. PTS uppskattar att de administrativa engångskostnaderna för

detta uppgår till 54 100 kronor (givet en tidsåtgång om 100 timmar och en lönekostnad om 541 kronor/timme).

PTS bedömer vidare att de administrativa årliga kostnaderna avser att hålla dokumentationen relaterad till loggning uppdaterad samt att genomföra eventuella utökningar eller andra justeringar. PTS uppskattar att de administrativa årliga kostnaderna för detta uppgår till 32 460 kronor för NI-ICS (givet en tidsåtgång om 60 timmar och en lönekostnad om 541 kronor/timme.

PTS bedömer att de administrativa engångskostnaderna för det allmänna rådet avser upprättandet av automatisk övervakning av loggar och att detta uppgår till 32 460 kronor, givet en tidsåtgång om 60 timmar och en lönekostnad om 541 kronor/timme.

PTS bedömer vidare att de administrativa årliga kostnaderna för det allmänna rådet om automatisk övervakning av loggar kan bestå av att anpassa ev. larmnivåer, samt att utöka eller minska den automatiska övervakningen. PTS uppskattar att de administrativa årliga kostnaderna för detta uppgår till 27 050 kronor, givet en tidsåtgång om 50 timmar och en lönekostnad om 541 kronor.

PTS bedömer att de övriga kostnaderna kan bestå av anskaffning av programvara och maskinvara. Det finns många olika typer av logghanterings- och logganalys-tjänster som erbjuds på marknaden. Kostnaden för dessa grundar sig på olika affärsmodeller. Vissa leverantörer baserar licenskostnaden per mängd lagrade data/uppgifter, andra på antalet anslutna enheter. Prisuppgifter för detta lämnas på offertbasis från leverantörer varför PTS saknar denna uppgift.

Övriga tillhandahållare

Övriga tillhandahållare, dvs. samtliga tillhandahållare förutom tillhandahållare av NI-ICS, omfattas redan av bestämmelser om loggning, med undantag för nättillhanda-hållare som inte omfattas av PTSFS 2014:1 (och därmed inte bestämmelserna om loggar för behandlade uppgifter). För att säkerställa att behandlade uppgifter skyddas är det enligt PTS av vikt att även nättillhandahållare omfattas av bestämmelserna. Som ovan angetts motsvarar de föreslagna bestämmelserna 6 § första och andra styckena PTSFS 2012:4 samt 7 § PTSFS 2014:1 med vissa språkliga och redaktionella ändringar samt med de materiella ändringarna att det införs krav på loggning av systemhändelser och nya allmänna råd om att automatisk övervakning av loggar bör ske.

Loggning av systemhändelser

PTS bedömer att de administrativa engångskostnaderna avseende kravet på loggning av systemhändelser avser vilka uppgifter som ska loggas och hur loggning

ska göras. Vidare behöver tillhandahållare upprätta (dokumentera) rutiner för kontroll av loggar och radering av loggar (retention policy). PTS uppskattar att de administrativa engångskostnaderna för detta uppgår till 108 200 kronor för stora företag (givet en tidsåtgång om 200 timmar och en lönekostnad om 541 kronor), 64 920 kronor för medelstora företag (givet en tidsåtgång om 120 timmar och en lönekostnad om 541 kronor), 32 460 kronor för små företag (givet en tidsåtgång om 60 timmar och en lönekostnad om 541 kronor) samt 16 230 kronor för mikroföretag (givet en tidsåtgång om 30 timmar och en lönekostnad om 541 kronor).

PTS bedömer vidare att de administrativa årliga kostnaderna avseende kravet på loggning av systemhändelser avser drift och underhåll av loggningsfunktionerna. PTS uppskattar att de administrativa årliga kostnaderna för detta uppgår till 21 640 kronor för stora företag (givet en tidsåtgång om 40 timmar och en lönekostnad om 541 kronor), 8 115 kronor för medelstora företag (givet en tidsåtgång om 15 timmar och en lönekostnad om 541 kronor), 2 705 kronor för små företag (givet en tidsåtgång om 5 timmar och en lönekostnad om 541 kronor) samt 1 082 kronor för mikroföretag (givet en tidsåtgång om 2 timmar och en lönekostnad om 541 kronor).

Automatisk övervakning av loggar

PTS bedömer att de administrativa engångskostnaderna för det allmänna rådet avser upprättandet av automatisk övervakning av loggar för detta uppgår till 32 460 kronor för stora företag (givet en tidsåtgång om 60 timmar och en lönekostnad om 541 kronor/timme), 21 640 kronor för medelstora företag (givet en tidsåtgång om 40 timmar och en lönekostnad om 541 kronor/timme), 8 115 kronor för små företag (givet en tidsåtgång om 15 timmar och en lönekostnad om 541 kronor/timme) samt 5 410 kronor för mikroföretag (givet en tidsåtgång om 10 timmar och en lönekostnad om 541 kronor/timme).

PTS bedömer vidare att de administrativa årliga kostnaderna för den automatiska övervakningen av loggar kan bestå av att anpassa ev. larmnivåer samt att utöka eller minska den automatiska övervakningen. PTS uppskattar att de administrativa årliga kostnaderna för detta uppgår till 54 100 kronor för stora företag (givet en tidsåtgång om 100 timmar och en lönekostnad om 541 kronor), 43 280 kronor för medelstora företag (givet en tidsåtgång om 80 timmar och en lönekostnad om 541 kronor/timme), 32 460 kronor för små företag (givet en tidsåtgång om 60 timmar och en lönekostnad om 541 kronor/timme) samt 21 640 kronor för mikroföretag (givet en tidsåtgång om 40 timmar och en lönekostnad om 541 kronor/timme).

Nättillhandahållares loggning avseende behandlade uppgifter

PTS uppskattar att de administrativa engångskostnaderna för nättillhandahållare att införa (driftsätta, konfigurera) loggning avseende behandlade uppgifter uppgår till 135 250 kronor för stora företag (givet en tidsåtgång om 250 timmar och en lönekostnad om 541 kronor/timme), 54 100 kronor för medelstora företag (givet en tidsåtgång om 100 timmar och en lönekostnad om 541 kronor/timme), 27 050 kronor för små företag (givet en tidsåtgång om 50 timmar och en lönekostnad om 541 kronor/timme) samt 5 410 kronor för mikroföretag (givet en tidsåtgång om 10 timmar och en lönekostnad om 541 kronor/timme).

PTS bedömer att de administrativa årliga kostnaderna för nättillhandahållare som föranleds av kravet om loggar avseende behandlade uppgifter består av arbete avseende årlig genomgång och uppdatering av rutiner avseende loggning samt kontroller av loggar. PTS bedömer att de administrativa årliga kostnaderna för detta uppgår till 21 640 kronor för stora företag (givet en tidsåtgång om 40 timmar och en lönekostnad om 541 kronor), 8 115 kronor för medelstora företag (givet en tidsåtgång om 15 timmar och en lönekostnad om 541 kronor), 2 705 kronor för små företag (givet en tidsåtgång om 5 timmar och en lönekostnad om 541 kronor) samt 1 082 kronor för mikroföretag (givet en tidsåtgång om 2 timmar och en lönekostnad om 541 kronor).

Övrigt med anledning av kravet i sin helhet

Eventuella investeringskostnader kan bestå av kostnader för ytterligare programvara och maskinvara. Prisuppgifter för detta lämnas, i likhet med vad som tidigare sagts, på offertbasis från leverantörer varför PTS inte har denna uppgift.

PTS uppskattar att övriga engångskostnader för tillhandahållare avseende utbildning i nyheterna kring loggning uppgår till 21 640 kronor för stora företag (givet en tidsåtgång om 40 timmar och en lönekostnad om 541 kronor/timme), 16 230 kronor för medelstora företag (givet en tidsåtgång om 30 timmar och en lönekostnad om 541 kronor/timme), 10 820 kronor för små företag (givet en tidsåtgång om 20 timmar och en lönekostnad om 541 kronor/timme) samt 5 410 kronor för mikroföretag (givet en tidsåtgång om 10 timmar och en lönekostnad om 541 kronor/timme).

Språkliga och redaktionella ändringar

I övrigt föreslås framför allt en språklig och redaktionell ändring. I förhållande till PTSFS 2014:1 utgår andra meningen i 7 § andra stycket och det allmänna rådet till 7 § då PTS anser att detta är något som är underförstått i bestämmelsen. Det är inte avsikten att samtliga loggar alltid ska kontrolleras, utan det är upp till tillhandahållare att avgöra vad som kontrolleras och med vilken periodicitet. PTS anser att det är

tillräckligt att i bestämmelserna stadga att kontroller ska göras systematiskt och återkommande. Någon ändring av bestämmelserna innebörd med anledning av denna ändring är dock inte avsedd varför PTS bedömer att ändringen inte kommer att innebära några ekonomiska konsekvenser.

6.12 Kryptering

10 kap. i de förslagna föreskrifterna innehåller bestämmelser om kryptering. Kryptering handlar om att skydda information genom att göra den oläsbar (eller mycket svår att läsa) för obehöriga.

Bestämmelserna motsvarar 6 § tredje och fjärde styckena PTSFS 2012:4 samt 9 § PTSFS 2014:1 med ett antal materiella ändringar. De materiella ändringarna innebär att det inte längre är möjligt att rutinmässigt låta överföringar av behandlade uppgifter ske utan kryptering även om berörd abonnent eller användare har samtyckt till det. Undantag får göras i de fall risken för säkerheten i nät och tjänster och för behandlade uppgifter efter en riskanalys bedöms vara låg. Ändringarna innebär vidare att även uppgifter som lagras för brottsbekämpande ändamål ska skyddas genom kryptering vid överföring via internet. Det införs vidare ett nytt krav om att anslutningar för konfiguration och styrning av tillgångar ska krypteras.

De föreslagna bestämmelserna om kryptering omfattar samtliga tillhandahållare, förutom de delar som rör uppgifter som lagras för brottsbekämpande ändamål som inte omfattar tillhandahållare av NI-ICS. För tillhandahållare av NI-ICS är de tillämpliga bestämmelserna nya. För övriga tillhandahållare – som redan omfattas av nuvarande föreskrifter – är det endast de materiella ändringarna som innebär en ändring i sak. Nättillhandahållare som behandlar uppgifter omfattas inte av PTSFS 2014:1 men omfattas av de föreslagna bestämmelserna. För dessa tillhandahållare är därmed kravet på kryptering av behandlade uppgifter i sin helhet nytt.

6.12.1 Beskrivning av bestämmelserna

Enligt 10 kap. 1 § ska behandlade uppgifter som överförs via internet skyddas genom kryptering, om inte risken för säkerheten i nät och tjänster och för behandlade uppgifter efter en riskanalys bedöms vara låg.

Enligt det allmänna rådet till 10 kap. 1 § bör behovet av kryptering och vilken nivå av säkerhet som ska eftersträvas avgöras av riskanalysen. Vid bedömning av risken bör hänsyn tas till typ och mängd av uppgifter.

Koder, lösenord och sammanställningar av uppgifter som rör en användare eller abonnent bör krypteras vid överföring via internet.

Sådan överföring kan t.ex. ske när tillhandahållare skickar avtal och fakturor via e-post till abonnenter eller erbjuder abonnenter möjlighet att ta del av sådana dokument via en webbtjänst. Det kan även röra sig om åtkomst till abonnentuppgifter som ges till återförsäljare eller entreprenörer via system som tillhandahålls av tjänstetillhandahållare över internet.

Vidare ska tillhandahållare, enligt 10 kap. 2 §, genom kryptering skydda anslutningar för konfigurering och styrning av tillgångar via internet eller nät som andra än tillhandahållare har rådighet över. T.ex. kan det omfatta anslutningar avseende support från *second line*, konfigurationsändringar i en basstation eller uppgradering av programvaran i en router. Tillsammans med autentisering och behörighetskontroll minskar det risken för att konfigurationsfiler förvanskas eller att skyddsvärd information om nät, utrustning eller användare läcker ut.

Tillhandahållare ska även, enligt 10 kap. 3 §, genom kryptering skydda loggar avseende åtkomst till uppgifter som lagras för brottsbekämpande ändamål i enlighet med 9 kap. 19 § nya LEK under lagring och överföring.

Genom kryptering görs information mycket svårläslig för alla som inte ska kunna läsa den, vilket enligt PTS är nödvändigt när integritetskänsliga uppgifter kommuniceras över internet. Kryptering omvandlar information från klartext till krypterad text. Kryptotexten kan sedan skickas till mottagaren som dekrypterar den. Syftet med bestämmelserna är att förhindra otillåten åtkomst eller otillåtet avslöjande av behandlade uppgifter som överförs via internet.

Kryptering ska enligt 10 kap. 4 § ske med en allmänt erkänd krypteringsmetod med tillräcklig nyckellängd. Krypteringsnycklar ska hanteras på ett säkert sätt. Exempel på sådana metoder är SSL/TLS för åtkomst till webbtjänster och uppkoppling via en s.k. VPN-tunnel. Det sker en ständig utveckling inom området och den allmänna uppfattningen om säkerhetsnivån i en viss krypteringsmetod kan snabbt förändras allteftersom metoder för att kringgå krypteringen uppdagas. PTS anser därför att det inte är lämpligt att närmare specificera vilken krypteringsmetod eller nyckellängd som ska användas.

Tillhandahållare ska enligt 10 kap. 5 § ha rutiner för kryptering och hantering av krypteringsnycklar.

Av bestämmelserna om övergripande säkerhetsarbete i 3 kap. följer att rutinerna ska upprättas, dokumenteras och revideras vid behov samt att tillhandahållare ska säkerställa att de anställda och uppdragstagare som berörs av dessa har kunskap om och tillämpar dem.

6.12.2 Föreslagna ändringar och dess konsekvenser

Tillhandahållare av NI-ICS

För tillhandahållare av NI-ICS är de föreslagna bestämmelserna om kryptering i 10 kap. nya. Dessa tillhandahållare omfattas dock inte av de delar av bestämmelserna som endast gäller uppgifter som lagras för brottsbekämpande ändamål.

Generellt bedömer PTS att kryptering redan används av samtliga tillhandahållare av NI-ICS i någon form eftersom det är en naturlig del i många programvaror och kommunikations- och applikationsprotokoll. Att ha en dokumenterad policy för hur detta ska göras och ha rutiner för t.ex. förnyelse av servercertifikat kan dock i vissa fall behöva ses över för att säkerställa överensstämmelse med bestämmelserna. För de tillhandahållare som t.ex. fjärrstyr servrar eller annan utrustning via internet behöver dessa uppkopplingar vara krypterade vilket kan medföra viss kostnad för att konfigurera krypteringsfunktioner.

PTS bedömer att de administrativa engångskostnaderna avser upprättande av policy och rutiner, samt konfigurationsarbete. PTS uppskattar att de administrativa engångskostnaderna för detta uppgår till 4 328 kronor, givet en tidsåtgång om 8 timmar och en lönekostnad om 541 kronor/timme. PTS bedömer vidare att de administrativa årliga kostnaderna avser revidering av policy, samt nyskapande och förnyelse av certifikat m.m. PTS uppskattar att de administrativa årliga kostnaderna för detta uppgår till 8 656 kronor, givet en tidsåtgång om 16 timmar och en lönekostnad om 541 kronor/timme.

Övriga tillhandahållare

Övriga tillhandahållare, dvs. samtliga tillhandahållare förutom tillhandahållare av NI-ICS, omfattas redan av bestämmelser om kryptering, med undantag för nättillhandahållare som inte omfattas av PTSFS 2014:1 (och därmed inte bestämmelserna om kryptering för behandlade uppgifter). För att säkerställa att behandlade uppgifter skyddas är det enligt PTS av vikt att även nättillhandahållare omfattas av bestämmelserna. Som ovan angetts motsvarar de föreslagna bestämmelserna 6 § tredje och fjärde styckena PTSFS 2012:4 samt 9 § PTSFS 2014:1 med de materiella ändringarna att det inte längre är möjligt att med stöd av användarens medgivande låta enstaka överföringar av behandlade uppgifter ske utan kryptering. De materiella ändringarna innebär även att uppgifter som lagras för brottsbekämpande ändamål ska skyddas genom kryptering vid överföring via internet samt att det införs krav om att anslutningar för konfiguration och styrning av tillgångar ska krypteras. Enligt PTS erfarenhet är incidenter vanliga i samband med oskyddad e-post, t.ex. att bekräftelsebrev med uppgifter om abonnemang och andra uppgifter skickas till fel

person. Risken för den typen av incidenter minskas genom att ge tillgång till informationen på en webbsida med autentisering och krypterad överföring.

Tillhandahållare som tidigare förlitat sig på oskyddade metoder för att kommunicera uppgifter i t.ex. avtal kan behöva övergå till metoder som medger krypterad överföring och i övrigt anpassa kommunikationen med kunder så att kravet uppfylls. I den mån tillhandahållare överför uppgifter som lagras för brottsbekämpande ändamål utanför sitt eget nätverk behöver servrar konfigureras att använda kryptering. Nätelement som inte kan administreras över det egna nätverket behöver konfigureras att använda kryptering.

PTS bedömer att de administrativa engångskostnaderna avser etablering av krypteringspolicy, processer för t.ex. hantering av kryptonycklar samt själva införandet av krypteringsfunktioner. PTS uppskattar att de administrativa engångskostnaderna för detta uppgår till 69 248 kronor för stora företag (givet en tidsåtgång om 128 timmar och en lönekostnad om 541 kronor), 69 248 kronor för medelstora företag (givet en tidsåtgång om 128 timmar och en lönekostnad om 541 kronor), 34 624 kronor för små företag (givet en tidsåtgång om 64 timmar och en lönekostnad om 541 kronor) samt 34 624 kronor för mikroföretag (givet en tidsåtgång om 64 timmar och en lönekostnad om 541 kronor).

PTS bedömer vidare att de administrativa årliga kostnaderna avser bl.a. hantering och förnyelse av certifikat, installation av certifikat samt kryptokonfiguration på nya nätelement och servrar. PTS uppskattar att de administrativa årliga kostnaderna för detta uppgår till 34 624 kronor för stora företag (givet en tidsåtgång om 64 timmar och en lönekostnad om 541 kronor), 17 312 kronor för medelstora företag (givet en tidsåtgång om 32 timmar och en lönekostnad om 541 kronor), 8 656 kronor för små företag (givet en tidsåtgång om 16 timmar och en lönekostnad om 541 kronor) samt 4 328 kronor för mikroföretag (givet en tidsåtgång om 8 timmar och en lönekostnad om 541 kronor).

6.13 Redundans och reservkraftssystem

11 kap. 1–9 §§ i de förslagna föreskrifterna innehåller bestämmelser om redundans och reservkraftssystem. Bestämmelserna handlar om att tillhandahållare med hjälp av redundanta tillgångar, förbindelser och kritiska komponenter samt reservkraftssystem ska minska risken för säkerhetsincidenter, i form av störningar eller avbrott, till följd av att tillgångar eller förbindelser upphör att fungera eller att strömavbrott inträffar.

Bestämmelserna motsvarar 15–22 §§ PTSFS 2015:2 med ett antal språkliga och redaktionella ändringar samt en materiell ändring. Den nuvarande bestämmelsen i 22 § i PTSFS 2015:2 innebär att tillhandahållare, i syfte att säkerställa att mobila

tjänster och nät fungerar vid strömavbrott, under vissa förutsättningar får begränsa antalet frekvensband. Dessutom får tillhandahållare fördela kapacitet så att vissa tjänster prioriteras framför andra om de kvarvarande frekvensbanden inte ger tillräcklig kapacitet. Den materiella ändringen innebär att en del av nuvarande bestämmelse tas bort. Det ska inte längre vara möjligt att stänga av vissa tjänster under tidsperioden och tillhandahållare måste upprätthålla samtliga tjänster under strömavbrottet.

De föreslagna bestämmelserna om redundans och reservkraftssystem omfattar samtliga tillhandahållare. För tillhandahållare av NI-ICS är bestämmelserna nya. För övriga tillhandahållare, som redan omfattas av nuvarande föreskrifter, är det endast den materiella ändringen ovan som innebär en ändring i sak.

6.13.1 Beskrivning av bestämmelserna

Bestämmelserna innebär att tillhandahållare ska ha redundans för tillgångar och förbindelser samt ha reservkraftssystem.

Med redundans avses två eller flera, identiska eller olika, sätt att oberoende av varandra fylla samma funktion.

Med reservkraftssystem avses system som oberoende av extern elförsörjning genererar elektricitet vid fel i den externa elförsörjningen.

Vilka krav i bestämmelserna som ska tillämpas avseende redundans och reservkraftssystem beror på vilken klass en tillhandahållares respektive tillgångar tillhör och vilka nät eller tjänster denne tillhandahåller.

Klassificering av tillgångar

Enligt 11 kap. 1 och 2 §§ ska tillhandahållare klassificera sina respektive tillgångar. Klassificeringen ligger sedan till grund för vilka av de efterföljande bestämmelserna som ska tillämpas.

Bestämmelserna innehåller två olika klassificeringsmodeller. Anledningen till att det finns två olika modeller är för att anpassa dem efter de olika förutsättningar som nät och tjänster verkar under. Vilken modell som ska tillämpas beror på vilka nät eller tjänster en tillhandahållare erbjuder.

Den första klassificeringsmodellen, 11 kap. 1 §

Den första klassificeringsmodellen, som regleras i 11 kap. 1 §, gäller för tillgångar vars funktion är nödvändig för att tillhandahålla ett nät eller en tjänst som *inte* är en nummeroberoende interpersonell kommunikationstjänst. Modellen ska således tillämpas av samtliga tillhandahållare förutom tillhandahållare av NI-ICS.

Modellen avspeglar till viss del Sveriges demografi men även hur näten är uppbyggda och hur många aktiva anslutningar som typiskt sett betjänas av olika tillgångar.

Modellen baseras på antalet aktiva anslutningar en tillgång har, dvs. anslutningar som kopplas till ett nät eller en tjänst och som möjliggör omedelbar användning av tjänster. För en utförligare beskrivning av begreppet aktiva anslutningar se avsnitt 6.6.

Att modellen baseras på antalet aktiva anslutningar – till skillnad från den andra modellen som baseras på antalet användare (se nedan) – beror på att många tillhandahållare kan beräkna antalet aktiva anslutningar men inte nödvändigtvis antalet användare. Till exempel finns det tillhandahållare som inte har abonnenter och som således saknar kunskap om antalet användare. Dessa kan istället ha kunskap om det antal aktiva anslutningar som deras tillgångar betjänar.

Eftersom föreskriften endast gäller nät och tjänster som är allmänna så omfattas inte anslutningar inom ett nät eller tjänst som *inte* är allmänna, t.ex. användare bakom en företagsväxel om dessa användare endast är anslutna till detta slutna nät. Skulle användarna bakom företagsväxeln emellertid använda mobiltelefoner som ansluter till ett allmänt nät ska dessa räknas som separata aktiva anslutningar och klassificeras enligt klassificeringsmodellen.

Att antalet aktiva anslutningar ska beräknas utifrån hur många som *kan* omfattas av en störning eller ett avbrott till följd av att tillgången upphör att fungera normalt innebär inte att klassificeringen fluktuerar beroende på hur många som är uppkopplade vid ett enskilt tillfälle. Den ska istället göras utifrån det antal aktiva anslutningar som normalt sett är beroende av tillgången för en fungerande uppkoppling.

I allmänna råd till 1 § anges att antalet aktiva anslutningar i mobila accessnät bör beräknas som antalet samtidigt möjliga aktiva anslutningar till basstationen, dvs. det maximala antalet samtidiga anslutningar till respektive basstation där varje anslutning har tillgång till fungerande tjänster.

Modellen innebär att tillgångar ska klassificeras i någon av klasserna A till E. Kraven på redundans och reservkraftssystem i de föreslagna föreskrifterna gäller emellertid primärt tillgångar i klass A till D. För tillgångar i klass E kan endast bestämmelserna om reservkraftssystem avseende mobila nät och tjänster aktualiseras. I övrigt saknas krav för dessa tillgångar. Av bestämmelserna om identifiering och dokumentation av tillgångar, informationsbehandlingstillgångar, förbindelser och uppdragstagare följer dock att även tillgångar i klass E ska dokumenteras. Det gäller även om bestämmelserna om reservkraftssystem inte gäller för dessa. Syftet med bestämmelsen om dokumentation av sådana tillgångar är av vikt för att säkerställa att klassificering av samtliga tillgångar har skett.

Den andra klassificeringsmodellen, 11 kap. 2 §

Den andra klassificeringsmodellen, som regleras i 11 kap. 2 § gäller för tillgångar vars funktion är nödvändig för att tillhandahålla en nummeroberoende interpersonell kommunikationstjänst och som tillhandahållare utövar direkt kontroll över. Modellen ska således tillämpas av tillhandahållare av NI-ICS.

Modellen baseras på antalet användare – till skillnad mot antalet aktiva anslutningar – eftersom tillhandahållare av NI-ICS typiskt sett har god kunskap om antalet användare, vilket alltså inte nödvändigtvis är fallet för övriga tillhandahållare. Till detta kommer att de tillgångar en tillhandahållare av NI-ICS har typiskt sett är centralt placerade och inte utspridda i landet som andra tillhandahållares tillgångar behöver vara. Tillhandahållare av NI-ICS behöver inte sprida ut sina tillgångar eftersom de tillhandahåller sina tjänster via de nät och de internettjänster som tillgängliggörs av andra. Den första klassificeringsmodellen, som till viss del baseras på demografiska hänsyn, är därför inte lämplig att tillämpa på tillhandahållare av NI-ICS. Om användare av en NI-ICS drabbas av en störning eller ett avbrott så kommer omfattningen med andra ord att bero på vilken server eller databas som har drabbats och vilken information som finns där, inte på hur stort det geografiska området är.

Modellen innebär att tillgångar ska klassificeras i någon av klasserna A eller B. Kraven på redundans och reservkraftssystem i de föreslagna föreskrifterna gäller endast tillgångar i dessa två klasser. Det krävs emellertid även att tillgångarna ska vara sådana som tillhandahållare utövar direkt kontroll över för att bestämmelserna ska bli tillämpliga. Syftet är att enbart de tillgångar som används för att tillhandahålla en NI-ICS ska omfattas av bestämmelserna och inte de internettjänster och nätverk som den nummeroberoende tjänsten är beroende av.

Redundans av tillgångar

Enligt 11 kap. 3 – 5 §§ ska tillhandahållare ha redundans för sina tillgångar i klasserna A till D. Syftet med bestämmelserna är att minska beroendet av enskilda tillgångar och därmed uppnå en högre säkerhet avseende tillgänglighet av nät och tjänster. Kraven på redundans ställs högre ju högre klass en tillgång tillhör. Kraven är således proportionerligt utformade i förhållande till de konsekvenser som ett bortfall av en tillgång kan innebära för nät och tjänsters tillgänglighet.

För tillgångar i klasserna A och B ska, enligt 11 kap. 3 §, redundans säkras med redundanta tillgångar så att ett bortfall av en tillgång inte leder till en säkerhets-incident i form av störning eller avbrott. Emellertid är störningar eller avbrott som består i att sessioner avbryts men omedelbart återupptas tillåtna, t.ex. att ett telefonsamtal bryts vid övergången till en redundant tillgång men att abonnenten omedelbart ska kunna ringa upp igen.

Kraven på redundans för tillgångar i klasserna A och B gäller endast om det är tekniskt tillämpbart. Kravet gäller således inte tillgångar som t.ex. kontrollfunktioner för basstationer, lasrar, våglängdsmultiplexorer och regeneratorer. För dessa tillgångar är det inte tekniskt möjligt att ta fram en redundant lösning på så sätt som är avsett.

Vidare ska tillgångar i klass A och deras redundanta funktion placeras på geografiskt lämpligt skilda platser. Syftet är att förhindra att tillgångarna påverkas av samma incident, t.ex. en översvämning.

För tillgångar i klass C ska, enligt 11 kap. 4 §, redundans säkras genom redundanta tillgångar eller redundanta kritiska komponenter inom tillgången. Det innebär att en tillgång inte behöver vara dubblerad men behöver istället t.ex. ha dubbla eller fler linjekort, processorer, lagringsmedia eller kraftaggregat.

På samma sätt som gäller tillgångar i klass A och B så tillåts störningar eller avbrott i en tillgång i klass C om den består i att sessioner avbryts men omedelbart kan återupptas.

För tillgångar i klass D ska tillhandahållare, enligt 11 kap. 5 §, säkerställa att kritiska komponenter i dessa tillgångar inte upphör att fungera och på så sätt orsakar en störning eller ett avbrott som överstiger tolv timmar en vardag eller 18 timmar övrig tid. Detta kan uppnås genom att antingen ha redundanta kritiska komponenter eller genom att säkerställa att reservdelar finns och att en fältserviceorganisation kan ersätta trasiga komponenter inom föreskriven tid.

Redundans av förbindelser

Enligt 11 kap. 6 och 7 §§ ska tillhandahållare ha redundans för de förbindelser som binder samman tillgångarna. Syftet med bestämmelserna är att minska beroendet av enskilda förbindelser och därmed uppnå en högre säkerhet avseende tillgängligheten på nät och tjänster. Precis som gäller för redundans av tillgångar ställs kraven på förbindelser högre ju högre klass de tillgångar har, som förbindelsen förbinder.

För förbindelser inom och mellan klasserna A till C ska, enligt 11 kap. 6 §, redundans säkras med redundanta förbindelser så att ett bortfall av en förbindelse inte leder till en säkerhetsincident i form av störning eller avbrott. Precis som för redundans av tillgångar i klasserna A till C gäller emellertid att störningar eller avbrott som består i att sessioner avbryts men omedelbart återupptas är tillåtna.

Vidare ska redundanta förbindelser mellan tillgångar inom och mellan klasserna A och B vara geografiskt lämpligt separerade. Kravet gäller emellertid inte förbindelser

mellan tillgångar inom samma anläggning. Kravet gäller inte heller förbindelser mellan tillgångar i klass C och andra tillgångar i klasserna A till C.

Med förbindelser mellan tillgångar inom och mellan klasserna A och B avses förbindelser mellan A- och A-tillgångar, A- och B-tillgångar, B- och A-tillgångar, samt B- och B-tillgångar. För dessa förbindelser gäller således att de dels ska vara redundanta, dels att förbindelserna som är redundanta till varandra ska vara geografiskt separerade, förutom gällande förbindelser mellan tillgångar inom en och samma anläggning. En lämplig geografisk separation kan vara att placera förbindelserna tillräckligt långt ifrån varandra för att förhindra att de redundanta förbindelserna påverkas av samma risk, t.ex. att de inte grävs av vid ett och samma tillfälle eller påverkas av ett och samma jordskred.

För förbindelser mellan en tillgång i klass D och tillgångar i klasserna A till C ska tillhandahållare, enligt 11 kap. 7 §, säkerställa att dessa förbindelser inte upphör att fungera och på så sätt orsakar en störning eller ett avbrott som överstiger tolv timmar en vardag eller 18 timmar övrig tid. Detta kan uppnås genom att antingen ha redundanta förbindelser eller genom att säkerställa att reservdelar finns och att en fältserviceorganisation kan reparera förbindelserna inom föreskriven tid.

Reservkraftssystem avseende tillgångar i klasserna A till D

Enligt 11 kap. 8 § ska tillhandahållare säkerställa att fel i extern elförsörjning inte orsakar störningar eller avbrott. Med fel i extern elförsörjning avses enligt definitionerna inte bara avbrott utan även störningar, såsom strömspikar, i den externa elförsörjningen. Tillhandahållare ska säkerställa att sådana fel inte orsakar störningar eller avbrott genom att under viss angiven tid upprätthålla tillgångarnas funktion med hjälp av reservkraftssystem.

Tiden som tillgångarnas funktion ska kunna upprätthållas anges i bestämmelserna. Tiden är beroende av tillgångarnas klass och i vissa fall deras geografiska placering (tätort med fler än 8 000 invånare eller övrig plats). Kraven ställs högre ju högre klass som tillgångarna tillhör. Kraven är således proportionerligt utformade i förhållande till de konsekvenser som ett bortfall av en tillgång innebär för nät och tjänsters tillgänglighet.

Tiden som tillgångarnas funktion ska kunna upprätthållas räknas från det att felet i den externa elförsörjningen inträffade.

Fel som drabbar samma tillgång med mindre än fyra timmars mellanrum ska anses utgöra ett (1) fel. Att flera avbrott och störningar kan räknas som ett och samma fel innebär således att tillhandahållare inte behöver tillämpa bestämmelserna om reservkraftssystem för varje avbrott och störning utan för felet i stort.

Ett exempel är ett strömavbrott som drabbar en tillgång i klass A. Tillhandahållare är skyldiga att med hjälp av reservkraftssystem upprätthålla sådana tillgångars funktion under 24 timmar. Om strömavbrottet varar i 18 timmar och strömmen därefter återkommer en kort stund för att sedan försvinna igen så behöver tillhandahållare endast upprätthålla tillgångens funktion under sex ytterligare timmar, som alltså är den tid som återstår när 18 av 24 timmar har passerat.

Paragrafen uppställer inte något krav på vilken typ av reservkraftssystem som ska användas. Tillhandahållare får själva avgöra om det behövs t.ex. ett diesel-aggregat eller om det är lämpligare med batterier för att efterleva bestämmelsen

Vidare innebär bestämmelsen att tillhandahållare ska utföra två olika sorters tester av reservkraftssystem.

Det första testet är ett funktionstest, dvs. en kontroll av att reservkraftssystemen fungerar som de ska. Funktionstester ska genomföras minst varje kvartal för tillgångar i klasserna A till C och minst en gång per år för tillgångar i klass D.

Tillhandahållare får själv avgöra vilka tester som är lämpliga för att kontrollera att reservkraften fungerar. Exempel på test som kan genomföras är att tillhandahållare på distans kontrollerar att t.ex. en dieselgenerator startar.

Det andra testet av reservkraftssystemen ska göras minst årligen. Testet ska utföras genom att till tillgångar i klasserna A till C bryta den externa elförsörjningen eller på annat sätt simulera bortfall av den externa elförsörjningen för att därefter granska att reservkraftssystemet fungerar, t.ex. startar korrekt och genererar erforderlig el för att hålla igång tillgångarna.

Av bestämmelserna om övergripande säkerhetsarbete i 3 kap. följer att testerna ska dokumenteras.

Slutligen innebär bestämmelsen om reservkraftssystem avseende tillgångar att tillhandahållare ska tillämpa processer för hur de ska planera, inrätta, testa, underhålla och byta ut sina reservkraftssystem.

Av bestämmelserna om övergripande säkerhetsarbete i 3 kap. följer att processerna ska upprättas, dokumenteras och revideras vid behov samt att tillhandahållare ska säkerställa att de anställda och uppdragstagare som berörs av dem har kunskap om och tillämpar dem.

Reservkraftssystem avseende mobila nät och tjänster

Enligt 11 kap. 9 § ska tillhandahållare av mobila kommunikationsnät och mobila kommunikationstjänster, utöver vad som följer av 11 kap. 8 §, under viss angiven tid säkerställa att fel i extern elförsörjning inte orsakar störningar eller avbrott eller att

tjänsters täckningsområde minskar. Tillhandahållare ska säkerställa detta med hjälp av reservkraftssystem. I tätort med fler än 8 000 invånare gäller kravet under åtminstone en timme från det att felet inträffade. På övriga platser gäller kravet under åtminstone fyra timmar från det att felet inträffade.

För tillhandahållare av mobila kommunikationsnät och mobila kommunikationstjänster gäller således både bestämmelserna om reservkraftssystem avseende tillgångar i klasserna A till D och bestämmelserna om reservkraftssystem avseende mobila nät och tjänster. Det innebär t.ex. att för en mobilnätstillgång i klass E gäller bestämmelserna om reservkraftssystem avseende mobila nät och tjänster även om den inte omfattas av bestämmelserna om reservkraftssystem avseende tillgångar i klasserna A till D.

Precis som gäller enligt bestämmelserna om reservkraftssystem avseende tillgångar i klasserna A till D enligt 11 kap. 8 § så anses fel som drabbar samma tillgång med mindre än fyra timmars mellanrum som ett fel.

Syftet med bestämmelsen i 11 kap. 9 § är att säkerställa att fel i extern elförsörjning inte orsakar störningar eller avbrott i nät och tjänster eller att täckningsområdet minskar. Täckningsområde är det geografiska område där kommunikationstjänsterna erbjuds under normala driftsförhållanden. Det är således inte tillåtet att under den tid som anges i bestämmelsen minska det geografiska täckningsområdet för tjänsterna.

Av bestämmelsens andra stycke framgår dock att tillhandahållaren under felets varaktighet får, om det är nödvändigt för att upprätthålla kommunikationstjänster under den tid som anges i första stycket och under förutsättning att täckningsområdet bibehålls, minska tillgångarnas elförbrukning genom att begränsa antalet frekvensband som används för kommunikationstjänsterna. Tillhandahållaren behöver därmed inte upprätthålla full kapacitet för tjänsterna i dessa fall, förutsatt att reducering behövs för att minska basstationernas elförbrukning.

Vidare innebär bestämmelsen att tillhandahållare ska tillämpa processer för hur denne ska planera, inrätta, underhålla och byta ut sina reservkraftssystem.

Av bestämmelserna om övergripande säkerhetsarbete i 3 kap. följer att processerna ska upprättas, dokumenteras och revideras vid behov samt att tillhandahållare ska säkerställa att de anställda och uppdragstagare som berörs av dem har kunskap om och tillämpar dem.

6.13.2 Föreslagna ändringar och dess konsekvenser

Tillhandahållare av NI-ICS

För tillhandahållare av NI-ICS är de föreslagna bestämmelserna om redundans och reservkraftssystem i 11 kap. 1–9 §§ nya.

Klassificering

PTS bedömer att tillhandahållare av NI-ICS behöver utreda och definiera vilka tillgångar denne har och om de omfattas av bestämmelserna om redundans och reservkraftssystem, vilket PTS bedömer utgör de administrativa engångskostnaderna. PTS uppskattar att denna kostnad uppgår till 17 312 kronor, givet en tidsåtgång om 32 timmar och en lönekostnad om 541 kronor. PTS bedömer vidare att de administrativa årliga kostnaderna avser klassificering av nytillkomna tillgångar och revidering av tillgångars klass, exempelvis om en tillgång kan ha kommit att påverka fler användare än tidigare. PTS uppskattar att de administrativa årliga kostnaderna för detta uppgår till 17 312 kronor, givet en tidsåtgång om 32 timmar och en lönekostnad om 541 kronor/timme).

Bestämmelserna om redundans och reservkraftssystem

PTS bedömning är att de mindre tillhandahållarna av NI-ICS är molnbaserade. Det innebär att de dels inte har rådighet över de direkta tillgångarna, dels att de drar nytta av det faktum att den fysiska infrastrukturen, som utgör grunden hos de stora leverantörerna av molntjänster, är redundant till sin natur. De flesta, om inte alla, av de datacenter som används har reservkraft för en längre tid, ofta med ambitionen att inte ha elavbrott alls, så länge leveranser av bränsle eller annan lokal energi-produktion fungerar.

De stora tillhandahållarna nyttjar vanligen sin egen infrastruktur, eftersom NI-ICS ofta bara är en av flera tjänster. Den infrastrukturen är ofta liknande den för en moln-tjänsteleverantör, eller till och med samma i de fall som tillhandahållare även agerar molntjänsteleverantör.

PTS gör därför bedömningen att tillhandahållare av NI-ICS generellt redan uppfyller bestämmelserna om redundans och reservkraftssystem och att dessa bestämmelser därför inte medför några konsekvenser.

Övriga tillhandahållare

Övriga tillhandahållare, dvs. samtliga tillhandahållare förutom tillhandahållare av NI-ICS, omfattas redan av bestämmelser om redundans och reservkraftssystem.

Som ovan angetts motsvarar de föreslagna bestämmelserna 15–22 §§ PTSFS 2015:2 med ett antal språkliga och redaktionella ändringar samt en materiell ändring som innebär att tillhandahållare inte längre får prioritera vissa tjänster framför andra i situationer av begränsat antal frekvensband.

Ändringen innebär att bestämmelserna nu stadgar att tillhandahållare ska säkerställa att mobila tjänster och nät fungerar under minst en timme i tätort respektive fyra timmar på andra platser även vid strömavbrott. Det är alltså inte möjligt att stänga av vissa tjänster helt under strömavbrottet. Säkerställande av fungerande nät och tjänster kan dels uppnås genom att skapa ökad uthållighet genom att förstärka reservkraften (t.ex. inköp av fler batterier) dels genom förbrukningsdämpande åtgärder såsom minskning av antalet frekvensband, avstängning av kylning, eller minskning av tillgänglig bandbredd (kapacitet).

Anledningen till att bestämmelsen tas bort är för att det inte längre går att göra uppdelningen mellan olika tjänster på sätt som anges i bestämmelsen. Tekniken för mobila kommunikationstjänster har utvecklats i snabb takt mot den ip-baserade tekniken, även för samtal och meddelandetjänster. Nuvarande bestämmelse är anpassad för 2G och 3G. I takt med att 2G och 3G avvecklas används både höga och låga frekvenser till 4G och 5G som medger både tal, meddelanden och allmän datatrafik, eftersom allt transporteras som data. De senare teknologierna är också effektivare och medger högre kapacitet i form av fler samtidiga sessioner, jämfört med äldre teknik. Den nu föreslagna ändringen är en anpassning till 4G, 5G och kommande generationers mobilnät. Det kommer således inte längre vara möjligt eller lämpligt att skilja samtalstjänster, meddelandetjänster och datakommunikations-tjänster åt.

PTS bedömer att ändringen av bestämmelsen inte medför några konsekvenser.

I övrigt föreslås en språklig ändring av bestämmelserna. Det gäller ett undantag från bestämmelserna om redundans av tillgångar i klasserna A och B som gäller kontrollfunktioner för basstationer för vilka det inte är tekniskt möjligt att säkerställa redundans. Då det finns ytterligare funktioner där det inte är tekniskt möjligt att säkerställa redundans omformuleras bestämmelserna så att de inte gäller tillgångar om det inte är tekniskt tillämpbart. Någon ändring av bestämmelserna innebörd är dock inte avsedd varför PTS bedömer att dessa inte kommer att innebära några ekonomiska konsekvenser.

6.14 Ansökan om undantag

11. kap. 10–12 §§ i de förslagna föreskrifterna innehåller bestämmelser om ansökan om undantag från kraven om redundans och reservkraftssystem. Undantagsmöjlig-heten syftar till att säkerställa att tillhandahållare inte behöver vidta oproportionerliga

åtgärder till följd av dessa krav. Bestämmelsen motsvarar 23 § PTSFS 2015:2 med språkliga och redaktionella ändringar.

De föreslagna bestämmelserna om undantag omfattar samtliga tillhandahållare. För tillhandahållare av NI-ICS är bestämmelserna nya. För övriga tillhandahållare – som redan omfattas av nuvarande föreskrifter – innebär bestämmelserna ingen ändring i sak.

6.14.1 Beskrivning av bestämmelserna

Bestämmelserna innebär att tillhandahållare skriftligen kan ansöka till PTS om att myndigheten ska medge undantag från bestämmelserna om redundans och reservkraftssystem. PTS kan medge undantag i det enskilda fallet om bestämmelserna om redundans eller reservkraftssystem skulle få konsekvenser som är oproportionerliga i förhållande till de kostnader som är förenade med åtgärden, som är olämpliga med hänsyn till tillgänglig teknik, som är olämpliga med hänsyn till annan reglering eller som är oproportionerliga med hänsyn till att berörda tillgångar eller förbindelser omfattas av beslut om avveckling. Det krävs att tillhandahållare vidtar lämpliga alternativa åtgärder när sådana finns.

Tillhandahållare ska när undantag medges vidta åtgärder för att begränsa negativa effekter av att den föreskrivna åtgärden inte vidtas.

Tillhandahållare ska i ansökan ange vilka åtgärdskrav ansökan avser, varför åtgärden är oproportionerlig eller olämplig, redovisa vilka alternativa och begränsande åtgärder som ska vidtas samt göra en bedömning av hur säkerheten i nät och tjänster påverkas av att föreskrivna åtgärder avseende redundans och reservkraftssystem inte vidtas. Utan att ange den här informationen föreligger inte tillräckliga underlag för PTS för att bedöma om undantag kan medges eller inte.

Syftet med bestämmelserna är således att lätta upp krav om redundans och reservkraft i de fall som åtgärderna skulle vara tekniskt mycket svårgenomförliga eller omöjliga eller om kostnaden framstår som orimlig i förhållande till nyttan. PTS bedömer att krav på redundans och reservkraftssystem medför betydande merkostnader för tillhandahållare. Fördelningen av enskilda krav inom och mellan olika kategorier av tillhandahållare uppvisar också stora variationer. Det finns således situationer där PTS bedömer att kostnaderna för att uppfylla bestämmelserna för en viss tillgång eller förbindelse inte står i proportion till den ökade säkerheten. I dessa situationer bedömer PTS att det därför är lämpligt med ett undantagsförfarande, som kan användas för att skapa bästa möjliga balans mellan kostnader, tillgänglig teknik och säkerhet. Det kan t.ex. röra reservkraftskrav där en anläggnings beskaffenhet avseende storlek eller funktionalitet tekniskt begränsar möjligheterna att uppfylla kravet.

6.14.2 Föreslagna ändringar och dess konsekvenser

Tillhandahållare av NI-ICS

För tillhandahållare av NI-ICS är de föreslagna bestämmelserna om ansökan om undantag i 11 kap. 10–12 §§ nya.

PTS bedömer att sådana tillhandahållare kommer att använda möjligheten att ansöka om undantag i mycket liten utsträckning, bl.a. på grund av att tillhandahållarna normalt inte har tillgångar på sådana platser där det kan vara en utmaning att installera reservkraftssystem eller redundanta tillgångar.

PTS bedömer därför att bestämmelserna inte kommer att innebära några ekonomiska konsekvenser.

Övriga tillhandahållare

Övriga tillhandahållare, dvs. samtliga tillhandahållare förutom för NI-ICS, omfattas redan av bestämmelser om ansökan om undantag. Som ovan angetts motsvarar den föreslagna bestämmelsen 23 § PTSFS 2015:2 med vissa språkliga och redaktionella ändringar. De språkliga och redaktionella ändringarna syftar endast till att förtydliga och förenkla bestämmelsen. Någon ändring av bestämmelsernas innebörd är dock inte avsedd varför PTS bedömer att dessa inte kommer att innebära några ekonomiska konsekvenser.

6.15 Åtgärder avseende övervakning och beredskap

12 kap. i de förslagna föreskrifterna innehåller en bestämmelse om åtgärder avseende övervakning och beredskap. Genom övervakning av nät och tjänster samt genom att ha en personell beredskap kan tillhandahållare förebygga och upptäcka säkerhetsincidenter samt snabbt hantera dem om de inträffar.

Bestämmelsen motsvarar 14 § PTSFS 2015:2 med vissa mindre språkliga och redaktionella ändringar samt en materiell ändring. Den materiella ändringen innebär att övervakningen och beredskapen inte bara ska syfta till att förebygga, upptäcka och åtgärda säkerhetsincidenter som innebär störningar eller avbrott (som gäller enligt nuvarande föreskrifter) utan ska förebygga, upptäcka och åtgärda även övriga typer av säkerhetsincidenter.

Den föreslagna bestämmelsen om åtgärder avseende övervakning och beredskap omfattar samtliga tillhandahållare. För tillhandahållare av NI-ICS är bestämmelsen ny. För övriga tillhandahållare – som redan omfattas av nuvarande föreskrifter – är det endast utvidgningen av bestämmelsens tillämpningsområde, till att omfatta samtliga typer av säkerhetsincidenter, som innebär en ändring i sak.

6.15.1 Beskrivning av bestämmelserna

Enligt 12 kap. 1 § ska tillhandahållare kontinuerligt övervaka tjänster och aktiva delar i nät för att kunna förebygga, upptäcka och åtgärda säkerhetsincidenter. När det gäller specifikt säkerhetsincidenter som innebär störningar eller avbrott ska tillhandahållare dessutom ha system som kan larma. Systemen ska således larma om t.ex. en hårddisk går sönder, temperaturen i en server stiger onormalt eller ett it-system som behandlar uppgifter får onormalt många anrop av någon viss typ.

Tillhandahållare ska ha personell beredskap för att dels hantera eventuella larm vid störningar och avbrott dels kunna initiera relevanta åtgärder för att hantera alla olika typer av säkerhetsincidenter (dvs. inte bara störningar och avbrott). Bestämmelsen gäller dygnet runt, dvs. även utanför kontorstid. Det är emellertid tillhandahållare själva som avgör hur en säkerhetsincident ska avhjälpas. I vissa fall kan det vara så att en åtgärd inte är nödvändig att påbörja direkt, men det kan också innebära att åtgärder behöver initieras med en gång t.ex. genom att relevant personal kontaktas så att felavhjälpning kan påbörjas.

Att vidta tekniska och organisatoriska åtgärder avseende övervakning och beredskap är enligt PTS en förutsättning för att tillhandahållare ska ha en förmåga att dels kunna upptäcka säkerhetsincidenter, dels snabbt kunna avhjälpa dem. Utan detta finns en risk att incidenter förblir oupptäckta eller onödigt utdragna i tiden. Eftersom tillhandahållare dessutom köper tillträde till nät och tjänster av varandra finns det även en risk att incidenter som inte hanteras av en tillhandahållare leder till incidenter även för andra tillhandahållare. Åtgärder avseende övervakning och beredskap är dessutom något som särskilt anges i EU:s verktygslåda för 5G-säkerhet som viktiga åtgärder för att hantera risker för hot mot centrala delar av nät. Till exempel omnämns hot mot kärnnät till följd av kompromitterad utrustning hos användare.[36]

Genom övervakningen erhålls en kontinuerlig indikation på (vetskap om) om de nät och tjänster som övervakas är tillgängliga, om intrångsförsök sker, att de har den kapacitet som behövs och fungerar som förväntat.

För att begränsa säkerhetsincidenter och undvika att återställande försenas – något som även kan drabba andra tillhandahållare – är det därför av vikt att det finns ständig beredskap dygnet runt. Det är möjligt för flera tillhandahållare att samverka och organisera gemensam övervakning och jourtjänstgöring.

[36] Se s. 25 i Cybersecurity of 5G networks- EU Toolbox of risk mitigating measures, TM05 *Ensuring secure 5G network management, operation and monitoring.*

6.15.2 Föreslagna ändringar och dess konsekvenser

Tillhandahållare av NI-ICS

För tillhandahållare av NI-ICS är den föreslagna bestämmelsen om åtgärder avseende övervakning och beredskap i 12 kap. 1 § ny.

PTS bedömning är emellertid att tillhandahållare av NI-ICS generellt redan vidtar åtgärder avseende kontinuerlig övervakning och beredskap av tjänster och aktiva tillgångar för att kunna upptäcka samt avhjälpa säkerhetsincidenter (framförallt tekniska åtgärder i form av bl.a. övervakningssystem eller -tjänster).

PTS bedömer att den administrativa engångskostnaden kan bestå av att vidare-utveckla sin övervaknings- och beredskapsförmåga. Till exempel. kan tillhandahållare som inte har tillräckligt med personal för övervakning och beredskap behöva avsätta tid för att bedriva övervakningen, alternativt upphandla en övervakningsförmågetjänst (*SOC, Security Operations Center*). Då tillhandahållare även kan behöva komplettera befintlig teknisk övervakning med ytterligare larm bedömer PTS att kravet kan medföra kostnader. PTS uppskattar att kostnaden för detta uppgår till 21 640 kronor, givet en tidsåtgång om 40 timmar och en lönekostnad om 541 kronor.

PTS bedömer att den administrativa årliga kostnaden består i att utföra själva bevakningen. PTS uppskattar att administrativa årliga kostnaden för detta uppgår till 54 100 kronor, givet en tidsåtgång om 100 timmar och en lönekostnad om 541 kronor.

Övriga kostnader kan bestå av kostnader relaterade till anskaffning av kompletterande teknisk utrustning och programvara. PTS uppskattar att dessa övriga kostnader uppgår till 750 000 kronor. Givet en diskonteringsränta på 4,44 % och en avskrivningstid på fem år ger det en årlig annuitetsberäknad kostnad på 170 550 kronor/år.

Övriga tillhandahållare

Övriga tillhandahållare, dvs. samtliga tillhandahållare förutom tillhandahållare av NI-ICS, omfattas redan av bestämmelser om åtgärder avseende övervakning och beredskap. Som ovan angetts motsvarar den föreslagna bestämmelsen 14 § PTSFS 2015:2 med vissa mindre språkliga och redaktionella ändringar samt med den materiella ändringen angående utvidgningen av bestämmelsens tillämpningsområde.

För tillhandahållare som tidigare endast har haft övervakning och beredskap för att kunna upptäcka och avhjälpa avbrott och störningar kan kravet innebära att tillhandahållare behöver investera i en ny typ av övervakningssystem eller övervakningstjänst med avseende på konfidentialitet, autenticitet och riktighet, samt att driftsätta (installera och konfigurera) detta, vilket inkluderar att lägga till vad som ska

övervakas, och att upprätta övervakning. PTS bedömer därmed att det föreslagna kravet kan medföra dels administrativa kostnader, dels övriga kostnader.

PTS bedömer att administrativa engångskostnader avser arbete med att inventera vad som behöver övervakas med avseende på konfidentialitet, autenticitet och riktighet. PTS uppskattar att kostnaderna för detta uppgår till 129 840 kronor för stora företag (givet en tidsåtgång om 240 timmar och en lönekostnad om 541 kronor), 21 640 kronor för medelstora företag (givet en tidsåtgång om 40 timmar och en lönekostnad om 541 kronor), 10 820 kronor för små företag (givet en tidsåtgång om 20 timmar och en lönekostnad om 541 kronor) samt 5 410 kronor för mikroföretag (givet en tidsåtgång om 10 timmar och en lönekostnad om 541 kronor).

PTS bedömer vidare att de administrativa årliga kostnaderna avser personalkostnader för att bedriva den ev. utökade övervakningen. PTS uppskattar att de administrativa årliga kostnaderna för detta uppgår till 75 740kronor för stora företag (givet en tidsåtgång om 140 timmar och en lönekostnad om 541 kronor), 75 740 kronor för medelstora företag (givet en tidsåtgång om 140 timmar och en lönekostnad om 541 kronor), 69 248 kronor för små företag (givet en tidsåtgång om 128 timmar och en lönekostnad om 541 kronor) samt 21 640 kronor för mikroföretag (givet en tidsåtgång om 40 timmar och en lönekostnad om 541 kronor).

PTS bedömer vidare att övriga kostnader kan avse inköp och införande av teknisk utrustning och programvara för den utökade bevakningen. PTS kan inte uppskatta vilka kostnader detta skulle kunna medföra eftersom det beror på vilken utrustning och andra lösningar som finns på plats idag, vilket bör vara olika hos olika tillhandahållare.

6.16 Intern incidenthantering

13 kap. i de förslagna föreskrifterna innehåller bestämmelser om intern incidenthantering. Intern incidenthantering handlar om att ha, samt tillämpa, en process som stöd för att minimera skadeverkning av säkerhets- och integritetsincidenter samt snabbt kunna återgå till ett normalläge.

Bestämmelserna motsvarar 10 och 11 §§ PTSFS 2014:1 samt 7 § PTSFS 2015:2 med vissa mindre språkliga och redaktionella ändringar samt en materiell ändring. Den materiella ändringen innebär att även integritetsintrång avseende uppgifter som lagras för brottsbekämpande ändamål omfattas av bestämmelserna.

De föreslagna bestämmelserna om intern incidenthantering omfattar samtliga tillhandahållare. För tillhandahållare av NI-ICS är bestämmelserna nya. Tillhandahållare av NI-ICS är emellertid inte skyldiga att säkerställa att uppgifter som lagras för brottsbekämpande ändamål skyddas eftersom dessa inte omfattas av skyldigheten

att lagra sådana uppgifter. Den interna incidenthanteringen omfattar således inte detta. För övriga tillhandahållare – som redan omfattas av nuvarande föreskrifter – är det endast tillägget avseende uppgifter som lagras för brottsbekämpande ändamål som för vissa tillhandahållare innebär en ändring i sak.

6.16.1 Beskrivning av bestämmelserna

Enligt 13 kap. 1 § ska tillhandahållare ha processer som säkerställer att intern rapportering av säkerhets- och integritetsincidenter sker, att åtgärder vidtas skyndsamt för att hantera uppkomna incidenter och att åtgärder vidtas för att undvika att liknande incidenter inträffar igen. Dessutom ska processerna säkerställa att incidenter och dess orsaker beaktas vid genomförande av riskanalyser.

Processerna är enligt PTS av vikt för att underlätta tillhandahållares arbete att säkerställa att incidenter fångas upp och tas om hand på ett systematiskt och effektivt sätt. Processerna säkerställer även att tillhandahållare kan dra lärdomar från incidenterna. När en incident inträffar är målsättningen således att kunna reagera skyndsamt på det inträffade för att begränsa skadan och återupprätta normaltillståndet på ett systematiskt och effektivt sätt. Målsättningen är även att kunna lära av och återföra kunskaper från inträffade incidenter till organisationen gällande det framtida säkerhetsarbetet så att liknande incidenter förebyggs och att tillhandahållare har en bättre beredskap. Enligt PTS är en effektiv hantering av incidenter en förutsättning för ett långsiktigt, kontinuerligt och systematiskt säkerhetsarbete.

Bestämmelserna innebär vidare att tillhandahållares processer ska utgå från etablerad standard på området. Exempel på etablerad standard är SS-ISO/IEC 27041 Vägledning för att säkerställa lämplighet och tillräcklighet av utredningsmetoder för incidenter samt SS-EN ISO/IEC 27043 Principer och processer för undersökning av incidenter.

13 kap. 1 § innebär även att när det särskilt gäller integritetsincidenter ska tillhandahållare av kommunikationstjänster dessutom ha rutiner för identifiering av sådana incidenter. Det anges även i 2 § vilka uppgifter dessa tillhandahållare ska ange i förteckningen över integritetsincidenter (som ska föras enligt 8 kap. 9 § nya LEK).

Av bestämmelserna om övergripande säkerhetsarbete i 3 kap. följer att processerna och rutinerna ska upprättas, dokumenteras och revideras vid behov samt att tillhandahållare ska säkerställa att de anställda och uppdragstagare som berörs av dem har kunskap om och tillämpar dem.

6.16.2 Föreslagna ändringar och dess konsekvenser

Tillhandahållare av NI-ICS

För tillhandahållare av NI-ICS är de föreslagna bestämmelserna om intern incidenthantering i 13 kap. nya. Tillhandahållare av NI-ICS är emellertid inte skyldiga att säkerställa att uppgifter som lagras för brottsbekämpande ändamål skyddas eftersom dessa inte omfattas av skyldigheten att lagra sådana uppgifter. Den interna incidenthanteringen omfattar således inte detta.

PTS bedömer att den administrativa engångskostnaden består i att etablera en incidenthanteringsprocess med tillhörande rutiner. PTS uppskattar att kostnaden för detta uppgår till 34 624 kronor, givet en tidsåtgång om 64 timmar och en lönekostnad om 541 kronor.

PTS bedömer att de administrativa årliga kostnaderna består i att årligen revidera processen med tillhörande rutiner och tillämpa den. PTS uppskattar att kostnaden för detta uppgår till 69 248 kronor, givet en tidsåtgång om 128 timmar och en lönekostnad om 541 kronor.

Övriga årliga kostnader utgörs av utbildning, framförallt för de som ska tillämpa rutinerna. Även om tillhandahållare av NI-ICS kan antas ha någon form av processer och rutiner för detta sedan tidigare, som en följd av systematiskt säkerhetsarbete och/eller regler i EU:s dataskyddsförordning, så behöver dessa i viss mån anpassas för att uppfylla kraven. PTS uppskattar att dessa övriga kostnader uppgår till 17 312 kronor, givet en tidsåtgång om 32 timmar och en lönekostnad om 541 kronor.

Övriga tillhandahållare

Övriga tillhandahållare, dvs. samtliga tillhandahållare förutom för NI-ICS, omfattas redan av bestämmelser om intern incidenthantering. Som ovan angetts motsvarar de föreslagna bestämmelserna 10 och 11 §§ PTSFS 2014:1 samt 7 § PTSFS 2015:2 med vissa mindre språkliga och redaktionella ändringar samt med den materiella ändringen att även integritetsintrång avseende uppgifter som lagras för brottsbekämpande ändamål omfattas av bestämmelserna.

PTS bedömer att för de tillhandahållare som ska lagra uppgifter för brottsbekämpande ändamål så avser de administrativa engångskostnaderna tidsåtgången för att revidera processer och rutiner rörande incidenthantering så att de omfattar integritetsintrång avseende uppgifter som lagras för brottsbekämpande ändamål. PTS uppskattar att de administrativa engångskostnaderna för detta uppgår till 34 624 kronor för stora företag (givet en tidsåtgång om 64 timmar och en lönekostnad om 541 kronor), 8 656 kronor för medelstora företag (givet en tidsåtgång om 16 timmar och en lönekostnad om 541 kronor), 4 328 kronor för små

företag (givet en tidsåtgång om 8 timmar och en lönekostnad om 541 kronor) samt 2 164 kronor för mikroföretag (givet en tidsåtgång om 4 timmar och en lönekostnad om 541 kronor).

PTS bedömer vidare att de administrativa årliga kostnaderna avser att tillämpa och vid behov revidera processer och rutiner för incidenthantering rörande integritetsintrång avseende uppgifter som lagras för brottsbekämpande ändamål. PTS uppskattar att de administrativa årliga kostnaderna för detta uppgår till 69 248 kronor för stora företag (givet en tidsåtgång om 128 timmar och en lönekostnad om 541 kronor), 17 312 kronor för medelstora företag (givet en tidsåtgång om 32 timmar och en lönekostnad om 541 kronor), 8 656 kronor för små företag (givet en tidsåtgång om 16 timmar och en lönekostnad om 541 kronor) samt 4 328 kronor för mikro-företag (givet en tidsåtgång om 8 timmar och en lönekostnad om 541 kronor).

6.17 Kontinuitetsplanering

14 kap. i de förslagna föreskrifterna innehåller bestämmelser om kontinuitetsplanering. Kontinuitetsplanering handlar om att planera för att kunna fortsätta tillhandahålla nät och tjänster även i händelse av att nödvändiga verksamhetsdelar eller resurser helt eller delvis slutar att fungera eller blir otillgängliga. Det kan t.ex. handla om situationer där servrar eller system slutar att fungera, att anställda av olika anledningar inte kan komma till arbetet eller att tillhandahållare inte får nödvändiga varor eller tjänster levererade till sig.

Bestämmelserna motsvarar 6 och 8 §§ PTSFS 2015:2 med språkliga och redaktionella ändringar samt en materiell ändring. Den materiella ändringen innebär att kontinuitetsplanerna även ska innehålla uppgifter om när och hur planerna övas och revideras. Detta krav gäller utöver det nuvarande kravet om att planerna ska upprättas, dokumenteras och åtminstone innehålla de åtgärder som behövs för att begränsa de konsekvenser som kan uppstå enligt konsekvensanalysen samt för att återställa kritiska verksamhetsdelar till normal funktionsförmåga.

De föreslagna bestämmelserna om kontinuitetsplanering omfattar samtliga tillhandahållare. För tillhandahållare av NI-ICS är bestämmelserna nya. För övriga tillhandahållare – som redan omfattas av nuvarande föreskrifter – är det endast tillägget gällande kontinuitetsplanernas innehåll som innebär en ändring i sak.

6.17.1 Beskrivning av bestämmelserna

Bestämmelserna innebär att tillhandahållare ska analysera vilka *konsekvenser* som kan uppstå i en situation där kritiska verksamhetsdelar och resurser helt eller delvis slutar att fungera eller blir otillgängliga, samt utifrån den analysen ta fram *kontinuitetsplaner* som ska tillämpas om en sådan situation skulle uppstå.

Syftet med bestämmelserna är att tillhandahållare genom kontinuitetsplaneringen ska minska konsekvenserna av och snabbare kunna återhämta sig från en inträffad händelse och på så sätt begränsa säkerhetsincidenter i form av störningar och avbrott. Tillhandahållare har då beredskap för händelser som typiskt sett inte kan förutses i en riskanalys. I en riskanalys beaktas orsaken till och sannolikheten för säkerhetsincidenter medan det i kontinuitetsplaneringen inte tas denna hänsyn, utan det avgörande är vilka konsekvenser som kan uppstå och hur de konsekvenserna ska hanteras oaktat hur sannolikt det är att en säkerhetsincident inträffar. En sådan förberedelse är enligt PTS av vikt för att kunna begränsa konsekvenserna av inträffade säkerhetsincidenter. Kontinuitetsplanering är dessutom något som särskilt anges som viktiga åtgärder i EU:s verktygslåda för 5G-säkerhet.[37]

Konsekvensanalys

Enligt 14 kap. 1 § ska tillhandahållare identifiera de verksamhetsdelar och resurser som är nödvändiga för att nätet eller tjänsterna ska kunna upprätthållas så att nätet eller tjänsten är tillgängliga.

I allmänna råd till 1 § ges exempel på vad sådana verksamhetsdelar och resurser kan vara.

Efter att ha identifierat nödvändiga verksamhetsdelar och resurser ska tillhandahållare analysera vilka konsekvenser som kan uppstå om dessa helt eller delvis slutar att fungera eller blir otillgängliga. Analysen ska omfatta en bedömning av när tillhandahållare ska verkställa sina kontinuitetsplaner. Det innebär alltså att tillhandahållare måste bedöma hur länge verksamheten kan upprätthållas utan den aktuella verksamhetsdelen eller resursen – oaktat orsaken till eller sannolikheten för att den skulle bli otillgänglig.

Konsekvensanalysen resulterar således i en kartläggning över hur verksamheten ser ut, vad som behövs för att kunna upprätthålla näten och tjänsterna samt hur länge näten och tjänsterna kan upprätthållas innan oacceptabla konsekvenser uppstår.

Konsekvensanalysen ska dokumenteras vilket utgör en förutsättning för en systematisk uppföljning av säkerhetsarbetet och kontroll av vilka bedömningar som gjorts inom ramen för kontinuitetsplaneringen. Konsekvensanalysen ska även revideras vid behov, t.ex. vid omfattande organisatoriska förändringar eller omfattande förändringar i näten eller tjänsterna såsom byte av underleverantör eller plattform.

[37] Se s. 27 i Cybersecurity of 5G networks- EU Toolbox of risk mitigating measures, TM11 *Reinforcing resilience and continuity plans.*

Kontinuitetsplaner

Utifrån konsekvensanalysen ska tillhandahållare enligt 14 kap. 2 § ta fram och tillämpa kontinuitetsplaner som syftar till att begränsa de konsekvenser som framgår av konsekvensanalysen samt för att så snart som möjligt kunna återställa verksamheten till normal funktionsförmåga om den kritiska delen skulle falla bort eller bli otillgänglig. Konsekvensanalysen utgör ett nödvändigt beslutsunderlag och är en förutsättning för att tillhandahållare ska kunna ta fram kontinuitetsplaner.

Kontinuitetsplanerna ska åtminstone innehålla åtgärder för att begränsa de konsekvenser som kan uppstå enligt konsekvensanalysen och för att återställa kritiska verksamhetsdelar till normal funktionsförmåga. Av kontinuitetsplanerna ska det alltså framgå vad som behövs för att säkerställa att verksamheten har en god beredskap för att hantera oväntade och oförutsedda händelser. De ska säkerställa att det i organisationen finns tillräckliga resurser, tillräckliga och tillgängliga befogenheter samt dokumenterade tillvägagångssätt för hur organisationen ska agera vid händelser som påverkar kritiska delar av verksamheten.

Kontinuitetsplanerna kan t.ex. omfatta definierade tillvägagångssätt och återställandeåtgärder, prioritetsordningar, processer för att säkerställa att extra resurser kan avsättas när det är nödvändigt. De kan även omfatta säkerställande av att det finns en tydlig organisation för utförande av beslutade åtgärder och uppgifter om vilken befattning eller funktion som är ansvarig för att olika åtgärder vidtas samt former för vidarerapportering inom verksamheten.

Kontinuitetsplanerna ska även innehålla en beskrivning av när och hur de ska övas och revideras. Att dessa uppgifter framgår av planerna är av vikt för att det ska vara känt för berörd personal och det utgör även ett underlag för tillhandahållares systematiska uppföljning av säkerhetsarbetet.

Planerna ska övas minst vartannat år och vid behov revideras. PTS bedömer att detta utgör en förutsättning för att tillhandahållare ska kunna bedöma om planerna fungerar och är ändamålsenliga, för att öka personalens kunskap om hur dessa ska användas samt för att skapa en organisationskultur som främjar kontinuitetsplanering. Förutsättningarna för verksamheten är föränderliga vilket kan påverka konsekvensanalysen och kontinuitetsplanerna.

Tillhandahållare ska utgå från etablerad standard på området vid framtagande av kontinuitetsplanerna. I allmänna råd till 2 § anges att tillhandahållare bör utgå från SS-EN ISO 22301 *Ledningssystem för kontinuitetshantering* eller motsvarande vid sitt framtagande av kontinuitetsplaner.

Av bestämmelserna om övergripande säkerhetsarbete i 3 kap. följer att kontinuitetsplanerna ska upprättas, dokumenteras och revideras vid behov samt att tillhandahållare ska säkerställa att de anställda och uppdragstagare som berörs av dem har kunskap om och tillämpar dem.

6.17.2 Föreslagna ändringar och dess konsekvenser

Tillhandahållare av NI-ICS

För tillhandahållare av NI-ICS är de föreslagna bestämmelserna om kontinuitetsplanering i 14 kap. nya.

PTS bedömer att den administrativa engångskostnaden består av att upprätta en kontinuitetsplan och dokumentera den. PTS uppskattar att de administrativa engångskostnaderna för detta uppgår till 21 640 kronor (givet en tidsåtgång om 40 timmar och en lönekostnad om 541 kronor).

Den återkommande administrativa kostnaden utgörs av övning vartannat år. PTS uppskattar att de administrativa årliga kostnaderna för detta uppgår till 25 968 kronor (givet en tidsåtgång om 48 timmar och en lönekostnad om 541 kronor).

Övriga tillhandahållare

Övriga tillhandahållare, dvs. samtliga tillhandahållare förutom tillhandahållare av NI-ICS, omfattas redan av bestämmelser om kontinuitetsplanering. Som ovan angetts motsvarar de föreslagna bestämmelserna 6 och 8 §§ PTSFS 2015:2 med vissa språkliga och redaktionella ändringar samt med den materiella ändringen att det införs krav på att kontinuitetsplanerna även ska innehålla uppgift om hur planerna övas och revideras.

Att kontinuitetsplanerna ska övas och revideras vid behov gäller redan enligt nuvarande bestämmelser. Det föreslagna tillägget begränsas således till att själva planerna ska kompletteras med uppgifter om detta. Även om det alltså redan krävs att planerna ska övas och revideras vid behov ser PTS ett behov av att dessa uppgifter finns med i planerna för att säkerställa att övning och revidering faktiskt sker och att tillhandahållare har en planering för när detta ska ske. Det är enligt PTS en förutsättning för en fungerande kontinuitetsplanering.

PTS bedömer således att bestämmelserna medför en administrativ engångskostnad som avser arbete med att revidera planerna i syfte att säkerställa att samtliga uppgifter finns med. PTS uppskattar att kostnaden för detta uppgår till 34 624 kronor för stora företag (givet en tidsåtgång om 64 timmar och en lönekostnad om 541 kronor), 8 656 kronor för medelstora företag (givet en tidsåtgång om 16 timmar och en lönekostnad om 541 kronor), 4 328 kronor för små företag (givet en

tidsåtgång om 8 timmar och en lönekostnad om 541 kronor) samt 2 164 kronor för mikroföretag (givet en tidsåtgång om 4 timmar och en lönekostnad om 541 kronor).

I övrigt föreslås följande språkliga och redaktionella ändringar av bestämmelserna om kontinuitetsplanering. Någon ändring av bestämmelserna innebörd är dock inte avsedd varför PTS bedömer att dessa inte kommer att innebära några ekonomiska konsekvenser.

- Begreppet ”handlingsplan” byts genomgående ut mot begreppet ”kontinuitetsplan” då PTS bedömer att det är ett mer vedertaget begrepp.
- Det förtydligas – vilket tidigare har varit underförstått – att tillhandahållare först behöver *identifiera* sina nödvändiga verksamhetsdelar och resurser innan konsekvensanalysen genomförs.
- Bestämmelserna om konsekvensanalyser och kontinuitetsplaner (i nuvarande regelverk ”handlingsplaner”) placeras tillsammans till skillnad från PTSFS 2015:2 där bestämmelserna hålls åtskilda.[38]
- Begreppet ”verksamhetsdelar” förtydligas genom att begreppet ”resurser” läggs till och bestämmelserna kompletteras också med allmänna råd som exemplifierar vad som avses med dessa begrepp.
- Bestämmelsen om att tillhandahållare ska utgå från etablerad standard kompletteras med allmänna råd som förtydligar och ger vägledning kring vilken standard detta bör vara.

6.18 Fredstida planering för totalförsvarets behov av elektronisk kommunikation

15 kap. i de förslagna föreskrifterna innehåller bestämmelser om den fredstida planeringen för totalförsvarets behov av elektronisk kommunikation. Bestämmelserna består av två delar. Den första delen handlar om att tillhandahållare – i tillägg till bestämmelserna om kontinuitetsplanering i 14 kap. – ska säkerställa att planeringen även omfattar höjd beredskap och krig. Den andra delen handlar om att tillhanda-hållare ska ta fram planer för att vid höjd beredskap ock krig kunna ställa personal till förfogande för samverkan med PTS.

Bestämmelserna om kontinuitetsplanerna för höjd beredskap och krig (15 kap. 1 och 2 §§) motsvarar 2 § första, andra och fjärde strecksatsen samt 3 § med språkliga och redaktionella ändringar samt ett antal materiella ändringar. De materiella ändringarna innebär att det anges vad planerna åtminstone ska innehålla, att

[38] Bestämmelser om konsekvensanalyserna regleras i PTSFS 2015:2 tillsammans med bestämmelser om riskanalyser, och bestämmelser om kontinuitetsplanerna – som i den föreskriften benämns handlingsplaner – regleras tillsammans med bestämmelser om planering för och hantering av inträffade händelser som kan orsaka störningar och avbrott.

planerna ska dokumenteras och vid behov revideras, att tillhandahållare vid framtagandet av planerna ska utgå från etablerad standard på området samt att planeringen ska revideras för det fall PTS informerar särskilt om det.

Bestämmelsen om att ta fram planer för samverkan (15 kap. 3 §) motsvarar 2 § tredje strecksatsen PTSFS 1995:1 med språkliga och redaktionella ändringar samt ett antal materiella ändringar. De materiella ändringarna innebär att en lättnad i förhållande till nuvarande reglering införs genom att den planering som ska göras begränsas till att avse samverkan enbart med PTS. Vidare innebär ändringen att syftet med samverkan och hur länge den ska kunna upprätthållas anges i bestämmelsen.

De föreslagna bestämmelserna om den fredstida planeringen för totalförsvarets behov av elektronisk kommunikation omfattar, precis som nuvarande reglering, samtliga tillhandahållare förutom tillhandahållare av NI-ICS. Tillhandahållare av NI-ICS föreslås inte heller omfattas av de nu föreslagna bestämmelserna.

6.18.1 Beskrivning av bestämmelserna

Kontinuitetsplaner för höjd beredskap och krig

Enligt 15 kap. 1 § ska samtliga tillhandahållare förutom tillhandahållare av NI-ICS, i tillägg till bestämmelserna om kontinuitetsplanering i 14 kap., upprätta kontinuitetsplaner även för höjd beredskap och krig. PTS bedömer att denna planering utgör en förutsättning för att tillhandahållare ska ha förmåga att upprätthålla sin verksamhet även i händelse av höjd beredskap och krig.

På samma sätt som krävs enligt 14 kap. ska kontinuitetsplanerna åtminstone innehålla de åtgärder som behöver vidtas för att begränsa konsekvenserna som kan uppstå enligt konsekvensanalysen och för att återställa kritiska verksamhetsdelar eller resurser till normal funktionsförmåga. Kontinuitetsplanerna ska även innehålla en beskrivning av när och hur kontinuitetsplanerna övas och revideras. Tillhandahållare ska dessutom utgå från etablerad standard på området vid framtagande av planerna.

Till skillnad från bestämmelserna om kontinuitetsplanering i 14 kap. krävs dock inte att kontinuitetsplanerna för höjd beredskap och krig faktiskt övas. Kontinuitetsplanerna ska dock innehålla uppgift om huruvida detta ska ske eller inte så att det blir känt för berörd personal. Av planerna ska det därför framgå om, och i sådana fall när och hur, tillhandahållare planerar att genomföra övning. Vidare innehåller bestämmelserna gällande höjd beredskap och krig inte heller något krav om när planerna ska tillämpas.

Av bestämmelserna om övergripande säkerhetsarbete i 3 kap. följer att kontinuitetsplanerna ska upprättas, dokumenteras och revideras vid behov samt att tillhanda-

hållare ska säkerställa att de anställda och uppdragstagare som berörs av dem har kunskap om och tillämpar dem.

Precis som bestämmelserna om kontinuitetsplanering i 14 kap. är syftet att mildra konsekvenserna av och snabbare kunna återhämta sig från en inträffad händelse oaktat orsaken till eller sannolikheten för händelsen. Eftersom varken orsak eller sannolikhet är något som beaktas kan planeringen för fredstid bära stora likheter med den för höjd beredskap och krig. Det kan dock vara så att ett läge av höjd beredskap och krig kan förutsätta att andra åtgärder vidtas. Det är därför av vikt att tillhandahållare tar fram planer även med detta perspektiv i åtanke. I tillägg till den eventuella anpassning av kontinuitetsplanerna som tillhandahållare på eget initiativ kan behöva göra är tillhandahållare enligt 15 kap. 2 § skyldiga att anpassa planeringen i enlighet med eventuell information som PTS förmedlar. I syfte att tillgodose totalförsvarets behov av elektroniska kommunikationer vid höjd beredskap och i krig kan PTS komma att informera tillhandahållare om sådant som kontinuitetsplaneringen måste omfatta. Det kan antingen röra sig om vilka verksamhetsdelar och resurser som ska omfattas av planeringen eller vad planerna i övrigt ska innehålla. Syftet är att fånga upp sådant som är av vikt för totalförsvarets behov av elektroniska kommunikationer vid höjd beredskap och i krig men som tillhandahållare inte själv har beaktat i sin kontinuitetsplanering. På vilket sätt sådan information förmedlas till tillhandahållare regleras inte utan får avgöras i det enskilda fallet.

Planering för samverkan med PTS

Enligt 15 kap. 3 § ska samtliga tillhandahållare förutom tillhandahållare av NI-ICS i fredstid ta fram planer för att vid höjd beredskap och i krig kunna ställa personal till förfogande för samverkan med PTS i den omfattning som krävs. Bestämmelsen syftar till att PTS ska ha tillgång till en samverkansfunktion hos tillhandahållare, som ska kunna utbyta information med PTS och i sin tur föra informationen vidare och bereda uppgifter inom tillhandahållares egen organisation.

Tillhandahållare ska ha beredskap för att kunna upprätthålla samverkansfunktionen dygnet runt i 90 dagar. Bestämmelsen är utformad i enlighet med att utgångspunkten för planeringen av totalförsvaret bör vara att under minst tre månader kunna hantera en säkerhetspolitisk kris.[39]

6.18.2 Föreslagna ändringar och dess konsekvenser

Kontinuitetsplaner för höjd beredskap och krig

De tillhandahållare som bestämmelserna gäller för omfattas redan idag av bestämmelser om den fredstida planeringen inför höjd beredskap och krig. Som

[39] Se bl.a. s. 27 i proposition 2020/21:30 *Totalförsvaret 2021–2025.*

angetts ovan motsvarar de föreslagna bestämmelserna 2 § första, andra och fjärde strecksatsen samt 3 § PTSFS 1995:1 med språkliga och redaktionella ändringar samt med ett antal materiella ändringar.

De språkliga och redaktionella ändringarna innebär att kravet omformuleras till en skyldighet att upprätta kontinuitetsplaner för höjd beredskap och krig. Det i sig innebär inte någon ändring av bestämmelsernas innebörd varför PTS bedömer att detta inte kommer innebära några ekonomiska konsekvenser.

De materiella ändringarna innebär att det införs krav på vad kontinuitetsplanerna åtminstone ska innehålla, att de ska dokumenteras och revideras vid behov samt att PTS kan komma att informera om vilka verksamhetsdelar och resurser som ska omfattas av planeringen samt vad kontinuitetsplanerna ska innehålla.

Bestämmelserna avser de administrativa åtgärderna till följd av att ta fram en plan, inte att vidta själva åtgärderna. PTS konstaterar att det inte på förhand går att ange vilken information som kan bli aktuell att förmedla om vilka verksamhetsdelar och resurser som ska omfattas av planeringen samt vad kontinuitetsplanerna ska innehålla. Bestämmelsen kommer sannolikt realiseras ytterst sällan och begränsas till revidering av processen.

PTS bedömer att tillhandahållare redan har en process för kontinuitetsplanering som de tillämpar för detta ändamål, men att denna behöver anpassas efter det förändrade kravet, vilket innebär en administrativ engångskostnad som utgörs av dokumentation och anpassning av kontinuitetsplanen. PTS uppskattar att denna kostnad uppgår till 34 624 kronor för stora företag (givet en tidsåtgång om 64 timmar och en lönekostnad om 541 kronor), 17 312 kronor för medelstora företag (givet en tidsåtgång om 32 timmar och en lönekostnad om 541 kronor), 8 656 kronor för små företag (givet en tidsåtgång om 16 timmar och en lönekostnad om 541 kronor) samt 4 328 kronor för mikroföretag (givet en tidsåtgång om 8 timmar och en lönekostnad om 541 kronor).

PTS bedömer vidare att de administrativa årliga kostnaderna avser revidering av kontinuitetsplanerna. PTS uppskattar att de administrativa årliga kostnaderna för detta uppgår till 34 624 kronor för stora företag (givet en tidsåtgång om 64 timmar och en lönekostnad om 541 kronor), 17 312 kronor för medelstora företag (givet en tidsåtgång om 32 timmar och en lönekostnad om 541 kronor), 8 656 kronor för små företag (givet en tidsåtgång om 16 timmar och en lönekostnad om 541 kronor) samt 4 328 kronor för mikroföretag (givet en tidsåtgång om 8 timmar och en lönekostnad om 541 kronor).

Planer för samverkan med PTS

De tillhandahållare som bestämmelsen gäller för omfattas redan av bestämmelser om planer för samverkan. Som ovan angetts motsvarar den föreslagna bestämmelsen 2 § tredje strecksatsen PTSFS 1995:1 med språkliga och redaktionella ändringar samt med ett antal materiella ändringar.

De materiella ändringarna innebär att skyldigheten att planera för samverkan behålls men begränsas till att endast avse samverkan med PTS och att det anges vad syftet med samverkan är och hur länge den ska kunna upprätthållas.

Ändringen av kravet innebär en försumbar årlig kostnad eftersom planeringsarbetet kan anses minska något, men innebär också att planerna behöver revideras vilket utgör en administrativ engångskostnad PTS uppskattar att dessa administrativa kostnader uppgår till 34 624 kronor för stora företag (givet en tidsåtgång om 64 timmar och en lönekostnad om 541 kronor), 17 312 kronor för medelstora företag (givet en tidsåtgång om 32 timmar och en lönekostnad om 541 kronor), 8 656 kronor för små företag (givet en tidsåtgång om 16 timmar och en lönekostnad om 541 kronor) samt 4 328 kronor för mikroföretag (givet en tidsåtgång om 8 timmar och en lönekostnad om 541 kronor).

6.19 Information till användare om konkreta och betydande hot om en säkerhetsincident

16 kap. i de förslagna föreskrifterna innehåller en bestämmelse om information till användare om konkreta och betydande hot om en säkerhetsincident. Bestämmelsen förtydligar när informationen ska lämnas samt på vilket sätt informationen bör lämnas och vad informationen bör bestå av.

Den föreslagna bestämmelsen omfattar samtliga tillhandahållare. Bestämmelsen är ny.

6.19.1 Beskrivning av bestämmelserna

Bestämmelsen kompletterar den nya skyldigheten enligt 8 kap. 4 § nya LEK om att tillhandahållare av nät och tjänster, om det finns ett konkret och betydande hot om en säkerhetsincident, ska informera de användare som kan komma att påverkas av hotet om vilka skydds- eller motåtgärder som de kan vidta, och, om det är lämpligt, om själva hotet.[40]

[40] I sammanhanget kan nämnas att en liknande bestämmelse sedan tidigare finns på integritetsområdet i 8 kap. 7 § nya LEK. Den innebär att om det vid tillhandahållande av en kommunikationstjänst finns en särskild risk för bristande skydd av behandlade uppgifter så ska den som tillhandahåller tjänsten

Informationsskyldigheten i nya LEK gäller konkreta och betydande hot om säkerhetsincidenter som upptäcks. Att hotet ska vara konkret och betydande innebär att det ska finnas ett konkret hot som kan drabba användare på ett ingående sätt, t.ex. genom att användare kan drabbas av avbrott i tjänster eller att känsliga uppgifter om användare riskerar att spridas. Informationen ska ange vilka skydds- eller motåtgärder som användarna kan vidta. Det kan t.ex. röra sig om användning av kryptering, byte av lösenord eller uppgradering av programvara. Vid bedömningen av om det är lämpligt att informera om själva hotet bör det t.ex. beaktas om spridning av uppgifter om vad en upptäckt säkerhetsbrist består i kan väntas förvärra hotet. Informationsskyldigheten befriar inte aktören från skyldigheten att vidta säkerhetsåtgärder som att avhjälpa hot och återställa en normal säkerhetsnivå.[41]

Enligt 16 kap. 1 § ska tillhandahållare informera användare som kan komma att påverkas av ett konkret och betydande hot om en säkerhetsincident så snart som möjligt efter att hotet har upptäckts, för att användarna ska kunna vidta de skydds- eller motåtgärder som rekommenderas av tillhandahållare.

I allmänna råd till 1 § anges att tillhandahållare bör försäkra sig om att informationen verkligen når ut till berörda användare. Informationen bör lämnas på ett säkert sätt så att inte informationen i sig ger upphov till nya säkerhetsincidenter. Det är enligt PTS viktigt att tillhandahållare säkerställer att kommunikationen med användarna sker på ett säkert och trovärdigt sätt. Det är här viktigt att typen av information och uppmaning till användarna inte öppnar nya vägar för t.ex. nätfiske (*phishing*) och andra bedrägerier.

I allmänna råd till 1 § anges även att informationen bör, om det är möjligt och lämpligt, beskriva den risk som hotet innebär och vad konsekvenserna kan bli om användarna inte vidtar rekommenderade åtgärder. Detta är enligt PTS särskilt viktigt om det inte är lämpligt att tillhandahållare informerar om själva hotet. Användare antas endast i låg utsträckning följa en uppmaning från sin tillhandahållare om de inte får information om varför eller vad som kan hända om de inte följer uppmaningen.

6.19.2 Föreslagets konsekvenser

Den föreslagna bestämmelsen är ny för samtliga tillhandahållare.

informera berörda abonnenter om risken. Om den som tillhandahåller tjänsten inte är skyldig att enligt 8 kap. 6 § nya LEK avhjälpa risken, ska abonnenterna informeras om hur och till vilken ungefärlig kostnad risken kan avhjälpas.

[41] Se prop. 2021/22:136 *Genomförande av direktivet om inrättande av en europeisk kodex för elektronisk kommunikation*, s. 496-497.

PTS bedömer att arbete för att uppfylla detta krav ryms inom nuvarande kundrelationsarbete, och medför därför ingen ytterligare kostnad.

6.20 Incidentrapportering till PTS

17 kap. i de förslagna föreskrifterna innehåller bestämmelser om den skyldighet tillhandahållare har att rapportera säkerhetsincidenter som har haft en betydande påverkan på nät och tjänster enligt 8 kap. 3 § nya LEK. Bestämmelserna förtydligar vilka säkerhetsincidenter som ska rapporteras, när och hur rapportering ska ske samt vad rapporterna ska innehålla.

I 1 kap 7 § nya LEK definieras säkerhetsincident som en händelse med en faktisk negativ inverkan på tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst, hos lagrade, överförda eller behandlade uppgifter eller hos de närliggande tjänster som erbjuds genom eller är tillgängliga via dessa elektroniska kommunikationsnät eller elektroniska kommunikationstjänster, eller på förmågan att motstå sådana händelser.

Definitionen omfattar fyra säkerhetsaspekter, se avsnitt 1.1.31.1.3 om det nya säkerhetsbegreppet. En incident kan röra negativ inverkan på en eller flera av de fyra säkerhetsaspekterna.

De föreslagna bestämmelserna motsvarar PTSFS 2012:2 med språkliga och redaktionella ändringar samt ett antal materiella ändringar. De materiella ändringarna innebär att säkerhetsincidenter, inte bara i form av störningar och avbrott, ska rapporteras och det anges under vilka förutsättningar det ska göras. Ändringarna innebär även att det införs en möjlighet att beviljas anstånd gällande den kompletterande rapporten.

De föreslagna bestämmelserna om incidentrapportering omfattar samtliga tillhandahållare. För tillhandahållare av NI-ICS är bestämmelserna nya. För övriga tillhandahållare – som redan omfattas av nuvarande föreskrifter – är det endast de materiella ändringarna som utgör en ändring i sak.

6.20.1 Beskrivning av bestämmelserna

Tillhandahållare ska enligt 8 kap. 3 § nya LEK *utan onödigt dröjsmål* rapportera säkerhetsincidenter som har haft en *betydande påverkan* på nät och tjänster till PTS.

En säkerhetsincident kan inträffa genom yttre påverkan men kan också bero på brister eller otillåtet förfarande hos den som tillhandahåller nätet eller tjänsten. Rapporteringsskyldigheten gäller oavsett hur händelsen påbörjats eller vem som är ansvarig för dess uppkomst. Avgörande är i stället vilka konsekvenser incidenten har

haft. Rapporteringsskyldigheten gäller även för säkerhetsincidenter hos t.ex. tredjepartsleverantörer och följdincidenter på grund av en sådan incident, om kravet på betydande påverkan på driften av nätet eller tjänsten är uppfyllt. Detta påverkar inte den rapporteringsskyldighet som leverantören självständigt kan ha med anledning av sin verksamhet.[42]

Syftet med bestämmelserna i 17 kap. är att PTS ska kunna bedöma om tillhandahållarna uppfyller sina skyldigheter enligt nya LEK, dvs. om kraven på säkerhetsåtgärder är uppfyllda, eller om det finns anledning att vidta tillsynsåtgärder till följd av inträffade incidenter. Syftet är även att möjliggöra insamling av de uppgifter som årligen ska sammanställas och lämnas in till kommissionen och ENISA, samt att vid behov kunna informera behöriga myndigheter i övriga medlemsstater och ENISA, eller att uppdra åt tillhandahållare att informera allmänheten i det fall en säkerhetsincident ligger i allmänhetens intresse.

Vilka säkerhetsincidenter som ska rapporteras

Säkerhetsincidenter ska rapporteras till PTS om de har haft en betydande påverkan på nät och tjänster.[43]

I 17 kap. specificeras när en säkerhetsincident är rapporteringspliktig.

Avgörande för om de säkerhetsincidenter som *innebär störning eller avbrott*, i tillhandahållna nät eller tjänster är rapporteringspliktiga enligt 17 kap. 5 § är en kombination av dess varaktighet och konsekvens. Incidentens varaktighet bestäms utifrån tiden som incidenten pågått. Incidentens konsekvens bestäms utifrån hur många aktiva anslutningar eller användare som berörs, hur stort geografiskt område som berörs eller hur stor andel av nätets eller tjänstens kapacitet som berörs.

Detta innebär att även mer kortvariga störningar ska rapporteras om konsekvenserna är mycket omfattande. Störningar som varar en längre tid ska också rapporteras, även om konsekvenserna inte är lika omfattande. Det är dock inte meningen att tillhandahållarna ska rapportera om alla de dagliga och kortvariga störningar och avbrott som normalt uppstår och som endast påverkar ett fåtal abonnenter.[44]

Regeln i 17 kap. 5 § i de föreslagna föreskrifterna är avsedd att tillämpas på incidenter som innebär störning eller avbrott. PTS har inte avsett någon utvidgning av

[42] Se prop. 2021/22:136 *Genomförande av direktivet om inrättande av en europeisk kodex för elektronisk kommunikation*, s. 320 och 497.
[43] Se prop. 2021/22:136 *Genomförande av direktivet om inrättande av en europeisk kodex för elektronisk kommunikation*, s. 495.
[44] Se prop. 2021/22:136 *Genomförande av direktivet om inrättande av en europeisk kodex för elektronisk kommunikation*, s. 495.

rapporteringsskyldigheten vad avser säkerhetsincidenter som innebär störningar eller avbrott i nät eller tjänster.

I allmänna råd till 5 § anges hur ett geografiskt område normalt bör definieras och hur ett kapacitetsbortfall exempelvis bör beräknas.

Att bestämmelsen anger att antalet aktiva anslutningar *eller* användare ska beräknas beror på att vissa tillhandahållare endast kan beräkna aktiva anslutningar men saknar kunskap om antalet användare och vice versa.

En säkerhetsincident är enligt 17 kap. 6 § rapporteringspliktig, utöver vad som framgår av 17 kap. 5 § om den har haft en betydande påverkan på nätets eller tjänstens funktion eller funktioner i samhället.

När, hur och vad ska rapporteras

När en säkerhetsincident ska rapporteras till PTS ska det göras utan onödigt dröjsmål.

Att rapportering ska göras utan onödigt dröjsmål betyder att den som regel ska ske så snart de första kritiska åtgärderna för att avhjälpa säkerhetsincidenten har vidtagits och de uppgifter som ska lämnas finns tillgängliga. Om det behövs internt utredningsarbete för att kunna sammanställa samtliga uppgifter som ska lämnas till PTS bör myndigheten lämpligen kunna underrättas dels i direkt anslutning till säkerhetsincidenten om det som då är känt, dels vid ett senare tillfälle när samtliga uppgifter har sammanställts.[45]

Enligt 17 kap. 2 § ska därför tillhandahållare lämna en inledande och en kompletterande rapport till PTS.

Incidentrapporteringen ska enligt 17 kap. 3 § aldrig göras senare än tre dagar efter den dag incidenten upptäcktes. En kompletterande rapport ska enligt 17 kap. 4 § vara PTS tillhandahålla inom två veckor från det att den inledande rapporten lämnades. Anstånd kan emellertid beviljas.

I allmänna råd till 2 § anges att rapporterna bör lämnas i elektronisk form. Information om incidentrapportering finns på PTS hemsida. Observera att om en incidentrapport innehåller säkerhetsskyddsklassificerade uppgifter gäller de krav på överföring av uppgifter m.m. som följer av säkerhetsskyddslagstiftningen.

I 17 kap. 3 och 4 §§ anges vad den inledande och den kompletterande rapporten ska innehålla för uppgifter. Uppgifterna är sådana som typiskt sett har betydelse för PTS

[45] Se prop. 2021/22:136 *Genomförande av direktivet om inrättande av en europeisk kodex för elektronisk kommunikation*, s. 496.

bedömning av om kraven på säkerhetsåtgärder är uppfyllda eller om det finns anledning att vidta tillsynsåtgärder till följd av händelsen.

I allmänna råd till 3 och 4 §§ anges hur tillhandahållare bör göra för att ta fram de efterfrågade uppgifterna.

Säkerhetsincident eller integritetsincident

Utöver skyldigheten att rapportera säkerhetsincidenter enligt 8 kap. 3 § nya LEK finns även en skyldighet att rapportera integritetsincidenter enligt 8 kap. 8 § nya LEK. När och hur rapportering av integritetsincidenter ska ske regleras i förordning 611/2013.

Det innebär alltså att incidenter med påverkan på uppgifter som behandlas i samband med tillhandahållandet av kommunikationstjänster även fortsättningsvis ska rapporteras enligt bestämmelserna i förordningen (se även avsnitt 1.1.3 om nytt säkerhetsbegrepp).

Integritetsincident definieras i 1 kap 7 § nya LEK som 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. Definitionen är densamma som i nuvarande LEK (se prop. 2010/11:115 s. 130 f. och 181).

Det finns händelser som enligt definitionerna kan vara både en säkerhetsincident och en integritetsincident. Skyldigheterna är delvis överlappande i och med att samma händelse kan vara rapporteringsskyldig enligt båda regelverken. Dock ställs i regelverken olika krav för vilka incidenter som ska rapporteras och vilka regler som gäller för rapporteringen.

6.20.2 Föreslagna ändringar och dess konsekvenser

För tillhandahållare av NI-ICS är de föreslagna bestämmelserna om incident-rapportering i 17 kap. nya.

Rapportering av incidenter på det sätt som anges i de föreslagna bestämmelserna är något som tillhandahållarna med säkerhet inte gör idag. Nya rutiner och processer behöver sättas upp utöver själva arbetet med att rapportera varje incident som blir rapporteringspliktig. Sannolikt kan inte tillhandahållare återanvända någon del av befintliga rutiner (för t.ex. incidentrapportering enligt EU:s dataskyddsförordning) eftersom förfarandena och vilken typ av information som ska rapporteras skiljer sig åt. En multinationell tillhandahållare kan sannolikt inte heller återanvända rutiner och processer som etablerats för att följa regler som implementerar kodexen i andra medlemsstater i EU. Anledningen är att det saknas harmonisering för rapportering av

sådana incidenter, både vad gäller trösklar för vad som är rapporteringspliktigt, vilka tidsfrister som gäller och vilken information som ska lämnas i rapporten.

PTS bedömer att de administrativa engångskostnaderna avser upprättandet av nya rutiner och processer. PTS uppskattar att kostnaden för detta uppgår till 8 656 kronor givet en tidsåtgång om 16 timmar och en lönekostnad om 541 kronor. PTS bedömer vidare att de administrativa årliga kostnaderna avser rapporteringen av inträffade incidenter. PTS uppskattar att rapporteringen av en incident tar fyra timmar och att varje tillhandahållare i snitt rapporterar fyra incidenter per år. Den administrativa årliga kostnaden för detta uppgår således till 8 656 kronor, givet en tidsåtgång om fyra gånger fyra timmar (16) och en lönekostnad om 541 kronor.

Utbildning av personal är en övrig kostnad (engångs) som PTS uppskattar till 17 312 kronor, givet en tidsåtgång om 32 timmar och en lönekostnad om 541 kronor.

Övriga tillhandahållare

Övriga tillhandahållare, dvs. samtliga tillhandahållare förutom tillhandahållare av NI-ICS, omfattas redan av bestämmelser om incidentrapportering. Som ovan angetts motsvarar de föreslagna bestämmelserna PTSFS 2012:2 med vissa mindre språkliga och redaktionella ändringar samt de materiella tilläggen gällande säkerhetsincidenter som inte innebär störningar eller avbrott och att anstånd kan beviljas gällande den kompletterande rapporten.

PTS bedömer att merparten av de konsekvenser som uppstår för tillhandahållare följer av nya LEK och utreds således av regeringen. De konsekvenser som uppstår till följd av de föreslagna föreskrifterna är försumbara.

I övrigt föreslås framför allt följande språkliga och redaktionella ändringar av bestämmelserna om incidentrapportering. Någon ändring av bestämmelsernas innebörd är dock inte avsedd varför PTS bedömer att dessa inte kommer att innebära några ekonomiska konsekvenser.

- I bestämmelsen om tröskelvärde avseende säkerhetsincidenter som innebär störning eller avbrott görs ett tillägg om att det är möjligt att beräkna antalet användare istället för antalet aktiva anslutningar. Tillägget är framför allt gjort för att anpassa bestämmelserna för tillhandahållare av NI-ICS.
- Bestämmelsen om tidpunkten för lämnande av den inledande rapporten förenklas från att ange att den ska lämnas senast vardagen efter den dag felet avhjälpts men aldrig senare än tre dagar efter att den blev rapporteringspliktig till att den ska lämnas senast 72 timmar efter upptäckt.

6.21 Totala kostnader för tillhandahållare

I denna del presenteras totala kostnader för tillhandahållare uppdelat på nättillhandahållare, tillhandahållare av NI-ICS och övriga tjänstetillhandahållare. Denna uppdelning görs då de olika kategorierna av tillhandahållare, som beskrivs i avsnitt 6.5–6.20, berörs olika av olika delar av förslaget. Observera att PTS i detta avsnitt med tjänstetillhandahållare avser samtliga tjänstetillhandahållare (med/utan nät) förutom NI-ICS, som alltså redovisas som en egen kategori.

För att belysa de materiella ändringar som PTS bedömer inte medför konsekvenser utöver dagens krav inkluderas även de delar där det bedöms att de tillkommande kostnaderna är noll.

De kostnader som här summeras, från avsnitten 6.5–6.20, är dels administrativa engångskostnader och dels administrativa årliga kostnader. Därtill finns ett fåtal investeringskostnader under kategorin övriga kostnader i avsnitt 6.5–6.20 ovan. Dessa har räknats om till årliga annuitetsberäknade kostnader, med en estimerad avskrivningstid på 5 år och en diskonteringsränta på 4,44 %[46] och återfinns bland de årliga kostnaderna i totalkostnadstabellerna. En rad produktionskostnader i form av utbildningskostnader ingår också i summeringen. Dessa kostnader är både av engångskaraktär och årligen återkommande och har inkluderats i totalkostnadstabellerna som engångs- respektive årlig kostnad tillsammans med övriga kostnadsposter. För nättillhandahållare och tjänstetillhandahållare har också en uppdelning över den relevanta populationen baserad på aktörernas storlek enligt tabell 1 och 2 i avsnitt 4 gjorts. PTS har valt att summera de exakta kostnader som är skattade baserat på antal timmar och andra kostnader, men det bör poängteras att siffrorna i tabellerna är skattningar förenade med osäkerhet.

Som framgår av tabell 2 i avsnitt 4 (kolumnerna A och B) bedömer PTS att det finns 105 nättillhandahållare och 328 tjänstetillhandahållare som träffas av regleringen. Till detta kommer ytterligare 80 aktörer (av de 155 aktörerna i kolumn C i samma tabell) som PTS också bedömer träffas av regleringen och som, med bas i storleksfördelningen i kolumn C, lagts till tjänstetillhandahållarkategorin. Detta gör att antalet tjänstetillhandahållare totalt blir 408.

Totala kostnader presenteras i tabell 3 och 4 nedan, för nättillhandahållare och tjänstetillhandahållare, dels som en summa av engångskostnader per aktör, dels som årligen återkommande kostnader per aktör, uppdelat på mikro, små, medel- och

[46] Detta är den kalkylränta som PTS fastställt för det fasta nätet år 2021; https://www.pts.se/globalassets/startpage/dokument/legala-dokument/beslut/2021/telefoni-och-internet/koppar/bilaga-2-kalkylranta-wacc-for-det-fasta-natet.pdf

stora aktörer. Mikrokategorin delas i sin tur in i två delgrupper, då vissa aktörer, enligt resonemang i avsnitt 4 och 8, bedöms träffas mindre av regleringen.[47]

Kostnadsestimaten i tabellerna 3 och 4 kommer från PTS egna skattningar, vilka också har beaktat de inkomna enkätsvaren från marknaden. För små, medelstora och stora aktörer finns en någorlunda god överensstämmelse mellan PTS och aktörernas skattningar i hur mycket tid som aktörerna totalt behöver lägga ner på åtgärder relaterade till den nya regleringen. För mikrokategorin bygger PTS skattningar i avsnitten 6.5–6.20 ovan emellertid inte på PTS egna skattningar för de allra minsta aktörerna (de som benämns ”Mikroaktör, 0-1 anställd” i tabell 3 och 4 nedan). Det eftersom PTS inte har samma kunskap om den gruppen för att på motsvarande sätt som för övriga göra egna kostnadsskattningar. Denna kategori av aktörer (aktörer med högst en anställd och, därtill, högst 2 miljoner kronor i intäkt) särredovisas därför i tabellerna, och den skattade kostnaden utgår istället helt från enkätsvaren. Kostnadsestimaten presenteras utifrån medelvärden, där inrapporterad tidsåtgång för varje åtgärd dividerats med antal svarande företag. Det antas därmed att nättillhandahållarna och tjänstetillhandahållarna i genomsnitt har samma kostnad för respektive åtgärd. Det eftersom inte tillräckligt många enkätsvar inkommit för att på ett meningsfullt sätt differentiera mellan nättillhandahållare och tjänstetillhandahållare. Nättillhandahållarna möter dock vissa krav som inte tjänstetillhandahållarna möter, vilket förklarar skillnaden i kostnad mellan dessa två grupper.

I övrigt, gällande skillnader och likheter mellan PTS egna kostnadsestimeringar och inkomna kostnadsuppgifter från enkäterna, gäller att för investeringar och andra kostnader (utbildning etc.) ligger PTS skattningar av totalkostnader oftast lägre än enkätsvaren från aktörerna. De relativt få enkätsvaren indikerar dock att vissa aktörer tolkat PTS enkätfrågor som att betydande investeringar behöver göras, vilket PTS bedömer inte behövs. PTS har sökt förtydliga vissa av åtgärderna i denna konsekvensutredning, som också kommer att skickas på remiss till ett urval aktörer. En osäkerhet finns också i enkätsvaren eftersom dessa generellt är få. PTS kan inte utesluta att exempelvis de aktörer som bedömer att de kommer att få högst kostnader också är de som svarat på enkäten.

Förutom medelvärden per aktör presenteras också den relevanta populationen av berörda aktörer i de olika storlekskategorierna samt den totala kostnaden för summan av alla aktörer i den relevanta populationen uppdelat i de olika storlekskategorierna för engångskostnader och årligen återkommande kostnader.

[47] För den mindre av de två mikrokategorierna presenteras endast totalkostnader per aktör, utan en uppdelning på enskilda regleringsområden.

För tillhandahållare av NI-ICS är inte antal aktörer kända. För tillhandahållare av NI-ICS presenteras således enbart totala engångskostnader och årliga kostnader per aktör, vilket görs i tabell 5 nedan.

Nedan i tabell 3 sammanfattas de totala kostnader som PTS skattat att förslaget skulle kunna medföra för nättillhandahållare. Stora nättillhandahållare träffas hårdast i absoluta kostnadsökningar med totala engångskostnader på 930 976 kronor per aktör och årliga kostnader på 820 761 kronor/år och aktör för samtliga föreslagna ändringar beskrivna i avsnitt 6. De medelstora nättillhandahållarna träffas av engångskostnader på 437 094 kronor per aktör och årliga kostnadsökningar på 450 144 kronor/år och aktör till följd av samtliga föreslagna ändringar. De små nättillhandahållarna berörs av engångskostnader på 204 219 kronor per aktör och årliga kostnadsökningar på 265 580 kronor/år och aktör. De nättillhandahållare som klassas som mikroföretag (undantaget de allra minsta aktörerna) berörs av engångskostnader på 116 577 kronor per aktör och årliga kostnader på 144 569 kronor/år och aktör. De aktörer i mikrokategorin som har högst en anställd (och med intäkter mindre än 2 miljoner kronor/år) skattas få engångskostnader på ca 46 000 kronor per aktör samt årliga kostnader på ca 30 000 kronor/år och aktör.

Summerat över den relevanta populationen kan det vidare ses att för de stora och medelstora aktörerna återfinns endast en aktör varvid den totala kostnaden för den relevanta populationen är den samma som per aktör. För de 25 små aktörerna blir de totala engångskostnaderna 5 105 475 kronor och de totala årliga kostnaderna 6 639 500 kronor/år. För mikroföretagen (undantaget de allra minsta aktörerna) som är 65 stycken blir de totala engångskostnaderna 7 577 505 kronor och de årliga kostnaderna 9 396 985 kronor/år.

Gällande de 13 nättillhandahållande aktörerna i mikrokategorin som har högst en anställd (och med årsintäkter om mindre än 2 miljoner kronor) kan det observeras att de totala engångskostnaderna för de 13 aktörerna uppgår till ca 600 000 kronor. Samma aktörer har också totala årliga kostnader på ca 390 000 kronor/år.

Tabell 3: Totala regleringskostnader för nättillhandahållare (kr)

	Mikroaktör, 0-1 anställd		Mikro övriga		Liten		Medel		Stor	
Ändrade krav	**Engångs-kostnad**	**Årlig kostnad**	**Engångs-kostnad**	**Årlig kostnad**	**Engångs-kostnad**	**Årlig kostnad**	**Engångs-kostnad**	**Årlig kostnad**	**Engångs-kostnad**	**Årlig kostnad**
6.5 Övergripande säkerhetskrav	NA	NA	13 246	53 410	15 410	70 820	50 820	117 640	116 230	227 165
6.6 Identifiering och dokumentation av till tillgångar m.m.	NA	NA	1 082	4 328	2 164	4 328	4 328	4 328	6 492	4 328
6.7 Riskanalys	NA	NA	10 820	19 476	21 640	38 952	51 936	77 904	103 872	155 808
6.8 Hantering av risker och åtgärder efter riskbedömning	NA	NA	3 787	6 492	7 574	12 984	15 184	25 968	43 280	69 248
6.9 Åtgärder avseende åtkomst och behörighet	NA	NA	1 082	1 353	2 164	3 246	4 328	32 790	8 656	43 940
6.10 Säkerhetskopiering	NA	NA	1 082	1 082	5 410	2 164	10 820	4 328	17 312	8 656
6.11 Loggning	NA	NA	32 460	23 804	78 445	37 870	156 890	59 510	297 550	97 380
6.12 Kryptering	NA	NA	34 624	4 328	34 624	8 656	69 248	17 312	69 248	34 624
6.13 Redundans och reservkraftssystem	NA	NA	0	0	0	0	0	0	0	0
6.14 Ansökan om undantag	NA	NA	0	0	0	0	0	0	0	0
6.15 Åtgärder avseende övervakning och beredskap	NA	NA	5 410	21 640	10 820	69 248	21 640	75 740	129 840	75 740
6.16 Intern incidenthantering	NA	NA	2 164	4 328	4 328	8 656	8 656	17 312	34 624	69 248
6.17 Kontinuitetsplanering	NA	NA	2 164	0	4 328	0	8 656	0	34 624	0
6.18 Fredstida planering för totalförsvarets behov av elektronisk kommunikation	NA	NA	8 656	4 328	17 312	8 565	34 624	17 312	69 248	34 624
6.19 Information till användare om konkreta och betydande hot om en säkerhetsincident	NA	NA	0	0	0	0	0	0	0	0
6.20 Incidentrapportering till PTS	NA	NA	0	0	0	0	0	0	0	0
Summa kostnader: Kronor/aktör	NA	NA	116 577	144 569	204 219	265 580	437 094	450 144	930 976	820 761
Svar enligt enkät: Kronor/aktör	46 422	30 192								
Totalt antal aktörer i den relevanta populationen	13	13	65	65	25	25	1	1	1	1
Total kostnad för den relevanta populationen	603 486	392 496	7 577 505	9 396 985	5 105 475	6 639 500	437 094	450 144	930 976	820 761

Från tabell 4, nedan, kan det observeras att tjänstetillhandahållarna berörs av något färre konsekvenser i form av kostnadsökningar i jämförelse med nättillhandahållarna beskrivet ovan. För de stora tjänstetillhandahållarna innebär summan av samtliga föreskriftsändringar beskrivna i avsnitt 6 ovan ökade engångskostnader på 515 488 kronor per aktör och 1 295 640 kronor/år och aktör. För de medelstora tjänstetillhandahållarna innebär samtliga ändringar ökade engångskostnader på 215 284 kronor per aktör och årliga kostnader på 589 392 kronor/år och aktör. För de små tjänstetillhandahållarna observeras ökade engångskostnader på 93 314 kronor per aktör och årliga kostnadsökningar på 202 824 kronor/år och aktör. För de 184

tjänstetillhandahållare som klassas som mikroföretag (undantaget de allra minsta aktörerna) kan det observeras engångskostnader på 68 969 kronor per aktör och årliga kostnader på 106 428 kronor/år och aktör.

Gällande de 87 tjänstetillhandahållande aktörerna i mikrokategorin som har högst en anställd (och med årsintäkter om mindre än 2 miljoner kronor) kan det observeras att engångskostnaderna uppgår till ca 35 000 kronor per aktör. För dessa aktörer observeras också årliga kostnader på ca 28 000 kronor/år och aktör.

Summerat över den relevanta populationen kan det vidare ses att tjänstetillhandahållarna som berörs av föreskriftsändringarna är fler än nättillhandahållarna. Detta avspeglas också i större totala kostnader summerat över den relevanta populationen.

För de stora tjänstetillhandahållarna, som är 10 stycken, uppgår de totala engångskostnaderna för samtliga aktörer till 5 154 880 kronor och de total årliga kostnaderna uppgår till 12 956 400 kronor/år för de 10 aktörerna. För de medelstora tjänstetillhandahållarna som är 29 till antalet uppgår de totala engångskostnaderna till 6 243 236 kronor och de totala årliga kostnaderna för samtliga 29 aktörer uppgår till 17 092 368 kronor/år.

För de små tjänstetillhandahållarna som är 98 stycken till antalet blir de totala engångskostnaderna 9 144 772 kronor och de totala årliga kostnaderna blir 19 876 752 kronor/år för samtliga 98 aktörer. För aktörerna inom mikrokategorin (undantaget de allra minsta aktörerna) som är 184 stycken uppgår de totala engångskostnaderna över hela populationen till 12 690 296 kronor och de årliga kostnaderna uppgår till 19 582 752 kronor/år för samtliga 184 aktörer.

Gällande de 87 tjänstetillhandahållande aktörerna i mikrokategorin som har högst en anställd (och med årsintäkter om mindre än 2 miljoner kronor) kan det observeras att de totala engångskostnaderna för de 87 aktörerna uppgår till ca 3.1 miljoner kronor för dessa 87 aktörer. Samma aktörer har också totala årliga kostnader på ca 2.4 miljoner kronor/år.

Tabell 4: Totala regleringskostnader för tjänstetillhandahållare (förutom NI-ICS) (kr)

	Mikroaktör, 0-1 anställd		Mikro övriga		Liten		Medel		Stor	
Ändrade krav	**Engångs-kostnad**	**Årlig kostnad**	**Engångs-kostnad**	**Årlig kostnad**	**Engångs-kostnad**	**Årlig kostnad**	**Engångs-kostnad**	**Årlig kostnad**	**Engångs-kostnad**	**Årlig kostnad**
6.5 Övergripande säkerhetskrav	NA	NA	10 000	48 000	10 000	60 000	40 000	96 000	100 000	192 000
6.6 Identifiering och dokumentation av till tillgångar m.m.	NA	NA	0	0	0	0	0	0	0	0
6.7 Riskanalys	NA	NA	2 164	17 312	4 328	34 624	17 312	69 248	34 624	138 496
6.8 Hantering av risker och åtgärder efter riskbedömning	NA	NA	3 787	6 492	7 574	12 984	15 148	25 968	43 280	69 248
6.9 Åtgärder avseende åtkomst och behörighet	NA	NA	0	0	0	0	0	0	0	0
6.10 Säkerhets-kopiering	NA	NA	0	0	0	0	0	0	0	0
6.11 Loggning	NA	NA	0	0	0	0	0	0	0	0
6.12 Kryptering	NA	NA	34 624	4 328	34 624	8 656	69 248	17 312	69 248	34 624
6.13 Redundans och reservkraft-system	NA	NA	0	0	0	0	0	0	0	0
6.14 Ansökan om undantag	NA	NA	0	0	0	0	0	0	0	0
6.15 Åtgärder avseende övervakning och beredskap	NA	NA	5 410	21 640	10 820	69 248	21 640	346 240	129 840	757 400
6.16 Intern incidenthantering	NA	NA	2 164	4 328	4 328	8 656	8 656	17 312	34 624	69 248
6.17 Kontinuitets-planering	NA	NA	2 164	0	4 328	0	8 656	0	34 624	0
6.18 Fredstida planering för totalförsvarets behov av elektronisk kommunikation	NA	NA	8 656	4 328	17 312	8 656	34 624	17 312	69 248	34 624
6.19 Information till användare om konkreta och betydande hot om en säkerhets-incident	NA	NA	0	0	0	0	0	0	0	0
6.20 Incident-rapportering till PTS	NA	NA	0	0	0	0	0	0	0	0
Summa kostnader: Kronor/aktör	NA	NA	68 969	106 428	93 314	202 824	215 284	589 392	515 488	1 295 640
Svar enligt enkät: Kronor/aktör	35 602	28 028								
Totalt antal aktörer i den relevanta populationen	87	87	184	184	98	98	29	29	10	10
Total kostnad för den relevanta populationen	3 097 374	2 438 436	12 690 296	19 582 752	9 144 772	19 876 752	6 243 236	17 092 368	5 154 880	12 956 400

Gällande tillhandahållare av NI-ICS är den relevanta populationen inte känd då detta är en ny grupp att regleras av de nu föreslagna föreskrifterna. Det kan dock observeras från tabell 5 nedan att de totala engångskostnaderna per tillhandahållare

av NI-ICS för samtliga föreskriftsförslag uppgår till 482 293 kronor per aktör och de årliga kostnaderna för samtliga krav uppgår till 807 793 kronor/år och aktör.

Tabell 5: Totala regleringskostnader för tillhandahållare av NI-ICS (kr)

Krav	NI-ICS	
	Engångskostnad	**Årlig kostnad**
6.5 Övergripande säkerhetskrav	44 624	227 165
6.6 Identifiering och dokumentation av tillgångar m.m.	18 935	9 738
6.7 Riskanalys	151 480	86 560
6.8 Hantering av risker och åtgärder efter riskbedömning	15 148	17 312
6.9 Åtgärder avseende åtkomst och behörighet	27 050	27 050
6.10 Säkerhetskopiering	12 984	8 656
6.11 Loggning	86 560	59 510
6.12 Kryptering	4 328	8 656
6.13 Redundans och reservkraftssystem	17 312	17 312
6.14 Ansökan om undantag	0	0
6.15 Åtgärder avseende övervakning och beredskap	21 640	224 650
6.16 Intern incidenthantering	34 624	86 560
6.17 Kontinuitetsplanering	21 640	25 968
6.18 Fredstida planering för totalförsvarets behov av elektronisk kommunikation	0	0
6.19 Information till användare om konkreta och betydande hot om en säkerhetsincident	0	0
6.20 Incidentrapportering till PTS	25 968	8 656
Summa kostnader: SEK/aktör	482 293	807 793
Totalt antal aktörer i den relevanta populationen	Inte känd	Inte känd

Totalkostnaderna för de 513 nät- och tjänstetillhandahållare som PTS skattat kostnader för ovan uppgår till ca 51 miljoner kronor i engångskostnader och ca 90 miljoner kronor i årliga kostnader. Någon sammanräkning för NI-ICS har som ovan framgår inte gjorts.

7. Konkurrens

Detta avsnitt analyserar effekter av de föreslagna föreskrifterna på konkurrens, med hjälp av OECD:s modell för konkurrensanalys vid reglering.[48] Modellen ligger till grund för Tillväxtverkets rekommendationer avseende hur en konkurrensanalys ska genomföras i en konsekvensutredning.[49]

Det första steget är att bedöma vilken den relevanta marknaden är. Den relevanta marknaden utgörs av de som omfattas av de föreslagna föreskrifterna, vilket är tillhandahållare av nät och tjänster, se avsnitt 4.

Tjänster som fast och mobil telefoni, fast och mobilt bredband etc. är i viss mån substitut till varandra. Aktörerna som tillhandahåller dessa tjänster ingår dock alla i gruppen aktörer som diskuteras i avsnitt 4, och omfattas alltså av PTS marknadsdefinition.[50] Här är det dock i vissa fall även relevant med en diskussion utifrån marknaden för antingen nät eller tjänster.[51]

Som ett andra steg ställs fyra huvudfrågor relaterade till konkurrens på den relevanta marknaden:

1. Påverkar de nya föreskrifterna antalet företag på marknaden?

2. Påverkar de nya föreskrifterna företagens förmåga att konkurrera?

3. Påverkar de nya föreskrifterna företagens incitament att konkurrera?

4. Påverkar de nya föreskrifterna konsumenters valmöjligheter och beteenden?

---

[48] https://www.oecd.org/daf/competition/COMP_Toolkit_Vol.3_ENG_2019.pdf.

[49] Påverkas konkurrensförhållanden? - Tillväxtverket (tillvaxtverket.se).

[50] En reglering som, hypotetiskt, träffar en grupp aktörer hårdare skulle kunna leda till att denna grupp aktörer höjer konsumentpriser och att konsumenterna i viss grad skiftar till andra tjänster (exv. från fasta till mobila tjänster, eller vice versa). Eftersom substituttjänsterna i detta fall också tillhandahålls av berörda LEK-aktörer ingår båda grupperna i den marknadsdefinition vi använder. Ett analogt resonemang kan föras för substitution mellan NI-ICS-tjänster och ”traditionella” tjänster inom elektronisk kommunikation: Båda grupperna ingår i vår marknadsdefinition.

[51] Nättillhandahållarna är t ex (jämfört med tjänstetillhandahållarna) i större utsträckning knutna till den geografiska platsen gällande konkurrensförhållanden kopplat till fast fiberbredband, vilket också kan inverka på deras konkurrensförmåga. Nättillhandahållare är också i större utsträckning än tjänstetillhandahållare (enligt vad som kan utläsas av STM) en del av ett större företag eller en kommun, vilket kan inverka på konkurrensförmåga hos mikroföretag enligt diskussion nedan.

Fråga ett handlar bl.a. om huruvida en reglering leder till inträdeshinder i form av höga kostnader eller kanske geografiska hinder. Huruvida alla aktörer behandlas lika eller om vissa aktörer träffas hårdare av ny reglering behandlas under fråga två, liksom om en för hög standard sätts, som det är svårare för vissa aktörer att uppfylla (exempelvis på grund av lägre finansiell eller personalmässig styrka). Frågan om en reglering leder till exempelvis samarbeten som begränsar konkurrensen behandlas under fråga tre och under fråga fyra behandlas konsumenternas faktiska valmöjligheter.

Under fråga ett (och två) anger OECD och Tillväxtverket förhållanden såsom införandet av särskilda system och rutiner, produktions- och produktspecifikationer, (vilka kan leda till) omställnings- och produktionskostnader. Den här diskuterade regleringen omfattar onekligen sådana förändringar.

En annan punkt som diskuteras i metoddokumenten, gällande fråga två, är huruvida vissa aktörer träffas i högre grad än andra aktörer. I tabell 6 presenteras två mått på hur omfattande de tillkommande årliga regleringskostnaderna är för nät- och tjänstetillhandahållare inom de olika storlekskategorierna: dels den skattade kostnaden i sig, dels samma kostnad ställd i förhållande till intäkter. Även om regleringen är teknikneutral och lika för alla inom en viss kategori av aktörer (exempelvis nättillhandahållare), stiger regleringskostnaderna med storleken på aktören (såsom analyserats i avsnitt 6), medan det omvända gäller när regleringskostnaderna ställs i relation till intäkter inom varje kategori.

Tabell 6: Årliga regleringskostnader och årliga regleringskostnader som andel av årsintäkt (kr)

	Nättillhandahållare		**Tjänstetillhandahållare**	
Storlek (enligt definition i tabell 1)	**Regleringskostnad**	**Andel av årsintäkt**	**Regleringskostnad**	**Andel av årsintäkt**
Mikro (högst 1 anställd och intäkt < 2 MSEK)	30 192	2,20 %	28 028	4,25 %
Mikro, övriga	144 569	2,00 %	106 428	1,65 %
Små	265 580	0,73 %	202 824	0,58 %
Medel	450 144	0,23 %	589 392	0,34 %
Stora	820 761	0,12 %	1 295 640	0,02 %

Tabell 6. Årliga regleringskostnad för nät- respektive tjänstetillhandahållare inom olika storlekskategorier (från tabell 3 och 4), respektive årlig regleringskostnad som andel av medelårsintäkten för aktörer inom respektive kategori. MSEK – miljoner kronor.

Medan de skattade kostnaderna för de större aktörerna är små i förhållande till intäkter, gäller inte detsamma för exempelvis de minsta aktörerna inom

mikrokategorin. Om man exempelvis tänker sig ett företag med en vinstmarginal (ungefärligen vinst/intäkt) på 10% så representerar 2.2% respektive 4.2% omfattande kostnader. Samma argument kan appliceras på kategorin övriga aktörer inom mikrokategorin. Det går inte att utesluta att de tids- och övriga kostnadskomponenter som ligger bakom kostnaderna i tabell 6 kan bli svåra för en del aktörer att bära och/eller att dessa aktörer får svårare att konkurrera med de större aktörerna. Eftersom de minsta aktörerna är överlägset flest bör dessa kostnader beaktas. Därmed kan det med avseende på fråga två ovan sägas att föreskriftsförändringarna kan komma att påverka aktörernas förmåga att konkurrera i den meningen att den höjer, relativt sett, kostnaderna för en grupp aktörer (främst inom mikrokategorin) relativt andra aktörer (främst de stora och medelstora aktörerna).

Gällande fråga ett (påverkan på antal aktörer på marknaden), kan de här beskrivna föreskriftsförändringarna potentiellt öka den totala kostnaden för en aktör att starta upp verksamheten och träda in på marknaden. De engångskostnader (och vissa andra årliga kostnader) som här observeras bör rimligen kunna ha karaktär av ”sänkta kostnader”[52], som inte kan återfås om aktören lämnar marknaden. Detta är en typ av kostnader som, om de är alltför höga, kan leda till inträdeshinder. Det bedöms här att det främst är aktörerna i mikrokategorin som relativt sätt kan möta regleringskostnader som kan bli betungande (se tabell 6, ovan). Dessa aktörer (”Mikroaktörer, med 0-1 anställd” och ”Mikro övriga”) utgör tillsammans ca 21 % av marknaden för nättillhandahållande och ca 1,3 % av marknaden för tjänstetillhandahållande, baserat på andelen av de totala intäkterna inom respektive kategori.

Förutom att det är ett problem i sig om aktörerna i mikrokategorin träffas relativt sätt hårdare kan det också vara ett konkurrensproblem att kostnaden för inträde/utträde ökar. I det fall vissa av aktörerna inom mikrokategorin skulle lämna marknaden och bli uppköpta av större konkurrenter, som kan erbjuda slutkunder likvärdiga tjänster bör det inte ses som ett konkurrensproblem i och med att marknadsandelarna är förhållandevis små. Det gäller speciellt tjänstetillhandahållarna där de 205 aktörerna inom mikrokategorin tillsammans har endast ca 1,3 % av marknadsintäkterna.

Gällande fråga två är de potentiella konkurrensaspekterna att aktörerna inom mikrokategorin får sämre marginaler relativt andra aktörer och/eller höjer priser mot slutkunder om de har möjlighet till det. Huruvida sådana effekter uppstår kan se mycket olika ut beroende på om aktörerna exempelvis har ett lokalt nätmonopol eller

[52] Med sänkt kostnad menas här en investeringskostnad som genererar en ström av intäkter över en lång tidshorisont men som inte kan återfås om aktören bestämmer sig för att sälja verksamheten och lämna marknaden. Rutiner, investeringar och utbildning/kunskap i säkerhet kopplat till förslagen i denna föreskrift är svåra att sälja och är kanske till begränsad nytta i ett annat verksamhetsområde som inte arbetar med IT-säkerhet överhuvudtaget. Om tjänsten köps in minskas dessa.

om de agerar på en fullt konkurrensutsatt tjänstemarknad. Allt annat lika bör det leda till att dessa aktörer kan få svårare att konkurrera.

Påverkan på slutkundspriser och t.ex. innovation från aktörerna inom mikrokategorin har inte utretts. Dock medför aktörernas ringa marknadsandelar speciellt för tjänstetillhandahållarna) att den totala inverkan på konkurrensen troligen är begränsad. Det bör dock påpekas att det är något svårare att dra klara slutsatser gällande nättillhandahållarna. Dels då dessa aktörers totala marknadsandelar är större jämfört med tjänstetillhandahållarna och dels då de i större utsträckning verkar på lokalt geografiskt avgränsade marknader, med potentiell inverkan på deras konkurrensförmåga i stort.

I det fall aktörer inom mikrokategorin lämnar marknaden och köps upp av exempelvis små eller medelstora aktörer kan det, allt annat lika, medföra att dessa förbättrar sina skalfördelar och konkurrensförmåga. De höga relativa kostnaderna för aktörerna i mikrokategorin är till viss del en funktion av att dessa aktörer är verksamma på en ineffektiv skala, där större aktörer har skalfördelar och kan vara mer konkurrenskraftiga gällande exempelvis säkerhet. Det leder till att storleksoberoende kostnader relativt sett slår hårdare mot de minsta företagen. Ett sätt för aktörerna i mikrokategorin att kringgå sin ineffektiva skala skulle kunna vara att de köper in färdigpaketerade säkerhetstjänster av större aktörer. Vidare kan det vara fallet att aktörerna i mikrokategorin endast är verksamma på en begränsad del av t.ex. ett nät och därmed endast behöver ta kostnaden för en begränsad del av säkerhetskraven. I vilken utsträckning förhållandena faktiskt ser så ut och vilka kostnadsminskningar det kan leda till har emellertid inte kunnat kvantifieras, varför det endast diskuteras som ett potentiellt beteende av mikroföretagen (och övriga företag) för att motverka sin skalnackdel och för att kostnadsminimera. I det fall aktörerna i mikrokategorin faktiskt köper in säkerhetstjänster från en större aktör, (eller endast utgör en del av och ingår i ett större nät- eller tjänstesystem), bör det även medföra att färre kostnadsposter (som skapas av säkerhetskraven i denna föreskrift) får karaktär av sänkta kostnader (som kan öka kostnaden för inträde/utträde). I ett sådant scenario får marknaden allt annat lika mer en karaktär av att vara ”utmaningsbar”, med avseende på att inträde är mer fritt och utträde har lägre kostnader (från engelskans Contestable market[53]). Det är dock viktigt att poängtera att det bara rör sig om gradskillnader, och andra fasta kostnader och sänkta kostnader som existerar oberoende av de här diskuterade säkerhetskraven förblir oförändrade. Beroende på hur stor andel av aktörerna i mikrokategorin som de facto bär kostnaden för säkerhet själv eller inte påverkar konkurrensen på marknaden således med avseende på både fråga ett (antal företag)

[53] Se t.ex; Baumol, W.J., Willing R., & Panzar, J., (1983) “Contestable Markets: An Uprising in the Theory of Industry Structure: Reply”. Artikel in American Economic Review · February 1983.

och fråga två (konkurrensförmåga). Denna andel har dock (som nämnts ovan) inte kunnat skattas.

I några fall gäller också att de minsta aktörerna är del av ett större företag eller en kommun, vars anställda och intäkter inte ingår i de STM-data som presenteras i avsnitt fyra (och i tabell 6 ovan). Detta är ett generellt metodproblem och en begränsning i PTS STM-data. Det faktum att aktörerna i vissa fall har andra verksamheter och intäkter kan göra att några av de, i STM-data, minsta aktörerna i verkligheten har lättare att bära exempelvis administrativa regleringskostnader än vad som framgår av diskussionen gällande siffrorna i tabell 6. Gällande nättillhandahållarna utgör summan av marknadsandelarna för de 78 aktörerna i mikrokategorin ca 21 % varvid de potentiellt kan inverka mer på marknadens konkurrens än tjänstetillhandahållarna[54]allt annat lika. Utifrån STM-data kan det dock konstateras att samtliga förutom drygt tio av de nättillhandahållande aktörerna i mikrokategorin antingen är en kommun (ett stadsnät) eller ett energibolag. PTS har inte gjort en detaljerad finansiell analys kring dessa aktörer, men det kan konstateras att dessa aktörer därmed bör ha intäkter och personal som inte direkt är registrerad i STM. Dessa aktörer kan därmed potentiellt ha bättre finansiell styrka och/eller personalstyrka än vad som framgår av PTS data. Med avseende på fråga två, kan aktörernas förmåga att konkurrera därmed komma att påverkas i mindre utsträckning av föreskriftens ökade säkerhetskrav, än om de varit helt fristående.

NI-ICS-kategorin är svårbedömd eftersom skattningarna är baserade på en typ av tjänst, snarare än en viss aktörsstorlek. Skattningarna (ca 480 000 kronor i engångskostnad och 807 793 kronor i årlig kostnad) är troligen mer tillämpbara på etablerade företag, såsom de internationella aktörer som verkar på NI-ICS-marknaden i Sverige. Långt lägre kostnader än dessa skulle dock kunna utgöra ett hinder för exempelvis uppstartsbolag. PTS har viss information från marknaden som tyder på att även en mindre tillhandahållare av NI-ICS skulle kunna få kostnader på upp till en tiondel av de här diskuterade kostnaderna. Det går inte att utesluta att regleringskostnader av den storleksordningen kan verka som ett hinder för uppstartsbolag och för innovation i allmänhet, även om kostnaderna kanske inte applicerar direkt efter att en verksamhet startar.

Förutom de konkurrenspåverkande aspekter som kopplats till fråga ett och fråga två och som beskrivits ovan har PTS inte funnit någon direkt inverkan i dagsläget vad gäller föreskriftens inverkan på konkurrensen gällande fråga tre och fyra ovan.

Mot ovanstående beskrivna konkurrensaspekter kopplat till fråga ett och två ska ställas att de minsta aktörerna också kan vara de som har störst behov av ett utökat

[54] Tjänstetillhandahållarna i mikrokategorin har endast ca 1,3 % av marknadsandelarna.

säkerhetsarbete. Höga kostnader kan vara motiverade, om betydande säkerhetsinvesteringar gynnar den enskilde aktören och dess kunder (och samhället i stort, exempelvis genom tidig upptäckt av dataintrång som sedan kan sprida sig).

En annan positiv effekt av ökad säkerhetsreglering kan vara att exempelvis större aktörer inom sektorn riktar sin efterfrågan (avseende tjänster från underleverantörer) till de aktörer som bedriver ett systematiskt säkerhetsarbete, vilket kan gynna aktörer i flera led. Att aktörer med ett mindre strukturerat säkerhetsarbete då skulle kunna slås ut kan vara förenat med samhällsekonomiska vinster, eller åtminstone med en effekt som kompenserar det faktum att vissa företag läggs ner.

Säkerhetsarbete i sig kan också utgöra en innovationsverksamhet som leder till nya verksamheter, eftersom efterfrågan på sådana tjänster torde öka.

Sammantaget kan det inte uteslutas att aktörer, speciellt många mindre, träffas av relativt höga kostnader. Samtidigt kan det särskilt vara små aktörer som har störst behov av ett utökat säkerhetsarbete. Den nya regleringen syftar också till samhälleliga vinster genom säkrare nät och tjänster för alla, och dessa vinster (i exempelvis personlig integritet) kan vara omfattande.

8. Särskild hänsyn till små företag

PTS har övervägt om särskild hänsyn behöver tas till små företag vid utformningen av de föreslagna föreskrifterna. 70% av tillhandahållarna återfinns inom kategorin mikroaktörer varför frågan är central. Som framgår av skattningarna i avsnitt 6 och diskussionen i avsnitt 7 går det inte att utesluta att dessa tillhandahållare träffas proportionerligt hårdare än de större aktörerna, trots att kostnaderna i kronor är betydligt lägre. Detta gäller troligtvis också små tillhandahållare av NI-ICS.

Att kostnader i form av tidsåtgång kan verka höga för mikroföretag kan bero på flera faktorer. Även om ansvaret för säkerheten i nät och tjänster inte kan avtalas eller upphandlas bort är det ofta så att delar av verksamheten i olika utsträckning drivs på entreprenad eller köps som en färdig tjänst. Det innebär att många tillhandahållare inte nödvändigtvis driver eller underhåller nät på egen hand utan köper färdiga tjänster för nät och underhåll, övervakning och trafikdatalagring. De kan även själva köpa tjänster som tillhandahålls över kommunikationsnät eller till och med återförsälja eller ompaketera en befintlig tjänst. De tjänster och nät som nyttjas av dessa mindre

aktörer är sådana som omfattas av säkerhetskraven, antingen direkt eller via kravställning och avtal, varvid kostnaderna kan slås ut på flera kunder. Det kan även vara så att en större organisation står bakom, som till exempel en kommun eller kommunalt energibolag.

Säkerhetskraven kan inte vara lägre för att en tillhandahållare har färre anställda. De föreslagna kraven är en miniminivå som ska hållas oavsett storlek på verksamhet. En aktör med exempelvis 0-1 anställda kan knappast tillhandahålla ett nät eller en tjänst utan att ta hjälp av andra för drift, underhåll eller teknisk expertis, på samma sätt som företag anlitar andra för t.ex. fakturering.

Sammanfattningsvis är det ofta så att även om samma krav gäller för mindre tillhandahållare, är det ofta någon annan (större) aktör som gör själva arbetet för att kraven ska vara uppfyllda, vilket innebär att en mindre tillhandahållare i många fall inte bär hela kostnaden för att uppfylla ett krav.

Bestämmelserna i de föreslagna föreskrifterna är dessutom generellt sett utformade som teknikneutrala funktionskrav eller s.k. ”vad”-krav. Det innebär att bestämmelserna fastställer *vad* tillhandahållare ska uppnå vid vidtagande av olika säkerhetsåtgärder utan att ställa tekniskt detaljerade krav på *hur* detta ska uppnås. Samtliga tillhandahållare, oaktat storlek, har således ett stort utrymme att göra egna bedömningar av hur bestämmelserna ska efterlevas och vilka åtgärder som behöver vidtas utifrån hur deras verksamhet ser ut och de risker som de behöver hantera. PTS bedömning är att föreskrifternas utformning ger en flexibilitet i regelverket och att någon ytterligare särskild hänsyn inte behöver tas till små företag.

9. Ekonomiska effekter för hushåll och konsumenter

I avsnitt 6 skattades de totala engångskostnader för samtliga tillhandahållare förutom tillhandahållare av NI-ICS till följd av de föreslagna föreskrifterna till ca 51 miljoner kronor och de årligen återkommande kostnaderna till ca 90 miljoner kronor i årliga kostnader. För tillhandahållare av NI-ICS kan ingen sådan sammanräkning göras.

Huruvida dessa kostnader kommer att leda till högre konsumentpriser beror bland annat på om de påverkar aktörernas fasta kostnader eller marginalkostnaderna (den kostnad som varierar med antal producerade enheter av en viss vara/tjänst). Det går

inte att utesluta att vissa av åtgärderna påverkar marginalkostnaderna. Exempelvis kan priset för en mjukvarulicens bero av hur mycket trafik som går i ett visst nät. Även ökade fasta kostnader kan påverka konsumentpriser, exempelvis eftersom antalet företag på en marknad påverkas av storleken på de fasta kostnaderna.

Ovanstående resonemang leder till att det inte går att utesluta att konsumentpriser påverkas av den nivå av regleringsåtgärder, och de därmed förenade kostnaderna, som diskuteras i denna konsekvensutredning. Det kan inte heller uteslutas att vissa aktörer i mikrokategorin lämnar marknaden och att tjänsten de utför mot slutkund inte omgående kan ersättas av en andra aktörer. Sämre service eller täckning under tid tills annat substitut ersätter kan därmed inte helt uteslutas i ett sådant scenario. Troligast är dock att substitut finns och att slutkunden därmed kan köpa en motsvarande tjänst av en annan aktör omgående.

De föreslagna föreskrifterna ger dock även positiva effekter. Föreskrifterna syftar till att nät, tjänster och uppgifter ska vara säkra. Konsumenter gynnas av att skyddet för slutanvändare stärks samt av den ökade tillförlitligheten och tillgängligheten till elektroniska kommunikationer som uppnås. När användare känner förtroende för marknaden kan benägenheten att använda nya tekniker öka.[55] Föreskriften kan därför bidra till en ökad tillit till elektroniska kommunikationstjänster.

10. Annan säkerhetsreglering

Av vikt att uppmärksamma är att nät och tjänster som omfattas av de nya föreskrifterna även kan omfattas av ytterligare reglering inom säkerhetsområdet. De föreslagna föreskrifterna utesluter således inte att annan, tangerande lagstiftning, kan gälla för dessa nät och tjänster. Här kan framförallt säkerhetsskyddslagstiftningen och EU:s dataskyddsförordning nämnas.

[55] Man kan tänka på detta scenario som att, för två i övrigt lika produkter, med samma pris, efterfrågar konsumenterna mer av den säkrare produkten (alternativt att konsumenterna, för samma kvalitet i övrigt, är beredda att betala mer för en säkrare produkt). Detta resonemang skulle kunna gälla exempelvis säkra internetbetalningslösningar, vilka torde ha en högre efterfrågan än betalningslösningar med en lägre säkerhetsnivå.

Säkerhetsskydd

Tillhandahållare vars verksamhet helt eller delvis är säkerhetskänslig omfattas, utöver nya LEK och de föreslagna föreskrifterna, av säkerhetsskyddslagen (2018:585) och därtill hörande föreskrifter. Sådana tillhandahållare måste således, i förekommande fall, se till att uppfylla kraven i båda regelverken.

EU:s dataskyddsförordning

Tillhandahållare omfattas även i vissa delar av EU:s dataskyddsförordning.

E-dataskyddsdirektivet, som i huvudsak genomförs i nuvarande LEK, preciserar och kompletterar de allmänna bestämmelserna i EU:s dataskyddsförordning. EU:s dataskyddsförordning utgör en generell reglering för personuppgiftsbehandling inom EU.

Artikel 95 i EU:s dataskyddsförordning reglerar förhållandet till e-dataskydds-direktivet. EU:s dataskyddsförordning ska enligt artikeln inte innebära några ytterligare förpliktelser för fysiska eller juridiska personer som behandlar personuppgifter inom ramen för tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster i allmänna kommunikationsnät i unionen, när det gäller områden inom vilka de redan omfattas av särskilda skyldigheter för samma ändamål i enlighet med e-dataskyddsdirektivet.

Som ett förtydligande till artikeln anges i ingresspunkt 173 att förordningen bör vara tillämplig på alla frågor som gäller skyddet av grundläggande rättigheter och friheter i förhållande till behandlingen av personuppgifter, vilka inte omfattas av särskilda skyldigheter med samma mål som anges i direktivet om integritet och elektronisk kommunikation, däribland den personuppgiftsansvariges skyldigheter och fysiska personers rättigheter.

EU:s dataskyddsförordning ska således inte tillämpas där e-dataskyddsdirektivet innehåller särskilda bestämmelser som har samma syfte (i den engelska versionen ”*same objective set out*”).[56] I övriga delar är dock EU:s dataskyddsförordning tillämplig.

[56] E-dataskyddsdirektivet ska, enligt dess artikel 3, tillämpas på behandling av personuppgifter i samband med att allmänt tillgängliga elektroniska kommunikationstjänster tillhandahålls i allmänna kommunikationsnät inom unionen, inbegripet allmänna kommunikationsnät som stöder datainsamling och identifieringsutrustning.

11. Ekonomiska effekter för offentlig sektor

11.1 Kommuner och regioner

Kommuner och regioner kan tillhandahålla nät och tjänster. Till exempel är det vanligt att fiberbaserad bredbandsutbyggnad sker i kommunal regi, vanligen genom stadsnät, vilket gör att dessa är att se som tillhandahållare enligt både nuvarande och nya LEK.

De föreslagna föreskrifterna kommer således gälla för kommuner och regioner på samma sätt som andra företag som tillhandahåller nät och tjänster. De effekter av de föreslagna föreskrifterna som redovisas i denna konsekvensutredning gäller därmed även dessa aktörer. PTS bedömer emellertid att förslaget inte innebär några förändringar av kommunala befogenheter eller skyldigheter, respektive grunderna för kommunernas eller regionernas organisation eller verksamhetsformer.

11.2 Domstolar

De beslut som kommer fattas enligt nya LEK och de föreslagna föreskrifterna är väsentligen av samma slag som beslut som fattas enligt nuvarande reglering. Emellertid kommer den nya regleringen gälla ytterligare en kategori av tillhandahållare, de som tillhandahåller NI-ICS, vilket skulle kunna ge upphov till fler beslut hos PTS vilka kan överklagas till allmän förvaltningsdomstol. Det är mycket svårt att bedöma hur många beslut och eventuella överklaganden det skulle kunna bli fråga om i praktiken.

11.3 Integritetsskyddsmyndigheten

PTS och Integritetsskyddsmyndigheten kan behöva samverka kring informationsinsatser för att tydliggöra gränsdragningen mellan nya LEK och de nya föreskrifterna och EU:s dataskyddsförordning. Det är av vikt att tydliggöra vilka bestämmelser i de olika regelverken som gäller och hur de förhåller sig till varandra.

12. Miljömässiga och sociala effekter

De föreslagna föreskrifterna bedöms inte innebära några direkta sociala eller miljömässiga effekter.

Emellertid syftar de föreslagna föreskrifterna till att säkerställa att nät och tjänster är tillförlitliga och konfidentiella. Säkra elektroniska kommunikationer är något som stärker skyddet för slutanvändare och bidrar till att tilliten för kommunikationerna stärks. Elektroniska kommunikationer är en förutsättning för att det digitala samhället ska fungera och kunna utvecklas. Genom att säkerställa att nät och tjänster fungerar och är säkra bidrar det således generellt till att kunna möjliggöra digitaliseringen av samhället och säkerställa allas tillgång till kommunikationstjänster. Digitaliseringen kan påverka människors sätt att leva, bo, arbeta, förhålla sig till varandra och möjligheter att delta i samhället. Digitaliseringen är dessutom verktyg som kan användas för att minska miljöpåverkan och nå miljömål både lokalt, nationellt och globalt. I tillägg kan nämnas att de föreslagna föreskrifterna tar höjd för att de tekniska lösningar som är tillgängliga på marknaden vid en given tidpunkt ska beaktas, se vidare avsnitt 6.3. Avsikten är att framsteg i den tekniska utvecklingen ska avspeglas i de åtgärder som vidtas. Föreskriften låser således inte tillhandahållare vid användandet av viss teknik utan möjliggör och uppmuntrar på så sätt innovationer inom området. Smarta innovationer kan bidra till en positiv påverkan på miljön.

13. Sammantagen proportionalitetsbedömning

I avsnitt 6–12 redovisas konsekvenserna som följer av de föreslagna bestämmelserna i de nya föreskrifterna.

PTS bedömer genomgående att nyttan med de föreslagna bestämmelserna överstiger konsekvenserna som dessa medför. Mot bakgrund av den ökade användningen och det ökade beroendet av säker elektronisk kommunikation anser

PTS att dessa konsekvenser är rimliga. Bestämmelserna är således motiverade att införa.

Säkerhets- och integritetsincidenter drabbar både tillhandahållare, användare och samhället i stort varför samtliga gagnas av ett förebyggande säkerhetsarbete. Ett förebyggande säkerhetsarbete minskar risken för att incidenter inträffar och reducerar negativa konsekvenser av de incidenter som ändå inträffar. Det innebär positiva ekonomiska effekter då bl.a. kostnaderna för incidenter minskar. De föreslagna bestämmelserna är nödvändiga för att säkerställa att ett förebyggande säkerhetsarbete och en lämplig nivå av säkerhet upprätthålls, både i förhållande till riskerna för incidenter och i förhållande till samhällets behov av säker elektronisk kommunikation. För att läsa mer i detalj om vad som motiverar varje enskild bestämmelse, se vidare i avsnitt 6 om respektive krav.

PTS anser alltså att bestämmelserna leder till ökad säkerhet i nät och tjänster vilket generellt bedöms innebära mindre konsekvenser än om incidenter inträffar. Detta gör att frågan om alternativ till föreslagna bestämmelser i många fall handlar om ifall det är rimligt att ett krav ska ställas eller inte, snarare än att utreda olika alternativa lösningar.

14. Övrigt

14.1 Tidpunkt för ikraftträdande

De föreslagna föreskrifterna kompletterar skyldigheter i nya LEK och PTS föreslår att de föreslagna föreskrifterna ska träda i kraft samtidigt som den nya lagen, dvs. den 1 augusti 2022.

Föreskriften syftar till att uppnå en enhetlig tillämpning av skyldigheterna i nya LEK så att nät och tjänster är säkra vilket gör att det är angeläget att nya LEK och de nya föreskrifterna träder i kraft samtidigt. Det är vidare angeläget ur rättssäkerhets-synpunkt att det finns en tydlighet och förutsägbarhet i regleringen.

14.2 Underrättelse för anmälan till Europeiska kommissionen

I 6 § förordningen (1994:2029) om tekniska regler anges att en myndighet som avser fatta beslut om en teknisk regel som ska anmälas till Europeiska kommissionen i god tid ska underrätta Kommerskollegium om det förslag som den har utarbetat. Av 1 §

samma förordning framgår att bestämmelserna i förordningen ansluter till Sveriges internationella förpliktelser enligt bl.a. Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster (anmälningsdirektivet).

I artikel 1.3 anmälningsdirektivet anges att direktivet inte ska tillämpas på föreskrifter om frågor som omfattas av unionsbestämmelser för teletjänster som avses i ramdirektivet. Ramdirektivet har upphävts och ersatts av kodexen. Enligt artikel 125 i kodexen ska dock hänvisningar till bl.a. ramdirektivet anses som hänvisningar till kodexen. Bestämmelser som har sin grund i kodexen omfattas därmed inte av anmälningsskyldigheten.

Merparten av de föreslagna föreskrifterna innehåller bestämmelser om frågor som omfattas av kodexen. Enligt PTS bedömning är dessa bestämmelser därmed inte att se som sådana tekniska regler som ska underrättas enligt nämnda förordning.

Av ingresspunkt 19 och artikel 14 i e-dataskyddsdirektivet kan utläsas att åtgärder i enlighet med direktivet i vissa fall ska notifieras i enlighet med anmälningsdirektivet. När det gäller föreslagna bestämmelser som har sitt ursprung i e-dataskyddsdirektivet ser PTS att dessa möjligen är att betrakta som sådana tekniska regler som ska underrättas enligt förordningen om tekniska regler. PTS kommer därför att underrätta Kommerskollegium om de föreslagna föreskrifterna i dessa delar.

14.3 Informationsinsatser

Den förslagna föreskriften kommer att remitteras före det att beslut om föreskrifterna fattas. Berörda aktörer kommer då att få ta del av förslaget och få möjlighet att yttra sig över det.

När föreskriften beslutas kommer den ingå i PTS författningssamling och publiceras på myndighetens webbplats tillsammans med allmän information om föreskrifterna.

Dessutom kommer PTS i samband med ikraftträdandet av nya LEK att genomföra kommunikations- och utbildningsinsatser rörande regleringen i stort riktade till de aktörer som berörs av reglerna.

Det bedöms inte i övrigt finnas behov av några speciella informationsinsatser.

14.4 Kontaktuppgifter

Kontaktpersoner för sakfrågor:

Erika Hersaeus, erika.hersaeus@pts.se (uppdragsledare fr.o.m. extern remiss)

Johanna Eklund, johanna.eklund@pts.se (uppdragsledare fram till extern remiss)

Mikael Ejner, mikael.ejner@pts.se (it-säkerhetsspecialist)

Kontaktperson för juridiska frågor:

Ulrica Ljunggren, ulrica.ljunggren@pts.se

Bilaga Jämförelsetabell och bemyndiganden

De nya föreskrifterna	Bemyndig-anden i nya LEK	PTSFS 1995:1	PTSFS 2012:2	PTSFS 2012:4	PTSFS 2014:1	PTSFS 2015:2
3 kap. Övergripande säkerhetsarbete	1 kap. 11 §, 8 kap. 1, 5 och 6 §§	3 §		Delvis 3 §, st. 2 och 4 i allmänna råd till 3 § samt st. 1 i allmänna råd till 4 §	3 §	3 §
4 kap. Dokumentation av tillgångar, informations-behandlings-tillgångar, förbindelser och uppdragstagare	8 kap. 1, 5 och 6 §§				4 § st. 1	4 §
5 kap. Riskanalys	8 kap. 1, 5, 6 §§			St. 1 i allmänna råd till 3 §	4 § st. 2	5 och 5 a §§
6 kap. Riskhantering och åtgärder efter riskbedömning	8 kap. 1, 5, 6 §§			Delvis 3 § och delvis 5 §	4 § st. 3 (inklusive allmänna råd) samt delvis 8 § st. 2 och 3	9 – 12 §§
7 kap. Åtgärder avseende åtkomst och behörighet	8 kap. 1, 5, 6 §§			St. 3 i allmänna råd till 3 §, 4 §, st. 2 – 4 i allmänna råd till 4 § samt delvis 5 §.	5 och 6 §§ (inklusive allmänna råd till 5 §) samt delvis 8 § st. 2 och 3.	13 §
8 kap. Säkerhets-kopiering m.m.	8 kap. 1, 5 och 6 §§			7 § (allmänna rådet utgår dock)	8 § st. 1 och allmänna råd till 8 §	
9 kap. Loggning	8 kap. 1, 5 och 6 §§			6 § st. 1 och 2	7 §	
10 kap. Kryptering	8 kap. 1, 5 och 6 §§			6 § st. 3 och 4	9 §	

De nya föreskrifterna	Bemyndig-anden i nya LEK	PTSFS 1995:1	PTSFS 2012:2	PTSFS 2012:4	PTSFS 2014:1	PTSFS 2015:2
11 kap. Redundans och reservkraft-system samt ansökan om undantag	8 kap. 1 §					15 – 23 §§
12 kap. Åtgärder avseende övervakning och beredskap	8 kap. 1 §					14 §
13 kap. Intern incident-hantering	8 kap. 1, 5, 6 och 9 §§				10 och 11 §§	7 §
14 kap. Kontinuitets-planering	8 kap. 1 §					6 och 8 §§
15 kap. Fredstida planering för totalförsvarets behov av elektroniska kommunikationer.	1 kap. 11 §	2 och 3 §§				
16 kap. Information till användare om konkret och betydande hot om en incident	8 kap. 4 §					
17 kap. Rapportering av säkerhets-incidenter till PTS	8 kap. 3 §		3 – 9 §§			

Post- och telestyrelsens författningssamling

ISSN 1400-187X

Post- och telestyrelsens föreskrifter och allmänna råd om säkerhet i nät och tjänster;

PTSFSÅR:NR

Utkom från trycket den välj datum

beslutade den välj datum.

Post- och telestyrelsen föreskriver[1] följande med stöd av xx § förordningen (xxxx:xx) om elektronisk kommunikation och beslutar följande allmänna råd.

1 kap. Tillämpningsområde

1 § Dessa föreskrifter innehåller bestämmelser om

– de tekniska och organisatoriska åtgärder som enligt 8 kap. 1 § lagen (XXX) om elektronisk kommunikation ska vidtas för att hantera risker som hotar säkerheten i nät och tjänster,

– rapportering enligt 8 kap. 3 § lagen om elektronisk kommunikation av säkerhetsincidenter som har haft en betydande påverkan på kommunikationsnät och kommunikationstjänster,

– skyldigheten enligt 8 kap. 4 § lagen om elektronisk kommunikation för tillhandahållare att informera användare vid ett konkret och betydande hot om en säkerhetsincident,

– de särskilda tekniska och organisatoriska åtgärder som enligt 8 kap. 5 § lagen om elektronisk kommunikation ska vidtas i samband med lagring och annan behandling av uppgifter för brottsbekämpande ändamål,

– de tekniska och organisatoriska åtgärder som enligt 8 kap. 6 § lagen om elektronisk kommunikation ska vidtas för att säkerställa att uppgifter som behandlas i samband med tillhandahållandet av kommunikationstjänsten skyddas,

– innehållet i förteckningen över integritetsincidenter enligt 8 kap. 9 § lagen om elektronisk kommunikation, och

– fredstida planering enligt 1 kap. 11 § lagen om elektronisk kommunikation för totalförsvarets behov av elektroniska kommunikationer.

[1] Se Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster.

2 kap. Ord och uttryck

1 § Ord och uttryck i dessa föreskrifter har samma betydelse som i lagen (XXX) om elektronisk kommunikation och förordningen (XXX) om elektronisk kommunikation.

2 § I dessa föreskrifter avses med

aktiv anslutning: anslutning till kommunikationsnät eller kommunikationstjänst, som inte är en nummeroberoende interpersonell kommunikationstjänst, och som möjliggör omedelbar användning av kommunikationstjänster,

behandlade uppgifter: uppgifter som behandlas i samband med tillhandahållande av kommunikationsnät eller kommunikationstjänster,

fel i extern elförsörjning: störning eller avbrott i extern elförsörjning,

förbindelse: del av kommunikationsnät mellan två tillgångar eller mellan en tillgång och en anslutning till ett kommunikationsnät,

informationsbehandlingstillgångar: system, databaser och fysiska resurser som används för informationsbehandling,

kapacitetsbortfall: reducerad förmåga att tillhandahålla visst kommunikationsnät eller viss kommunikationstjänst angiven såsom andel i förhållande till normal nivå vid tillhandahållande av kommunikationsnätet eller kommunikationstjänsten eller som andel aktiva anslutningar eller användare, i förhållande till det totala antalet aktiva anslutningar eller användare för kommunikationsnätet eller kommunikationstjänsten, som till följd av avbrottet eller störningen inte kan nyttja tjänsten,

kommunikationsnät: sådant allmänt elektroniskt kommunikationsnät som avses i 1 kap. 7 § lagen (XXX) om elektronisk kommunikation,

kommunikationstjänst: sådan elektronisk kommunikationstjänst, som avses i 1 kap. 7 § lagen om elektronisk kommunikation,

kritisk komponent: del av en tillgång som är nödvändig för att sända, motta, bearbeta eller lagra information,

redundans: två eller flera, identiska eller olika, sätt att oberoende av varandra fylla samma funktion,

reservkraftsystem: system som oberoende av extern elförsörjning genererar elektricitet vid fel i den externa elförsörjningen,

session: pågående informationsöverföring mellan minst två parter genom en kommunikationstjänst,

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

tillhandahållare: den som tillhandahåller kommunikationsnät eller kommunikationstjänster,

uppdragstagare: den som anlitats av tillhandahållaren för att utföra installation, underhåll, felavhjälpning, drift eller liknande hantering av tillhandahållarens tillgångar, informationsbehandlingstillgångar och förbindelser,

vardag: dag som inte är lördag, söndag, midsommarafton, julafton, nyårsafton eller annan allmän helgdag.

3 kap. Övergripande säkerhetsarbete

1 § Tillhandahållarens säkerhetsarbete ska bedrivas långsiktigt, kontinuerligt och systematiskt. Arbetet ska omfatta såväl normala förhållanden som extraordinära händelser.

Allmänt råd till 1 §
Till stöd för det långsiktiga, kontinuerliga och systematiska säkerhetsarbetet bör tillhandahållaren utgå från etablerad standard på området, SS-ISO/IEC 27000-serien eller motsvarande.

2 § Tillhandahållaren ska i säkerhetsarbetet ha en tydlig rollfördelning med särskilt utpekade ansvariga för arbetet. Rollfördelningen ska dokumenteras.

3 § Tillhandahållaren ska upprätta, dokumentera och vid behov revidera de processer, rutiner och planer som anges i dessa föreskrifter. Tillhandahållaren ska dokumentera de tester som har utförts i enlighet med dessa föreskrifter.

4 § Tillhandahållaren ska säkerställa att anställda och uppdragstagare har kunskap om och tillämpar de processer, rutiner och planer som de är berörda av.

5 § Tillhandahållaren ska dokumentera de åtgärder som vidtas enligt 6 kap. 2–4 §§ och 7–12 kap. dessa föreskrifter samt följa upp dessa åtgärder årligen och vid behov.

Allmänt råd till 5 §
Vid uppföljning av sådana vidtagna åtgärder som avses ovan bör tillhandahållaren använda sig av erfarenheter och resultat från exempelvis genomförda tester. Penetrationstester bör användas som en del av säkerhetsarbetet för att följa upp de åtgärder som har vidtagits.

4 kap. Identifiering och dokumentation av tillgångar, informationsbehandlingstillgångar, förbindelser och uppdragstagare

1 § Tillhandahållaren ska identifiera och dokumentera samtliga sina tillgångar, informationsbehandlingstillgångar, förbindelser och uppdragstagare.

Tillhandahållaren ska för respektive tillgång, informationsbehandlingstillgång och förbindelse åtminstone dokumentera

1. en unik beteckning,
2. vilken funktion den har,
3. geografisk placering, om sådan finns,
4. en hänvisning till aktuell riskanalys enligt 5 kap. dessa föreskrifter, och
5. tillverkare.

För tillgångar ska även klass enligt 11 kap. dessa föreskrifter dokumenteras.

Tillhandahållaren ska för respektive uppdragstagare åtminstone dokumentera

1. uppdragstagarens namn, organisationsnummer och kontaktuppgifter, och
2. en beskrivning av uppdraget.

Dokumentationen ska hållas uppdaterad och varje version ska bevaras i fem år från det att den upprättats eller uppdaterats.

5 kap. Riskanalys

1 § Tillhandahållaren ska genomföra riskanalyser.

I en riskanalys ska tillhandahållaren analysera risken för att tillgångar, informationsbehandlingstillgångar eller förbindelser orsakar eller drabbas av säkerhets- eller integritetsincidenter. Riskanalyser ska göras för varje tillgång, informationsbehandlingstillgång och förbindelse.

Inför planerade förändringar ska tillhandahållaren i stället analysera risken för att förändringen orsakar en säkerhetsincident.

Allmänt råd till 1 §

För likvärdiga tillgångar, informationsbehandlingstillgångar och förbindelser kan en gemensam riskanalys göras.

2 § Riskanalyser ska genomföras minst en gång per år, samt

– inför planerade förändringar,

– i samband med att sådana säkerhetsincidenter som ska rapporteras enligt 17 kap. dessa föreskrifter har inträffat,

– inför upphandling av tillgångar, informationsbehandlingstillgångar, förbindelser och uppdragstagare, och

– efter att tidigare okända hot som är relevanta för riskanalysen identifierats.

Information om sådana hot som avses i första stycket kan förmedlas av Post- och telestyrelsen.

3 § Riskanalyserna ska innefatta åtminstone följande delar.

1. Identifiering av relevanta hot mot den aktuella tillgången, informationsbehandlingstillgången eller förbindelsen som kan leda till att en säkerhets- eller integritetsincident inträffar.

2. En bedömning av vilka konsekvenser som kan uppstå i händelse av att identifierade hot realiseras.

3. En bedömning av sannolikheten för att identifierade hot realiseras.

4. En sammanvägd bedömning av sannolikheten för att identifierade hot inträffar och de konsekvenser det kan medföra om de realiseras (riskbedömning).

Riskanalyser inför planerade förändringar ska i stället för första stycket 1 innefatta en identifiering av relevanta hot mot säkerheten i tillgångar och förbindelser med anledning av den planerade förändringen.

Allmänt råd till 3 §

Vid genomförandet av riskanalyser bör tillhandahållaren åtminstone analysera organisatoriska, logiska och fysiska hot.

En analys av organisatoriska hot bör åtminstone omfatta kritiska personberoenden, otillräcklig kompetensförsörjning, bristfällig incidenthantering, bristfällig behörighets- och åtkomsthantering samt bristfälliga processer för säkerhetsarbetet i övrigt.

En analys av logiska hot bör åtminstone omfatta kända sårbarheter i mjukvara, logiska överbelastningsattacker, logiska intrång, konfigurationsfel, fel och brister i hårdvara eller mjukvara (såväl egenutvecklad som utvecklad av annan) samt bristfällig segmentering av nätverk.

En analys av fysiska hot bör åtminstone omfatta hot relaterade till väder, klimatförändringar och den omgivande miljön, t.ex. nederbörd, brand, vind,

blixtnedslag, fukt, skadliga temperaturer, översvämningar, vattenläckor, samt ras, skred och erosion. Analysen av fysiska hot bör även omfatta intrång, sabotage och annan yttre påverkan, t.ex. anlagda bränder, stöld, kabelbrott och strömavbrott. Den bör även omfatta brist på utrustning och reservdelar till följd av bristande förmåga hos underleverantörer att säkra leveranser och beroenden av en enskild leverantör.

Riskanalysen bör innehålla en beskrivning av hur tillgångarna, informationsbehandlingstillgångarna eller förbindelserna kan påverkas i samband med att identifierade hot realiseras och hur detta kan påverka kommunikationsnät och kommunikationstjänster.

4 § Vid genomförande av riskanalyser ska tillhandahållaren beakta erfarenheter från tidigare inträffade säkerhets- och integritetsincidenter, allmänt uppmärksammade säkerhets- och integritetsincidenter samt aktuella och relevanta omvärldsföreteelser.

Vid genomförande av riskanalyser ska tillhandahållaren tillämpa processer som utgår från etablerad standard på området.

Tillhandahållaren ska ha en plan för vid vilka tidpunkter och i vilka situationer tillhandahållaren kommer att genomföra riskanalyser.

Tillhandahållaren ska dokumentera genomförda riskanalyser.

6 kap. Riskhantering och åtgärder efter riskbedömning

Riskhantering

1 § Tillhandahållaren ska utifrån riskbedömningen besluta hur respektive risk ska hanteras genom att avgöra om riskerna ska undvikas, reduceras eller accepteras. Sådana beslut ska dokumenteras. Beslut om att acceptera en risk ska även motiveras.

Allmänt råd till 1 §
Tillhandahållare bör alltid eftersträva att reducera risker framför att acceptera dem. Tillhandahållare bör endast acceptera risker om säkerheten i nät och tjänster i stort kan upprätthållas trots att hotet förverkligas eller incidenten inträffar.

Åtgärder efter riskbedömning

2 § Tillhandahållaren ska vidta tekniska och organisatoriska åtgärder för att hantera de risker som ska undvikas eller reduceras. Åtgärderna ska vidtas på en nivå som är anpassad till den risk som föreligger, med beaktande av tillgänglig teknik och kostnaderna för åtgärderna.

Första stycket andra meningen gäller inte för sådana uppgifter som lagras för brottsbekämpande ändamål enligt 9 kap. 19 § lagen (XXX) om elektronisk kommunikation. Tillhandahållaren ska för sådana uppgifter vidta åtgärder i enlighet med [37 § förordningen (2003:396) om elektronisk kommunikation].

Allmänt råd till 2 §
Tillhandahållarens åtgärder bör följa etablerad standard, normer, praxis och säkerhetsvägledningar.

3 § Tillhandahållarens bedömning vid val av åtgärder ska dokumenteras samt följas upp årligen och vid behov.

4 § När tillhandahållarens riskanalys enligt 5 kap. dessa föreskrifter visar att det finns risker för att planerade förändringar kan orsaka rapporteringspliktiga säkerhetsincidenter enligt 17 kap. dessa föreskrifter ska tillhandahållaren utöver vad som följer av 2 § åtminstone

– utföra tester inför förändringen och efter förändringen verifiera att den inte påverkat säkerheten negativt,

– säkerhetskonfigurera (härda) berörda tillgångar, samt

– ta fram planer för att återställa kommunikationsnätet och kommunikationstjänsten i händelse av att en säkerhetsincident inträffar.

Tester, härdning, och planer för återställande ska vara anpassade till den planerade förändringens art och omfattning.

Tillhandahållaren ska tillämpa en process vid genomförande av planerade förändringar (förändringshantering) som utgår från etablerad standard på området.

7 kap. Åtgärder avseende åtkomst och behörighet

1 § Tillhandahållaren ska medge åtkomst till tillgångar och behandlade uppgifter endast till den som är behörig. Tillhandahållaren ska tilldela sådan behörighet endast till de anställda eller uppdragstagare som behöver det för att kunna utföra sina arbetsuppgifter.

Tillhandahållaren ska tillämpa en process för tilldelning, ändring och uppföljning av tilldelade behörigheter enligt första stycket. Tilldelade behörigheter ska dokumenteras samt följas upp årligen och vid behov.

Tillhandahållaren ska ha system för hantering och kontroll av identiteter och behörigheter.

Tillhandahållaren ska säkerställa att åtkomst endast ges till den som har upplysts om tystnadsplikten i de fall 9 kap. 31 och 32 §§ lagen (XXX) om elektronisk kommunikation är tillämpliga.

Allmänt råd till 1 §

Tillhandahållaren bör se till att den som kommer i kontakt med behandlade uppgifter regelbundet får utbildning och information om när och hur behandlade uppgifter får hanteras. Den som kommer i kontakt med behandlade uppgifter bör även få utbildning i att upptäcka integritetsincidenter och att analysera tänkbara konsekvenser av en inträffad integritetsincident för abonnenter och användare.

Tilldelade behörigheter bör vara begränsade i tid och omfattning, särskilt för tillfälliga uppdragstagare. Tilldelade behörigheter bör tas bort efter utfört uppdrag.

8 kap. Säkerhetskopiering m.m.

1 § Tillhandahållaren ska vidta åtgärder för att säkerställa att behandlade uppgifter som varaktigt lagras skyddas mot oavsiktlig eller otillåten utplåning eller förlust.

Allmänt råd till 1 §
Säkerställande av skydd mot oavsiktlig eller otillåten utplåning eller förlust bör ske genom säkerhetskopiering. Återläsning av säkerhetskopior bör verifieras åtminstone årligen.

2 § Uppgifter som lagras för brottsbekämpande ändamål enligt 9 kap. 19 § lagen (XXX) om elektronisk kommunikation ska i stället för vad som framgår av 1 § skyddas mot oavsiktlig eller otillåten utplåning samt oavsiktlig förlust eller ändring genom lagring på minst två fysiskt åtskilda platser.

Första stycket gäller även loggen enligt 9 kap. 1 § dessa föreskrifter avseende åtkomst till uppgifter som ska lagras för brottsbekämpande ändamål.

Säkerhetskopior eller motsvarande ska omfattas av samma skydd och utplånas samtidigt som de uppgifter som lagras för brottsbekämpande ändamål.

Allmänt råd till 2 §
Skydd för uppgifter som lagras för brottsbekämpande ändamål kan uppnås genom redundant lagring, säkerhetskopiering eller liknande.

9 kap. Loggning

1 § Tillhandahållaren ska logga

1. all läsning, kopiering, ändring och utplåning av behandlade uppgifter, och
2. åtkomst till de system som används för behandling av sådana uppgifter.

Loggning ska ske på ett sådant sätt att det går att se vem som har vidtagit vilken åtgärd med vilka uppgifter och vid vilken tidpunkt. Vid misstanke om att en integritetsincident har inträffat ska relevanta loggar alltid kontrolleras.

Tillhandahållaren ska ha rutiner för kontroll av loggar. Kontroller av loggar ska ske systematiskt och återkommande. Genomförda kontroller av loggar ska dokumenteras.

2 § Tillhandahållaren ska logga systemhändelser nödvändiga för att kunna utreda säkerhetsincidenter.

Allmänt råd till 1 och 2 §§
Tillhandahållaren bör tillämpa automatisk övervakning av loggar, i syfte att snabbt upptäcka onormala användarmönster, händelser eller serier av händelser. Detta gäller dock inte för loggar avseende åtkomst till uppgifter som ska lagras för brottsbekämpande ändamål enligt 9 kap. 19 § lagen (XXX) om elektronisk kommunikation.

3 § Den som är skyldig att lagra uppgifter för brottsbekämpande ändamål enligt 9 kap. 19 § lagen (XXX) om elektronisk kommunikation ska säkerställa att den som har haft tillgång till sådana uppgifter inte ges tillgång till loggen avseende åtkomst till uppgifterna.

4 § Innan uppgifter som lagras för brottsbekämpande ändamål utplånas i enlighet med 9 kap. 22 § lagen (XXX) om elektronisk kommunikation ska tillhandahållaren utföra en systematisk kontroll av loggen avseende åtkomst till uppgifterna. I samband med att uppgifterna utplånas ska även loggar utplånas.

10 kap. Kryptering

1 § Behandlade uppgifter som överförs via internet ska skyddas genom kryptering, om inte risken för säkerheten i nät och tjänster och för behandlade uppgifter efter en riskanalys bedöms vara låg.

Allmänt råd till 1 §
Behovet av kryptering och vilken nivå av säkerhet som ska eftersträvas bör avgöras av riskanalysen. Vid bedömning av risken bör hänsyn tas till typ och mängd av uppgifter.

Koder, lösenord och sammanställningar av uppgifter som rör en användare eller abonnent bör krypteras vid överföring via internet.

2 § Anslutningar för konfigurering och styrning av tillgångar via internet eller kommunikationsnät som andra än tillhandahållaren har rådighet över ska skyddas genom kryptering.

3 § Loggar avseende åtkomst till uppgifter som lagras för brottsbekämpande ändamål enligt 9 kap. 19 § lagen (XXX) om elektronisk kommunikation ska skyddas genom kryptering under lagring och överföring.

4 § Kryptering ska ske med en allmänt erkänd krypteringsmetod med tillräcklig nyckellängd. Krypteringsnycklar ska hanteras på ett säkert sätt.

5 § Tillhandahållaren ska ha rutiner för kryptering och hantering av krypteringsnycklar.

11 kap. Redundans och reservkraftsystem

Klassificering av tillgångar

1 § Tillgångar vars funktioner är nödvändiga för att tillhandahålla ett kommunikationsnät eller en kommunikationstjänst som inte är en nummeroberoende interpersonell kommunikationstjänst indelas i följande fem klasser utifrån det antal aktiva anslutningar som kan drabbas av en säkerhetsincident som innebär störning eller avbrott till följd av att tillgången upphör att fungera normalt.

Klass	Antal aktiva anslutningar
A	≥ 200 000
B	≥ 30 000
C	≥ 8 000
D	≥ 2 000
E	> 0

Allmänt råd till 1 §
Antalet aktiva anslutningar i mobila accessnät bör beräknas som antalet samtidigt möjliga aktiva anslutningar till basstationen, det vill säga det maximala antalet samtidiga användare av respektive basstation.

2 § Tillgångar vars funktioner är nödvändiga för att tillhandahålla en nummeroberoende interpersonell kommunikationstjänst och som en tillhandahållare av sådan tjänst utövar direkt kontroll över indelas i följande två klasser utifrån uppskattat antal användare i Sverige som kan drabbas av en säkerhetsincident som innebär störning eller avbrott till följd av att tillgången upphör att fungera normalt.

Klass	Antal drabbade användare
A	≥ 200 000
B	≥ 30 000

Åtgärder efter klassificering av tillgångar

Redundans av tillgångar i klasserna A och B

3 § Tillhandahållaren ska med redundanta tillgångar säkerställa att tillgångar i klasserna A och B som upphör att fungera inte orsakar störning eller avbrott i en kommunikationstjänst. Sådan störning eller avbrott som består i att sessioner avbryts är dock tillåten, om användare omedelbart kan upprätta nya sessioner.

Kravet i första stycket gäller endast om det är tekniskt tillämpbart.

Redundanta tillgångar i klass A ska vara placerade i geografiskt lämpligt separerade områden.

Redundans av tillgångar i klass C

4 § Tillhandahållaren ska med redundanta tillgångar eller redundanta kritiska komponenter säkerställa att tillgångar i klass C som upphör att fungera inte orsakar störning eller avbrott i en kommunikationstjänst. Sådan störning eller avbrott som består i att sessioner avbryts är dock tillåten, om användare omedelbart kan upprätta nya sessioner.

Säkerställande av tillgångar i klass D

5 § Tillhandahållaren ska säkerställa att kritiska komponenter i en tillgång i klass D som upphör att fungera, inte orsakar störning eller avbrott i en kommunikationstjänst som överstiger 12 timmar om störningen eller avbrottet inträffar en vardag och 18 timmar om störningen eller avbrottet inträffar under övrig tid.

Redundans av förbindelser mellan tillgångar i klasserna A, B och C

6 § Tillhandahållaren ska med redundanta förbindelser mellan samtliga tillgångar inom och mellan klasserna A, B och C säkerställa att förbindelser som upphör att fungera inte orsakar störning eller avbrott i en kommunikationstjänst. Sådan störning eller avbrott som består i att sessioner avbryts är dock tillåten, om användare omedelbart kan upprätta nya sessioner.

Redundanta förbindelser mellan samtliga tillgångar inom och mellan klasserna A och B ska vara geografiskt lämpligt separerade. Detta gäller inte förbindelser mellan tillgångar inom samma anläggning.

Säkerställande av förbindelser mellan en tillgång i klass D och tillgångar i klasserna A, B och C

7 § Tillhandahållaren ska säkerställa att förbindelser mellan en tillgång i klass D och en tillgång i klasserna A, B eller C som upphör att fungera, inte orsakar störning eller avbrott i en kommunikationstjänst som överstiger 12 timmar om störningen eller avbrottet inträffar en vardag och 18 timmar om störningen eller avbrottet inträffar under övrig tid.

Reservkraftsystem avseende tillgångar i klasserna A, B, C och D

8 § Tillhandahållaren ska med reservkraftsystem säkerställa att fel i extern elförsörjning inte orsakar störning eller avbrott i de kommunikationsnät och kommunikationstjänster som denne tillhandahåller, under åtminstone

1. 24 timmar för tillgångar i klasserna A och B,
2. 8 timmar för tillgångar i klass C i tätort med fler än 8 000 invånare,
3. 12 timmar för tillgångar i klass C på övriga platser,
4. 2 timmar för tillgångar i klass D i tätort med fler än 8 000 invånare, samt
5. 4 timmar för tillgångar i klass D på övriga platser.

Tiden beräknas från det att felet i den externa elförsörjningen inträffade.

Om det inträffar ett fel i extern elförsörjning mindre än fyra timmar efter ett tidigare, avseende samma tillgång, anses det utgöra samma fel.

Tillhandahållaren ska utföra funktionstest av reservkraftsystem varje kvartal för tillgångar i klasserna A, B och C, samt varje år för tillgångar i klass D.

Tillhandahållaren ska årligen utföra test av reservkraftsystem genom att bryta den externa elförsörjningen eller motsvarande till tillgångar i klasserna A, B och C.

Tillhandahållaren ska tillämpa processer för planering, inrättande, tester, underhåll och utbyte av reservkraftsystem.

Reservkraftsystem avseende mobila kommunikationsnät och kommunikationstjänster

9 § Tillhandahållare av mobila kommunikationsnät och mobila kommunikationstjänster ska med reservkraftsystem, utöver vad som följer av 8 §, säkerställa att fel i extern elförsörjning inte orsakar störning eller avbrott i kommunikationsnät och kommunikationstjänster som denne tillhandahåller eller minskar kommunikationstjänsters täckningsområde, under åtminstone en timme i tätort med fler än 8 000 invånare och fyra timmar på övriga platser, från det att felet i extern elförsörjning inträffade. Fel i extern elförsörjning som inträffar med mindre än fyra timmars mellanrum avseende samma fysiska tillgång ska anses utgöra ett fel.

Tillhandahållaren får under felets varaktighet, om det är nödvändigt för att upprätthålla kommunikationstjänster under den tid som anges i första stycket och under förutsättning att täckningsområdet bibehålls, minska tillgångarnas elförbrukning genom att begränsa antalet frekvensband som används för kommunikationstjänsterna.

Tillhandahållaren ska tillämpa processer för planering, inrättande, underhåll och utbyte av reservkraftsystem.

Ansökan om undantag från 3–9 §§

10 § Post- och telestyrelsen kan, efter skriftlig ansökan från en tillhandahållare, medge undantag från krav på åtgärd enligt 3–9 §§ om i det enskilda fallet dess tillämpning skulle få konsekvenser som är

1. oproportionerliga i förhållande till kostnader förenade med åtgärden,
2. olämpliga med hänsyn till tillgänglig teknik,
3. olämpliga med hänsyn till annan reglering, eller
4. oproportionerliga med hänsyn till att berörda tillgångar eller förbindelser omfattas av beslut om avveckling.

11 § I de fall undantag medges ska tillhandahållaren vidta lämpliga alternativa åtgärder för att begränsa negativa effekter av att den föreskrivna åtgärden inte vidtas.

12 § Tillhandahållaren ska i ansökan redogöra för vilka åtgärdskrav ansökan avser, varför åtgärden är oproportionerlig eller olämplig samt vilka alternativa och begränsande åtgärder enligt 11 § som tillhandahållaren avser att vidta. Ansökan ska även innehålla en bedömning av hur säkerheten i nät och tjänster påverkas av att föreskrivna åtgärder inte vidtas.

12 kap. Åtgärder avseende övervakning och beredskap

1 § Tillhandahållaren ska kontinuerligt övervaka kommunikationstjänster och aktiva delar i kommunikationsnät för att kunna förebygga, upptäcka och åtgärda säkerhetsincidenter.

Tillhandahållaren ska ha system som skapar larm vid säkerhetsincidenter som innebär störningar eller avbrott.

Tillhandahållaren ska dygnet runt kunna initiera relevanta åtgärder för att hantera säkerhetsincidenter.

13 kap. Intern incidenthantering

1 § Tillhandahållaren ska säkerställa att

1. inträffade säkerhets- eller integritetsincidenter rapporteras internt,
2. åtgärder vidtas skyndsamt för att hantera en uppkommen säkerhets- eller integritetsincident,
3. åtgärder vidtas för att undvika liknande säkerhets- eller integritetsincidenter, och
4. erfarenheter från inträffade säkerhets- eller integritetsincidenter beaktas vid genomförande av riskanalyser enligt 5 kap. dessa föreskrifter.

Vid åtgärder enligt första stycket (incidenthantering) ska tillhandahållaren tillämpa processer som utgår från etablerad standard på området.

Tillhandahållare av kommunikationstjänster ska också ha rutiner för identifiering av integritetsincidenter.

2 § Vid integritetsincidenter ska den som tillhandahåller en kommunikationstjänst löpande föra en förteckning i enlighet med 8 kap. 9 § lagen (XXX) om elektronisk kommunikation. Förteckningen ska innehålla

1. datum då integritetsincidenten inträffade,
2. en beskrivning av integritetsincidenten,

3. uppskattat antal berörda abonnenter eller användare,
4. bedömda konsekvenser av integritetsincidenten,
5. orsak till att integritetsincidenten inträffade,
6. de åtgärder som vidtagits, och
7. referensnummer.

14 kap. Kontinuitetsplanering

1 § Tillhandahållaren ska identifiera de verksamhetsdelar och resurser som är nödvändiga för att kunna begränsa omfattande säkerhetsincidenter i form av störningar eller avbrott. Tillhandahållaren ska analysera vilka konsekvenser som kan uppstå när dessa verksamhetsdelar och resurser helt eller delvis blir otillgängliga. Analysen ska omfatta en bedömning av när kontinuitetsplaner enligt 2 § detta kapitel ska tillämpas.

Konsekvensanalysen enligt första stycket ska dokumenteras och revideras vid behov.

Allmänt råd till 1 §
En sådan verksamhetsdel och resurs som avses i 1 § kan t.ex. vara en central databas över användare som, om den slutar att fungera, omöjliggör användandet av tjänsten. En sådan verksamhetsdel kan även utgöras av personella resurser som på grund av sin befattning, roll, funktion eller kunskap inom ett visst område är nödvändiga för att verksamheten ska fungera. Även en underleverantör av för tillhandahållaren helt nödvändig utrustning kan utgöra en sådan verksamhetsdel.

2 § Tillhandahållaren ska upprätta kontinuitetsplaner utifrån konsekvensanalysen i 1 §. Kontinuitetsplanerna ska åtminstone innehålla

1. de åtgärder som ska vidtas för att begränsa de konsekvenser som kan uppstå enligt konsekvensanalysen och för att återställa påverkade verksamhetsdelar eller resurser till normal funktionsförmåga,
2. när och hur kontinuitetsplanerna ska övas, samt
3. när och hur kontinuitetsplanerna ska revideras.

Tillhandahållaren ska utgå från etablerad standard på området vid framtagande av kontinuitetsplanerna.

Tillhandahållaren ska öva planerna minst vartannat år.

Allmänt råd till 2 §
Tillhandahållaren bör vid sitt framtagande av kontinuitetsplaner utgå från SS-EN ISO 22301 Ledningssystem för kontinuitetshantering eller motsvarande.

3 § Kontinuitetsplanerna ska tillämpas i enlighet med bedömningen i konsekvensanalysen.

15 kap. Fredstida planering för totalförsvarets behov av elektroniska kommunikationer

1 § Den som tillhandahåller ett kommunikationsnät eller en kommunikationstjänst som inte är en nummeroberoende interpersonell kommunikationstjänst ska utifrån

konsekvensanalysen enligt 14 kap. 1 § dessa föreskrifter även ta fram kontinuitetsplaner för höjd beredskap och krig. Sådana kontinuitetsplaner ska uppfylla kraven som framgår av 14 kap. 2 § första och andra stycket.

2 § Post- och telestyrelsen kan i fredstid komma att informera tillhandahållare om
– vilka verksamhetsdelar och resurser som är kritiska för totalförsvarets behov av elektroniska kommunikationer vid höjd beredskap och i krig, och
– vad kontinuitetsplanerna ska innehålla för att tillgodose totalförsvarets behov av elektroniska kommunikationer vid höjd beredskap och i krig.

När Post- och telestyrelsen förmedlar information enligt första stycket ska tillhandahållaren revidera sina kontinuitetsplaner i enlighet med informationen.

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

16 kap. Information till användare om konkret och betydande hot om en säkerhetsincident

1 § Tillhandahållaren ska informera användare som kan komma att påverkas av ett konkret och betydande hot om en säkerhetsincident så snart som möjligt efter att hotet har upptäckts, för att användarna så snart som möjligt ska kunna vidta de skydds- eller motåtgärder som rekommenderas av tillhandahållaren.

Allmänt råd till 1 §
Tillhandahållaren bör försäkra sig om att informationen verkligen når ut till berörda användare. Informationen bör lämnas på ett säkert sätt så att inte informationen i sig ger upphov till nya säkerhetsincidenter. Informationen bör, om det är möjligt och lämpligt, beskriva den risk som hotet innebär och vad konsekvenserna kan bli om användarna inte vidtar rekommenderade åtgärder.

17 kap. Rapportering av säkerhetsincidenter till Post- och telestyrelsen

1 § Tillhandahållaren ska till Post- och telestyrelsen rapportera sådana säkerhetsincidenter som anges i 5–7 §§ detta kapitel.

Rapportering

2 § Vid incidentrapportering enligt 8 kap. 3 § lagen (XXX) om elektronisk kommunikation ska tillhandahållaren lämna en inledande och en kompletterande rapport till Post- och telestyrelsen.

Allmänt råd till 2 §
Rapporterna bör lämnas i elektronisk form.

Inledande rapport

3 § Den inledande rapporten ska vara Post- och telestyrelsen till handa inom 72 timmar från det att säkerhetsincidenten upptäcktes och innehålla följande uppgifter:

1. när säkerhetsincidenten inträffade,
2. hur länge säkerhetsincidenten har pågått,
3. vilka kommunikationsnät eller kommunikationstjänster som har berörts av störningen eller avbrottet,
4. säkerhetsincidentens omfattning,
5. tillhandahållarens preliminära bedömning av orsaken till säkerhetsincidenten,
6. hur säkerhetsincidenten har påverkat berörda aktiva anslutningar eller användare i Sverige,
7. om säkerhetsincidenten har medfört begränsningar i möjligheten till nödkommunikation via det kommunikationsnät eller den kommunikationstjänst som berörts av säkerhetsincidenten, och
8. tillhandahållarens kontaktuppgifter och referensnummer för ärendet.

Allmänt råd till 3 §

Tillhandahållaren bör göra en uppskattning av tidpunkten för när säkerhetsincidenten har inträffat i de fall en exakt tidpunkt inte kan fastställas med stöd av system för övervakning eller loggning. Uppskattningen bör göras med utgångspunkt från kända fakta om incidenten.

Redogörelsen för vilka kommunikationsnät eller kommunikationstjänster som säkerhetsincidenten har omfattat bör innehålla såväl uppgifter om de berörda nätteknologierna, som uppgift om berörda slutanvändartjänster, till exempel rösttelefoni eller internetanslutning.

Antalet aktiva anslutningar i mobila accessnät bör beräknas som antalet samtidigt möjliga aktiva anslutningar till basstationen, det vill säga det maximala antalet samtidiga användare av respektive basstation.

Redogörelsen för säkerhetsincidenten bör innehålla en beskrivning av på vilket sätt och i vilken utsträckning tjänstens eller nätets funktionalitet försämrades.

Kompletterande rapport

4 § Den kompletterande rapporten ska vara Post- och telestyrelsen till handa inom två veckor från det att den inledande rapporten lämnades. Anstånd kan beviljas.

Rapporten ska innehålla följande uppgifter:

1. komplettering och uppdatering av uppgifterna som lämnats i den inledande rapporten,
2. orsakerna till säkerhetsincidenten,
3. vilken information som har lämnats till allmänheten och berörda personer samt när och hur denna information lämnades,
4. de åtgärder som har vidtagits för att minimera effekterna av säkerhetsincidenten inför slutligt avhjälpande,
5. de åtgärder som har vidtagits för att avhjälpa de fel och brister som orsakat säkerhetsincidenten med angivande av när åtgärderna vidtogs,
6. de åtgärder som har vidtagits och som planeras för att undvika liknande säkerhetsincidenter, med angivande av när dessa åtgärder vidtogs eller bedöms vara genomförda, och
7. referensnummer för ärendet.

Allmänt råd till 4 §
Tillhandahållarens redogörelse för orsakerna till säkerhetsincidenten bör beskriva samtliga kända omständigheter som har eller kan ha bidragit till att incidenten inträffade.

Tröskelvärden för rapportering

5 § En säkerhetsincident som innebär störning eller avbrott i tillhandahållna kommunikationsnät eller kommunikationstjänster är rapporteringspliktig under följande förutsättningar.

Tid som incidenten pågått	*Incidentens uppskattade omfattning*
≥ 1 timme	≥ 150 000 användare eller aktiva anslutningar i Sverige, ≥ 50 % kapacitetsbortfall eller ≥ 15 000 km² sammanhängande berört område
≥ 2 timmar	≥ 30 000 användare eller aktiva anslutningar i Sverige, ≥ 30 % kapacitetsbortfall eller ≥ 5 000 km² sammanhängande berört område
≥ 6 timmar	≥ 5 000 användare eller aktiva anslutningar i Sverige, ≥ 20 % kapacitetsbortfall eller ≥ 2 500 km² sammanhängande berört område
≥ 24 timmar	≥ 2 000 användare eller aktiva anslutningar i Sverige, ≥ 10 % kapacitetsbortfall eller ≥ 1 000 km² sammanhängande berört område

Allmänt råd till 5 §
Berört område för kommunikationstjänster som tillhandahålls över mobila nätanslutningar bör normalt vara det sammanlagda täckningsområdet för berörda celler eller motsvarande i mobilnätet.

Kapacitetsbortfall bör till exempel kunna beräknas som andelen berörda användare eller aktiva anslutningar i förhållande till det totala antalet användare eller aktiva anslutningar för kommunikationstjänsten, eller, andel misslyckade samtalsförsök.

6 § Utöver vad som framgår av 5 § är en säkerhetsincident rapporteringspliktig om den har haft en betydande påverkan på nätets eller tjänstens funktion eller funktioner i samhället.

---

1. Dessa föreskrifter träder i kraft den 1 augusti 2022.
2. Genom föreskrifterna upphävs
a) Post- och telestyrelsens föreskrifter (PTSFS 1995:1) om fredstida planering för totalförsvarets behov av telekommunikation m.m.
b) Post- och telestyrelsens föreskrifter och allmänna råd (PTSFS 2012:2) om

rapportering av störningar eller avbrott av betydande omfattning,
c) Post- och telestyrelsens föreskrifter och allmänna råd (PTSFS 2012:4) om skyddsåtgärder i samband med lagring och annan behandling av uppgifter för brottsbekämpande ändamål,
d) Post- och telestyrelsens föreskrifter och allmänna råd (PTSFS 2014:1) om skyddsåtgärder för behandlade uppgifter,
e) Post- och telestyrelsens föreskrifter (PTSFS 2015:2) om krav på driftsäkerhet.

På Post- och telestyrelsens vägnar

DAN SJÖBLOM

Karolina Asp