Avdelningen för säker kommunikation

Konsekvensutredning avseende ändring av föreskrifter om krav på driftsäkerhet

Post- och telestyrelsen (PTS) avser att med stöd av 30 § förordningen (2003:396) om elektronisk kommunikation revidera föreskrifter avseende tekniska och organisatoriska åtgärder för att säkerställa att verksamheten uppfyller rimliga krav på driftsäkerhet, nedan kallade ändringsföreskrifterna.

PTS redovisar härmed sin utredning enligt förordning (2007:1244) om konsekvensutredning vid regelgivning.

Sammanställning av uppskattning av kostnader, se Bilaga 1.

Förslag till föreskrifter bifogas, se Bilaga 2.

Post- och telestyrelsen

Postadress:
Box 5398
102 49 Stockholm

Besöksadress:
Valhallavägen 117 A
www.pts.se

Telefon: 08-678 55 00
Telefax: 08-678 55 05
pts@pts.se

Innehåll

1 Inledning

PTS är sektorsmyndighet för området elektronisk kommunikation i Sverige.

Enligt 5 kap. 6 b § lagen (2003:389) om elektronisk kommunikation (LEK) ska den som tillhandahåller elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att verksamheten uppfyller rimliga krav på driftsäkerhet.

Enligt 30 § förordningen (2003:396) om elektronisk kommunikation får PTS utfärda föreskrifter om på vilket sätt skyldigheten enligt 5 kap. 6 b § LEK ska fullgöras. I juni 2015 beslutade PTS om sådana föreskrifter med krav på driftsäkerhet (PTSFS 2015:2).

Syftet med föreskrifterna är främst att förtydliga vilka tekniska och organisatoriska åtgärder som tillhandahållare ska vidta för att säkerställa en rimlig nivå av driftsäkerhet vid tillhandahållande av allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster. Syftet med de nu föreslagna ändringsföreskrifterna till PTS föreskrifter med krav på driftsäkerhet är att på lämpligt sätt hantera vissa risker som aktualiserats sedan föreskrifterna beslutades. Dessa risker relaterar bl.a. till utbyggnaden av 5G-nät i Sverige och risker förknippade med att samhället blir alltmer beroende av säkra elektroniska kommunikationsnät och -tjänster.

I den fortsatta framställningen används begreppen ”kommunikationsnät” eller ”nät” synonymt med begreppet ”allmänt kommunikationsnät”, definierat i LEK. Vidare används begreppen ”kommunikationstjänst” eller ”tjänst” synonymt med begreppet ”elektronisk kommunikationstjänst”, även detta definierat i LEK. Med ”tillhandahållare” avses nedan såväl tillhandahållare av nät som av tjänster.

2 Beskrivning av problemet och vad PTS vill uppnå

PTS har bl.a. till uppgift att främja tillgången till säkra och effektiva elektroniska kommunikationer. Allt fler tjänster och samhällsfunktioner förlitar sig på fungerande elektroniska kommunikationstjänster och -nät, samtidigt som vårt alltjämt ökande beroende till elektronisk kommunikation innebär risker för samhället om tjänsterna och näten inte är tillräckligt säkra. Tjänsterna och näten kan exempelvis utgöra potentiella måltavlor för säkerhetsattacker, såsom sabotage, med stora samhälleliga negativa konsekvenser som följd.

2.1 Utbyggnad av 5G

Under de senaste månaderna har flera länder beslutat om åtgärder för att hantera risker kopplade till t.ex. användandet av underleverantörer vars utrustning har bedömts kunna utnyttjas för diverse säkerhetsangrepp. Frågan har inte minst aktualiserats i och med att tillhandahållare inom kort förväntas genomföra omfattande investeringar i ny utrustning för utbyggnad och säkerställande av 5G-funktionalitet, inklusive underliggande infrastruktur såsom fibernät etc. För svensk del beräknas utbyggnaden ta fart efter den frekvenstilldelning som är planerad till början av 2020.

De elektroniska kommunikationsnäten och -tjänsterna består av ett lapptäcke av teknisk utrustning, underleverantörsförhållanden och horisontella samarbeten och beroenden. Den tekniska utrustning som tillhandahållare investerar i för framtida behov – såsom införandet av 5G - kommer inte att vara autonoma eller avgränsade i förhållande till den idag befintliga infrastrukturen. Eftersom näten och tjänsterna inte är säkrare än sin svagaste länk omfattar säkerhetsproblematiken samtliga tillhandahållare, och såväl framtida som befintlig infrastruktur.

5G-näten förväntas innebära stora förändringar i vår användning av elektronisk kommunikation. Bland annat kommer det så kallade ”internet of things” eller på svenska ”sakernas internet” att få en allt större och viktigare roll i samhället. Fler och fler saker kommer att vara uppkopplade och kommunicera med varandra, hastigheterna i näten kommer avsevärt att öka m.m. De nya, breda användningsområdena som 5G förväntas möjliggöra innebär dock att samhället blir mer sårbart för det fall att näten och tjänsterna inte fungerar, eller på annat sätt är osäkra, i takt med att samhället blir mer digitalt. Dessa risker behöver, enligt PTS bedömning, hanteras så snart som möjligt.

EU har också vidtagit åtgärder inom området och rekommenderat medlemsstaterna att bl.a. ta fram nationella riskanalyser, som ska ligga till grund för gemensamma verktyg och skyddsåtgärder inom unionen. PTS har, med hjälp av ett flertal tillfrågade marknadsaktörer, haft uppdraget att ta fram ett förslag till Sveriges riskanalys, vars slutsatser delvis ligger till grund för PTS

bedömning av att kraven på driftsäkerhet kopplat till utrullningen av 5G i Sverige behöver skärpas[1].

2.2 Problemområden

I den nationella riskanalysen som PTS nyligen varit med om att ta fram lyfts särskilt ett antal problemområden som de föreslagna ändringarna till viss del ämnar hantera. Det rör bl.a. risk för obehörig åtkomst, risker med utrustningens kvalitet och leverantörsberoenden.

2.2.1 Problem med obehörig åtkomst till system

Risken för obehörig åtkomst till viktiga system är redan idag en utmaning att hantera. Med 5G-nät kommer mer komplexa tekniska lösningar i kärnnät och delar som rör stödsystem kräva mer hjälp från olika kategorier av leverantörer, såväl på plats hos tillhandahållarna, som fjärrmässigt från platser som dessa inte har kontroll över.

Det allvarligaste hotet kopplat till obehörig åtkomst till kärnnät och stödsystem bedöms vara en kvalificerad antagonist som har strategiska avsikter och lång tid på sig att uppnå sitt mål. Dessa antagonister kan exempelvis utnyttja undermålig kvalitet i utrustning och avsiktlig introduktion av svagheter i utrustning och tjänster för att uppnå sina syften, t.ex. sabotage.

2.2.2 Problem med utrustningens kvalitet

Avseende utrustningens kvalitet konstaterar flera tillhandahållare som tillfrågats att denna har förbättrats avsevärt under de senaste tio åren. Detta har avspeglats t.ex. i att vissa system på senare år har blivit så stabila att det nu bara krävs en uppdatering per år. Detta gynnar tillgängligheten i tillhandahållarnas tjänster.

Dock finns det exempel på analyser[2] av kvaliteten på vissa leverantörers produkter som delvis pekar åt ett annat håll. Dessa analyser har genomförts i samverkan mellan statliga aktörer och leverantören själv. Resultaten av dessa analyser pekar mot att det kan finns kvalitetsbrister i produkter och produktionsprocessen som allvarligt kan påverka möjligheten att upprätthålla säkerheten i nät som byggs upp av dessa produkter. Detta bedöms bero på brister i mjukvaruproduktionsprocessen och tillhörande process för cybersäkerhet, vilket leder till risker för att sårbarheter uppstår i produkterna. Analyserna pekar också på att det kommer finnas stora utmaningar att hantera dessa problem även på lång sikt.

Ett allvarligt hot kopplat till problem med utrustningens kvalitet är en kvalificerad antagonist som har strategiska avsikter och har lång tid på sig att

[1] PTS förslag till riskanalys avseende nationell 5G-infrastruktur, PTS dnr 19-5389.
[2] Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Annual Report 2019, A report to the National Security Adviser of the United Kingdom March 2019, https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2019

uppnå sitt mål. Dessa antagonister kan exempelvis utnyttja undermålig kvalitet i utrustningen för att uppnå sina syften, t.ex. sabotage.

2.2.3 Problem med leverantörsberoenden

Flera tillhandahållare har lyft fram problem med leverantörsberoenden som svårbedömda och komplexa. Dessutom får detta område långtgående konsekvenser för möjligheten att utveckla och förvalta de komplexa och omfattande nät som kommer krävas för att åstadkomma 5G-funktionalitet. Aktörerna som tillfrågats i riskanalysen nämner här t.ex. svårigheterna att bedöma leveranssäkerheten för vissa leverantörer om dessa i sin tur inte kan garantera leverans från sina underleverantörer på grund av regleringar eller handelshinder.

Detta skapar stora svårigheter vid upphandlingar av nät och tjänster där stora och långsiktiga investeringar ska göras med svårbedömda kostnader, samtidigt som det ska ske med upprätthållande av en nödvändigt långsiktig tillit till leverantörerna ur flera perspektiv (t.ex. leveranssäkerhet, produktkvalitet, interoperabilitet).

2.3 Behov av revideringar

I de befintliga föreskrifterna med krav på driftsäkerhet finns bl.a. bestämmelser om att tillhandahållaren ska genomföra riskanalyser och vidta lämpliga skyddsåtgärder, samt vissa krav på rutiner för åtkomst och behörigheter. PTS ser nu ett behov av att skyndsamt revidera kraven på driftsäkerhet för att på lämpligt sätt kunna hantera de problemområden som identifierats. De revideringar som föreslås är främst

- Ökade dokumentationskrav
    - Tillgångars och förbindelsers tillverkare ska dokumenteras och dokumentationen sparas i fem år.
    - Uppdragstagare och uppdragens omfattning ska dokumenteras och dokumentationen sparas i fem år.
- Ytterligare hot ska analyseras i riskanalysen
    - Tydliggörande att ”sabotage” alltid är ett relevant hot som ska analyseras.
    - Information som förmedlas från PTS om hot ska alltid analyseras.
- Ytterligare tidpunkter för riskanalys
    - Inför upphandling av uppdragstagare.
    - Inför upphandling av tillgångar och förbindelser.
- Förtydligande avseende åtkomst och behörighet
    - Kravet gäller såväl egen personal som annans.

2.4 Alternativa lösningar och vilka effekterna blir om någon ändring inte kommer till stånd

Den rimliga nivån av driftsäkerhet ska enligt lagen säkerställas genom åtgärder som behöver beakta såväl riskerna för störningar och avbrott, som åtgärdernas kostnad och den tillgängliga tekniken. Allteftersom samhället blir mer beroende av fungerande elektronisk kommunikation ökar också riskerna med användningen av telefoni- och internettjänster. Den tekniska utvecklingen och kostnaderna förenade med vidtagande av säkerhetsåtgärder är inte heller konstanta. Detta innebär sammantaget att vad som är en rimlig nivå av driftsäkerhet varierar över tid. PTS behöver av den anledningen kontinuerligt se över de krav som ställs på tillhandahållarna för att säkerställa att nivån på driftsäkerhet är den lämpliga.

I december 2020 förväntas en ny lag om elektronisk kommunikation träda ikraft, vilken genomför EU:s direktiv om inrättande av en kodex för elektronisk kommunikation[3]. Med stor sannolikhet kommer PTS att få fortsatt bemyndigande att utfärda föreskrifter om säkerhet enligt den nya lagen, och ett omfattande arbete i denna fråga planeras därför starta inom det närmaste året. Eftersom det är angeläget ur säkerhetssynpunkt att skärpta regler om driftsäkerhet införs så snart som möjligt anser PTS att de föreslagna, nödvändiga regeländringarna bör införas redan under början av 2020.

PTS avser därför att nu revidera föreskrifterna. Alternativet till revideringen skulle vara att avvakta med ändringarna till dess att man genomför den stora revideringen 2020. PTS har övervägt detta alternativ men kommit fram till att frågan är av sådan brådskande karaktär, eftersom den har koppling till den kommande frekvenstilldelningen av 5G-spektrum, att det inte är lämpligt att vänta. Det är önskvärt att de säkerhetskrav som i synnerhet ska beaktas i denna revidering är kommunicerade till tillhandahållarna i god tid inför att dessa genomför t.ex. upphandlingar av ny utrustning och kontraktering av uppdragstagare inför utrullningen av 5G.

Om föreskrifterna inte revideras i tid, eller inte revideras alls, ser PTS negativa konsekvenser med att tillhandahållare inför 5G-utrullningen inte vidtar tillräckliga åtgärder för att säkerställa driftsäkerheten. Sådana konsekvenser kan t.ex. bestå i att tillhandahållare investerar i utrustning eller kontrakterar uppdragstagare, som man i ett senare skede av säkerhetsskäl inte finner godtagbara att använda. Analys och skyddsåtgärder för dessa risker behöver därför genomföras så snart som möjligt.

Sammantaget anser PTS att det är nödvändigt med en tvingande reglering och att meddela föreslagna föreskrifter om ändring i PTS föreskrifter om krav på driftsäkerhet.

[3] EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation

3 Aktörer som berörs av regleringen

De aktörer som berörs av förslaget är desamma som redan nu berörs av gällande driftsäkerhetsföreskrifter.

Av 5 kap. 6 b § LEK framgår att den som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att verksamheten uppfyller rimliga krav på driftsäkerhet. De som omfattas av skyldigheterna i de föreslagna ändringarna utgörs således av samtliga tillhandahållare.

Det finns även ett antal aktörer som berörs indirekt av regleringen, t.ex. slutanvändare, samhällsviktiga aktörer, tillverkare, leverantörer och myndigheter.

3.1 Företagen och dess storlek

Den svenska marknaden för elektronisk kommunikation är avreglerad sedan 1992. Avregleringen har skapat en mångfacetterad marknad som karaktäriseras av en ökad konkurrens och snabb teknikutveckling, vilket i sin tur inneburit att Sverige idag har ett brett och diversifierat utbud av nät och tjänster. Sektorn består idag av över 600 tillhandahållare, alltifrån stora multinationella företag med utbredda nät och stort tjänsteutbud, till mindre aktörer som erbjuder mindre nät eller en begränsad mängd tjänster inom ett begränsat geografiskt område.

Tillhandahållare erbjuder sina nät och tjänster på en rad olika nivåer. Det finns tillhandahållare som endast erbjuder nät och tjänster till andra tillhandahållare och det finns tillhandahållare som erbjuder nät och tjänster till slutkunder. Det finns också tillhandahållare som erbjuder nät och tjänster till såväl slutkunder som andra tillhandahållare. På grund av de höga investeringskostnader som kopplas till ny kommunikationsinfrastruktur är det idag också vanligt med samäganden där flera tillhandahållare erbjuder nät och tjänster till slutkunder via samma infrastruktur. Marknaden för elektronisk kommunikation tillgodoser i stort sett samtliga företag, hushåll och enskilda individer i Sverige med olika typer av kommunikationstjänster. Allmänna kommunikationsnät av sådant slag som vanligen tillhandahålls mot ersättning eller allmänt tillgängliga elektroniska kommunikationstjänster får endast tillhandahållas efter anmälan till PTS, enligt 2 kap. 1 § LEK. Idag är cirka 630 företag anmälda till PTS.

Av PTS rapport, Svensk telemarknad 2019, framgår att de totala slutkundsintäkterna 2018 uppgick till ca 50 miljarder kronor och att intäkten per månad från ett genomsnittshushåll var 612 kronor. De totala intäkterna på slutkundsmarknaden har legat stabilt på samma nivå under de senaste fem åren.

Med utgångspunkt i totala slutkundsintäkter, för såväl tjänstetillhandahållare som nättillhandahållare, för alla elektroniska kommunikationstjänster kan konstateras att fem aktörer innehar över 3,8 procent vardera (sammanlagt cirka 90 procent av marknaden), cirka 25 aktörer innehar mer än 0,1 procent, men mindre än 3 procent vardera och resterande aktörer, cirka 600 stycken, innehar mindre än 0,1 procent vardera av den totala marknaden. Som utgångspunkt för bedömningen av de kostnader som uppstår som en följd av dessa föreskrifter och allmänna råd benämns dessa grupper som **stora** (större än 3,8 procent), **medelstora** (mindre än 3,8 procent, men större än 0,1 procent) och **små** aktörer (mindre än 0,1 procent).

4 Konsekvenser

4.1 Förslagens innehåll och kostnadsmässiga konsekvenser

I följande avsnitt beskrivs de enskilda föreslagna ändringarna, tillkommande krav samt PTS bedömning av de ekonomiska konsekvenserna för berörda tillhandahållare. Kostnaderna för ändringarna, vilka sammanställs i Bilaga 1, redovisas som administrativa engångskostnader, administrativa årliga kostnader, samt som övriga kostnader.

4.1.1 Ytterligare definitioner

I 2 § föreslås en ny definition av ”uppdragstagare” som aktör ”den som anlitats av tillhandahållaren för att utföra installation, underhåll, felavhjälpning och drift eller liknande hantering av tillhandahållarens tillgångar och förbindelser”. Definitionen syftar till att tydliggöra vilka sorts aktörer som avses i kommande krav och avser bl.a. att snäva in begreppet till att omfatta vissa typer av uppdrag kopplade till tillgångar och förbindelser.

PTS bedömer att den nya definitionen inte är förenad med några ökade kostnader.

4.1.2 Ytterligare dokumentationskrav

PTS föreslår tillägg till dokumentationskravet i 4 § som innebär att tillhandahållare i sin dokumentation av tillgångar och förbindelser även behöver ange tillgångars och förbindelsers tillverkare. PTS föreslår vidare en ändring som innebär att varje version av dokumentationen enligt kravet ska sparas i fem år. Tidigare fanns endast ett krav på att dokumentationen ska hållas uppdaterad.

Syftet med tilläggen är att säkerställa att tillhandahållare ska kunna överblicka och spåra, inte bara t.ex. tillgångens och förbindelsens placering och funktion, utan även vilka tillverkare som står bakom den. Genom en god kontroll över detta ges bättre förutsättningar för till exempelvis genomförande av riskanalyser, såväl inför upphandling som av befintlig utrustning. Ett exempel på när detta skulle kunna vara viktigt är om en viss tillverkares utrustning visar sig vara behäftad med sårbarheter som behöver hanteras, se ovan under 2.2.2. Dokumentationen ger då lämplig överblick över var och på vilket sätt den tillverkarens utrustning används, vilket bör användas som underlag i riskanalys och vid vidtagande av skyddsåtgärder m.m.

När det gäller tillgångar är det tillhandahållarna själva som har att avgränsa vad som är en tillgång enligt gällande regler. Det får till följd att det i detta fall även blir upp till tillhandahållare att avgöra den närmare nivån på dokumentation av tillverkare, eftersom detta ska göras för varje tillgång.

Eftersom det redan finns ett dokumentationskrav i befintliga regler bedömer PTS att samtliga tillhandahållare har dokumentation över sina tillgångar och förbindelser. Dock innebär tillägget att dokumentationen nu kan behöva justeras för det fall att tillhandahållaren inte redan har dokumenterat samtliga tillgångars och förbindelsers tillverkare. De administrativa engångskostnaderna avser justering av befintlig dokumentation och de årliga administrativa kostnaderna avser löpande uppdateringar vid förändringar av tillhandahållarens tillgångar och förbindelser. PTS bedömer att tillhandahållare i normalfallet har uppgifter om tillverkare i sina system. En översyn och inventering av att dokumentationen uppfyller kraven på detta bedöms motsvara ungefär 25 procent ytterligare arbetsinsats jämfört med den tidsåtgång som bedömdes i samband med att krav på dokumentation infördes genom PTS föreskrifter om krav på driftsäkerhet (PTSFS 2015:2).

Eftersom kravet innefattar att fler uppgifter ska dokumenteras än vad tillhandahållarna är skyldiga att göra idag, samt att dokumentationen ska sparas i fem år, innebär det att systemen i sig kan behöva anpassas. Övriga kostnader som är förknippade med kravet utgörs således av de personalkostnader som i förekommande fall krävs för systemanpassningar. Dessa kostnader bedöms endast utgöras av en engångskostnad. Anpassningen av systemen bedöms vara marginell eftersom dessa redan i dagsläget i stor utsträckning är anpassade för att på ett ändamålsenligt sätt bevara dokumentationen av tillgångar. PTS bedömer att kostnaderna även i denna del ökar med 25 procent jämfört med befintliga krav. För sammanställning av beräknade kostnader, se bilaga 1.

Vidare föreslår PTS ett nytt dokumentationskrav i 4 a§. Enligt bestämmelsen ska tillhandahållaren även föra dokumentation över samtliga uppdragstagare som används och ange såväl namn och kontaktuppgifter, som uppdragets omfattning i dokumentationen. Förteckningen ska uppdateras löpande och varje version av den ska sparas i fem år.

PTS avser att med bestämmelsen tillse att tillhandahållarna vid var tid har en uppdaterad förteckning över vilka uppdragstagare som kontrakterats för att utföra installation, underhåll, felavhjälpning och drift eller liknande hantering av tillgångar och förbindelser. Att dokumentationen ska sparas i fem år möjliggör en spårbarhet, vilket underlättar för tillhandahållaren att kontrollera vilken uppdragstagare som utfört ett visst uppdrag även sedan en viss tid förflutit.

PTS ser att en stor del av tillhandahållarna har kontrakterat uppdragstagare till att utföra en stor variation av uppdrag i nät och tjänster. Utkontraktering till annan innebär samtidigt risker att man som tillhandahållare inte har tillräckligt bra överblick, spårbarhet och kontroll över sina nät och tjänster. Genom att ha uppdragstagare och dess uppdrag dokumenterade ökar kontrollen över vilka utomstående som medges åtkomst till tillgångar och förbindelser och under vilka förutsättningar.

PTS bedömer att i stort sett samtliga tillhandahållare redan har system för dokumentation av uppdragstagare, men att tillhandahållarna kan behöva göra

anpassningar i dokumentationen för att närmare beskriva uppdragens omfattning i enlighet med kravet. De administrativa engångskostnaderna avser upprättandet av den dokumentation som krävs och de administrativa årliga kostnaderna avser löpande uppdateringar vid förändringar av tillhandahållarens uppdragstagare och uppdrag.

Eftersom kravet innefattar att fler uppgifter ska dokumenteras än vad tillhandahållarna är skyldiga att göra idag, samt att dokumentationen ska sparas i fem år, innebär det att systemen i sig kan behöva anpassas så att dessa uppgifter kan inrymmas i dokumentationen. Övriga kostnader som är förknippade med kravet utgörs således av de personalkostnader som i förekommande fall krävs för systemanpassningar. Dessa kostnader bedöms endast utgöras av en engångskostnad. Även i dessa fall bedömer PTS att kostnaderna för systemanpassningar och därpå följande löpande arbetsinsatser medför fördyrningar om uppskattningsvis 25 procent jämfört med befintliga krav. För sammanställning av beräknade kostnader, se bilaga 1.

4.1.3 Ändring av befintligt riskanalyskrav

PTS föreslår vissa ändringar av det befintliga riskanalyskravet i 5 §. Ändringarna består i att myndigheten föreslår vissa hot som alltid ska analyseras. Dessa utgörs av hotet sabotage, samt information som förmedlas från PTS om hot till tillhandahållare.

Syftet med att införa krav på analys av sabotage är att tydliggöra att detta är ett viktigt hot vars realiserande bedöms kunna leda till stora konsekvenser för samhället. PTS ser att hotet kan anses inrymmas i hotet ”annan yttre påverkan”, som redan finns med i föreskrifterna, men med en egen angivelse ser PTS att det blir ännu tydligare att detta kontinuerligt måste beaktas och analyseras.

I och med teknikutvecklingen förväntas samhället få del av många nya och omfattande tjänster och användningsområden för elektronisk kommunikation. Samtidigt som detta sker ökar dock sårbarheten i samhället och därmed också riskerna för säkerhetsattacker. Att skydda befintliga tillgångar och förbindelser mot sabotage blir därmed en förutsättning för en god driftsäkerhet, varför PTS ser att förtydligandet behövs och är rimligt. Eftersom ändringen endast utgör ett förtydligande ser PTS inte att den är förenad med några ytterligare kostnader.

Vidare ser PTS ett behov av att införa ett krav på att den information som eventuellt förmedlas från PTS om hot till tillhandahållare är sådant som denne inte kan underlåta att ta med i sin riskanalys. Det skulle t.ex. kunna röra sig om information om olika hot som PTS genom t.ex. Säkerhetspolisen eller utländska myndigheter får del av och vill försäkra sig om att tillhandahållare känner till och beaktar. På vilket sätt sådan information kan förmedlas till tillhandahållare regleras inte utan får avgöras från fall till fall.

Riskanalyskrav har funnits i såväl PTS föreskrifter som allmänna råd sedan många år och baserat på tillsyn som myndigheten genomfört bedömer PTS att

samtliga tillhandahållare har och tillämpar en process för riskanalys för att hantera säkerhetsrisker i verksamheten. De administrativa engångskostnaderna för tilläggen enligt detta krav avser merkostnaderna för genomförande av riskanalyserna för information som kan komma att förmedlas av PTS om hot. De administrativa årliga kostnaderna avser genomförande av nya sådana riskanalyser. De tillkommande kostnader som kan komma ifråga i detta sammanhang hänför sig till de fall där PTS förmedlar hot som inte skulle beaktats inom ramen för den ordinarie riskanalysverksamheten. PTS bedömer att tillhandahållarna torde uppmärksamma flertalet hot men uppskattar att tillkommande arbetsinsatser och fördyrningar på cirka 10 procent kan uppstå jämfört med befintliga krav. Dessa bedömningar har avrundats till närmaste hel timme.

PTS bedömer att de övriga kostnaderna som är förknippade med kravet avseende riskanalyser är hänförliga till personalkostnader, såsom kostnader för eventuell utbildning av personal avseende ändringarna i riskanalysarbetet. Dessa kostnader bedöms dock inte vara särskilt omfattande eftersom PTS bedömer att den personal hos tillhandahållarna som arbetar med dessa frågor i de flesta fall är väl förtrogna med riskanalysarbete och löpande justeringar av riskanalysprocessen. Kostnaderna bedöms försumbara i denna del.

För sammanställning av beräknade kostnader, se bilaga 1.

4.1.4 Nytt krav på riskanalys inför upphandling och kontraktering

PTS krav på genomförande av riskanalyser i 5 § omfattar de befintliga tillgångar och förbindelser som tillhandahållare använder för sina nät och tjänster. PTS har dock sett ett behov av att införa ett krav på att tillhandahållare även inför upphandling av tillgångar och förbindelser, samt inför ingående av avtal med uppdragstagare, genomför riskanalyser.

Syftet med kravet är att se till att de hot som ska analyseras enligt 5 § även analyseras och bedöms i förhållande till sådan utrustning och sådana uppdragstagare som ännu inte anskaffats eller kontrakterats. På så vis kan tillhandahållare fatta bättre och säkrare beslut.

De största operatörerna har vid genomförande av den nationella riskanalysen för 5G inkommit med uppgifter om att dessa under senare år har skärpt kraven på säkerhet vid upphandlingar, både som en följd av bedömt växande hot och av GDPR[4]. Leverantörer och operatörer har utvecklat gemensamma standarder för säkerhet inom ramen för arbetet i GSM Association[5] och dessa standarder har utgjort en del av kravmassan vid senare systemupphandlingar.

[4] 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 (allmän dataskyddsförordning).
[5] Network Equipment Security Assurance Scheme (NESAS)

Operatörerna gör i anslutning till upphandlingar också bedömningar av om det finns en risk för att en leverantörs verksamhet upphör. Under de senaste 10 åren har flera stora systemleverantörer antingen gått i konkurs eller blivit uppköpta, vilket fortsättningsvis behöver beaktas.

De administrativa engångskostnaderna för detta krav avser merkostnaderna för genomförande och kontroll av dessa riskanalyser, justering av riskanalysprocesserna och ytterligare dokumentation av genomförda riskanalyser. De administrativa årliga kostnaderna avser genomförande av nya riskanalyser inför kommande upphandlingar. Nuvarande regler innehåller krav på att tillhandahållarna ska genomföra en riskanalys av befintliga tillgångar. Det tillkommande kravet innebär att denna riskanalys ska göras redan i samband med införskaffandet. Utöver en initial insats som medför att administrativa engångskostnader för att ändra befintliga rutiner och dokumentation tidigareläggs bedömer PTS att de tillkommande kostnaderna i denna del är försumbara.

PTS bedömer att de övriga kostnaderna som är förknippade med kravet avseende riskanalyser är hänförliga till personalkostnader, såsom kostnader för eventuell utbildning av personal avseende ändringarna i riskanalysarbetet. Dessa kostnader bedöms dock inte vara särskilt omfattande eftersom PTS bedömer att den personal hos tillhandahållarna som arbetar med dessa frågor i de flesta fall är väl förtrogna med riskanalysarbete och löpande justeringar av riskanalysprocessen. PTS bedömer därför att dessa kostnader är försumbara.

För sammanställning av beräknade kostnader, se bilaga 1.

4.1.5 Åtgärder efter riskbedömning

PTS befintliga föreskrifter om driftsäkerhet bygger, när det gäller riskanalyser, på att tillhandahållare först behöver bedöma risken för olika hot, för att sedan innefatta krav på vidtagande av skyddsåtgärder för att på en rimlig och lämplig nivå hantera risken. Eftersom PTS nu föreslår att nya hot ska analyseras i riskbedömningen enligt 5 §, samt att riskanalys även ska genomföras inför upphandling enligt 5 a §, föreslår PTS även att det läggs till krav på vidtagande av skyddsåtgärder för dessa hot och risker.

I 10 § föreslås ett tillägg i form av hotet ”sabotage” när det gäller vilka hot som tillhandahållaren enligt paragrafen ska vidta åtgärder för att skydda sig mot. Som tidigare nämnts så är tillägget snarast ett förtydligande av vad som redan anses omfattas i ”annan yttre påverkan”, varför PTS inte ser att kravet är förenat med några ytterligare kostnader för operatörerna.

Vidare föreslås i 9 a § ett krav på vidtagande av åtgärder för att skydda tillgångar och förbindelser mot risker som framkommit efter analys av information som förmedlats från PTS om hot. Kravet innebär således att om PTS förmedlat information om hot mot driftsäkerheten som tillhandahållaren enligt 5 och 5 a §§ har analyserat, så ska tillhandahållaren även vidta åtgärder för att skydda sig mot sådana risker. PTS ser att det kan finnas eller uppstå hot mot

driftsäkerheten som tillhandahållaren inte har kännedom om. Eftersom föreskrifterna idag lämnar utrymme för att tillhandahållaren själv kan bedöma vad som är ett relevant hot, ser PTS att det finns en risk att myndigheten har kännedom om hot som tillhandahållaren inte känner till och således inte beaktar. Genom att införa ett krav på analys av hot som PTS förmedlar samt krav på att tillhandahållaren måste vidta skyddsåtgärder för att hantera sådana hot, minskar riskerna för detta.

PTS konstaterar härvid att det inte på förhand går att ange vilken hotinformation som kan bli aktuell att förmedla, och således går det inte heller att ange vilka skyddsåtgärder som behöver vidtas. Det får avgöras från fall till fall.

Slutligen föreslår PTS att det i 11 a § läggs till ett krav om att tillhandahållare ska vidta åtgärder för att skydda sina nät och tjänster mot risker som identifierats vid riskanalysen som man enligt förslaget är skyldig att utföra inför upphandling enligt 5 a §.

I sammanhanget kan det vara av vikt att påpeka att tillhandahållaren, som en yttersta skyddsåtgärd för det fall att analysen visar på betydande risker med t.ex. en viss tillverkare eller en viss tillgång, kan behöva använda sig av en annan leverantör eller tillgång. Tillhandahållarens bedömning av val av nivå på skyddsåtgärderna ska alltjämt dokumenteras enligt 9 §.

De administrativa engångskostnaderna för dessa ändringar avser den ytterligare proportionalitetsbedömning, och dokumentation av denna, som krävs för efterlevnad av kraven. De administrativa årliga kostnaderna avser eventuell revidering av bedömningarna och dokumentationen. Kostnaderna begränsas till viss del av att krav på riskanalyser har funnits under många år och att tillhandahållarna, enligt PTS bedömning, i stor utsträckning redan arbetar med riskhantering.

När det gäller övriga kostnader så är detta beroende på vilken nivå av skydd som tillhandahållare har idag. Kraven i de föreslagna föreskrifterna kan innebära allt från små till mycket stora investeringar i åtgärder för att skydda verksamheten mot störningar och avbrott.

Liksom vid framtagningen av de befintliga föreskrifterna med krav på driftsäkerhet har PTS nu inte möjlighet att göra en fullständig kostnadsuppskattning för skyddsåtgärderna enligt kraven. Kostnaderna går inte att kvantifiera eller uppskatta mot bakgrund av att det är omöjligt att i förväg känna till hot som måste beaktas och vilka investeringar som respektive tillhandahållare kommer att behöva göra efter genomförda riskanalyser. Exempel på investeringar som kan komma att krävas efter riskbedömning är byte av uppdragstagare eller tillverkare, investeringar i lås, dörrar, säkerhetsfönster, larmsystem, kylsystem, översvämningsskydd, åskskydd m.m. Beroende på vilka hot som vid var tid föreligger och nivån av skydd

tillhandahållaren har idag kan investeringarna variera från mycket låg nivå till höga belopp.

För sammanställning av beräknade kostnader, se bilaga 1.

4.1.6 Åtkomst och behörighet

PTS föreslår att det i 13 § om åtkomst och behörighet läggs till att bestämmelsen gäller såväl för uppdragstagare som för tillhandahållarens egna anställda.

Syftet med bestämmelsen är att tydliggöra att man som tillhandahållare måste tillse att också uppdragstagare omfattas av krav på behörigheter och åtkomsthantering. PTS har i tillsyn uppmärksammat att det funnits vissa oklarheter gällande om så var fallet eller inte och vill med tillägget förtydliga vad som gäller.

Tillägget utgör ett förtydligande och är således inget nytt krav, varför PTS inte bedömer att det är förenat med några ökade kostnader.

4.2 Påverkan på konkurrensförhållandena för företag

De företag som berörs av regleringen verkar på en konkurrensutsatt marknad. Konsumenternas möjligheter att välja mellan olika tillhandahållare varierar, dels mellan olika typer av kommunikationstjänster och dels mellan olika platser i landet.

De förändringar som nu föreslås kan antas påverka de företag som verkar på marknaden i varierande utsträckning beroende på hur utvecklade rutiner de har idag för t.ex. genomförande av riskanalyser inför upphandling.

Det finns dock anledning att tro att mindre aktörer har mindre utvecklade rutiner och processer och att de därför också har ett visst merarbete att genomföra för att kunna efterleva bestämmelsen. Å andra sidan har dessa aktörer också mindre kundstockar och ofta en mer begränsad geografisk täckning vilket torde innebär att risken för driftsavbrott är mindre och att inträffade incidenter drabbar färre användare över en mindre yta.

Indirekt kan kraven komma att påverka de tillverkare och uppdragstagare som inte idag lever upp till en godtagbar standard vad gäller säkerhet. De föreslagna ändringarna medför dock inte ett förbud eller liknande gentemot specifika företag, utan sätter ribban för vilken nivå av driftsäkerhet som tillhandahållarna behöver få tillgodosedda av bl.a. tillverkare. Det kan mot bakgrund av detta inte uteslutas att det finns tillverkare och uppdragstagare m.m. som påverkas såtillvida att man inte blir kontrakterad om man inte kan uppvisa en godtagbar säkerhetsnivå. Det kan medföra kostnader för de företag som idag inte lever upp till en sådan nivå.

PTS gör bedömningen att den totala kostnaden som ett företag har för att kunna bedriva en verksamhet som berörs av regleringen endast i rimlig utsträckning påverkas av de föreslagna ändringarna.

De eventuella kostnader och den konkurrenspåverkan som ändringarna i övrigt kan medföra bedömer PTS såsom rimliga i förhållande till nyttan av att stärka driftsäkerheten.

PTS gör sammantaget bedömningen att konkurrensförhållandena på marknaden inte i någon högre utsträckning torde påverkas av den föreslagna regleringen.

4.3 Ändringarnas effekter för kommuner och landsting

Kommuner och landsting som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster omfattas av samma skyldigheter som andra tillhandahållare av sådana nät och tjänster. I övrigt kan inga effekter förutses med mindre än att dessa aktörer, liksom övriga användare, förväntas få en högre driftsäkerhetsnivå i de nät och tjänster som används i verksamheten.

5 Övrigt

5.1 Regleringens överensstämmelse med de skyldigheter som följer av Sveriges anslutning till EU

Ändringsföreskrifterna förtydligar vilka lämpliga åtgärder som tillhandahållare har att vidta enligt 5 kap. 6 b § LEK. Denna bestämmelse genomför i sin tur artikel 13a i Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster, senast ändrat genom direktiv 2009/140/EG av den 25 november 2009.

Även tillämpningen av de nationella regler som genomför artikel 13a är harmoniserad, främst genom medlemsländernas samarbete i en arbetsgrupp som drivs av ENISA, den europeiska nät- och informationssäkerhetsbyrån. PTS medverkar aktivt i denna arbetsgrupp. Med stöd av arbetsgruppen har ENISA utfärdat rekommendationer som berör tillämpningen av artikel 13a. I rekommendationen ”Technical Guideline on Security Measures” anges ett antal övergripande sakområden vilka medlemsstaterna rekommenderas att ställa krav inom, för att uppnå en rimlig driftsäkerhetsnivå. De föreslagna ändringarna är i linje med dessa rekommendationer.

Mot bakgrund av ovanstående gör PTS bedömningen att förslaget till nya föreskrifter överensstämmer med de skyldigheter som följer av Sveriges anslutning till EU.

5.2 Behovet av särskilda hänsyn till små företag

PTS har beaktat frågan om särskilda hänsyn behöver tas till små företag vid reglernas utformning. Bland de som berörs av föreskrifterna uppskattar PTS att det finns allt från företag med en årsomsättning på mindre än en miljon kronor till företag med en årlig omsättning på trettio miljarder kronor. PTS bedömer sammanfattningsvis att kostnaderna för att uppfylla bestämmelserna i föreskrifterna är rimliga i förhållande till behovet och nyttan av driftsäkerheten i nät och tjänster uppfyller rimliga krav, samt att några ytterligare särskilda hänsyn inte behöver tas till små företag vid reglernas utformning.

5.3 Tidpunkten för ikraftträdande och behovet av särskilda informationsinsatser

PTS kommer att, inom ramen för myndighetens tillsynsverksamhet, kontrollera efterlevnaden av föreskrifterna. I tillsynsarbetet kan viss hänsyn tas till tillhandahållarnas behov av tid för att genomföra de anpassningar som krävs till följd av de föreslagna ändringarna.

PTS gör vidare bedömningen att det inte finns något behov av att ta fram information om den förändrade regleringen i direkt samband med reglernas

ikraftträdande. Utgångspunkten för denna bedömning är bl.a. att samtliga berörda företag kommer att erhålla information om förändringen i samband med att föreskriftsförslaget remitteras.

Utöver detta ser PTS behov av att uppdatera eller komplettera den information om reglerna som finns på PTS webbplats, liksom sådan information som lämnas till nyanmälda aktörer på marknaden.

Reglerna bedöms kunna träda ikraft under våren 2020.

6 Avslutning

6.1 Underrättelse för anmälan till Europeiska kommissionen

I 6 § förordningen (1994:2029) om tekniska regler framgår att en myndighet som avser fatta beslut om en teknisk regel i god tid ska underrätta Kommerskollegium om det förslag som den har utarbetat. Bestämmelserna i förordningen ansluter till Sveriges internationella förpliktelser enligt bl.a. Europaparlamentets och rådets direktiv 98/34/EG av den 22 juni 1998, ändrat genom Europaparlamentets och rådets direktiv 98/48/EG, om ett informationsförfarande beträffande tekniska standarder och föreskrifter och beträffande föreskrifter för informationssamhällets tjänster.

Enligt PTS bedömning är nu föreslagna föreskrifter inte att se som sådana tekniska regler som ska underrättas enligt nämnda förordning. Någon underrättelse till Kommerskollegium behöver således inte göras.

6.2 Kontaktpersoner

För sakfrågor:

Karin Lodin, avdelningen för säker kommunikation

karin.lodin@pts.se

För juridiska frågor:

Erica Nyström, rättsavdelningen

erica.nystrom@pts.se