

## PTS tillsynsplan 2020-2021 för säkra kommunikationsnät och -tjänster

Post- och telestyrelsen (PTS) är tillsynsmyndighet över sektorn elektronisk kommunikation. Myndigheten publicerar här sina planlagda tillsynsinsatser för 2020-2021 inom områdena konfidentiell kommunikation och driftsäkerhet. Utöver planlagd tillsyn inom dessa områden bedriver PTS även löpande händelsestyrd tillsyn.

### 1 Konfidentiell kommunikation

Ett av PTS övergripande mål är att alla användare har tillgång till tillförlitliga och säkra elektroniska kommunikationsnät och -tjänster. En viktig säkerhetsfråga är skyddet av konfidentialitet för uppgifter som behandlas i samband med tillhandahållandet av tjänster. PTS arbetar för att alla i Sverige ska kunna kommunicera elektroniskt utan att riskera att informationen kommer på avvägar eller används på ett oönskat sätt.

#### 1.1 Regler om konfidentiell kommunikation

Lagen (2003:389) om elektronisk kommunikation (LEK) innehåller regler om rätten till konfidentiell kommunikation och gäller tillhandahållare av elektroniska kommunikationsnät och -tjänster. Det finns krav på att vidta tekniska och organisatoriska säkerhetsåtgärder för att skydda de uppgifter som behandlas. Reglerna i LEK kompletteras av PTS föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter (PTSFS 2014:1).

Enligt bestämmelser i LEK, kompletterade av en direkt tillämplig EU-förordning<sup>1</sup>, är tjänstetillhandahållare även skyldiga att rapportera inträffade integritetsincidenter till PTS och berörda abonnenter eller enskilda personer. En integritetsincident utgörs av 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 tillhandahållande av tjänsten. Rapporterna ger PTS underlag om de viktigare orsakerna till integritetsincidenter och hur tillhandahållarna arbetar för att förebygga och hantera inträffade händelser. Rapporterna kan även ge PTS anledning att misstänka att bestämmelserna om skydd av behandlade uppgifter inte efterlevs och i sådana fall bedriva tillsyn.

## 2 Driftsäkerhet

En annan viktig säkerhetsfråga är att elektroniska kommunikationsnät och -tjänster är tillgängliga, dvs. att de är driftsäkra. PTS arbetar för att nät och tjänster ska ha en nivå av driftsäkerhet som motsvarar användarnas behov.

### 2.1 Regler om driftsäkerhet

Enligt 5 kap. 6 b § LEK ska tillhandahållare av allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att verksamheten uppfyller rimliga krav på driftsäkerhet. Skyldigheterna preciseras i PTS föreskrifter (PTSFS 2015:2) om krav på driftsäkerhet (driftsäkerhetsföreskrifterna).

Tillhandahållarna är även skyldiga att rapportera in störningar eller avbrott av betydande omfattning till PTS. Det framgår av 5 kap. 6 c § LEK. Skyldigheten preciseras i PTS föreskrifter och allmänna råd om rapportering av störningar eller avbrott av betydande omfattning (PTSFS 2018:4). Föreskrifterna uppdaterades i början av 2019. Ändringarna innebär bl.a. att tidpunkten för inrapportering justeras och att tillhandahållaren redan i den inledande rapporten behöver ange preliminär orsak till störningen eller avbrottet

Rapporterna ger PTS underlag om de viktigare orsakerna till störningar och avbrott, och hur tillhandahållarna arbetar för att förebygga och hantera inträffade händelser. Rapporterna kan även ge PTS anledning att misstänka att bestämmelserna om driftssäkerhet inte efterlevs och i sådana fall bedriva tillsyn.

---

<sup>1</sup> Kommissionens förordning (EU) nr 611/2013

## **3 Planlagd tillsyn 2020-2021**

### **3.1 Årlig tillsyn av inträffade störningar och avbrott samt integritetsincidenter**

PTS granskar löpande de rapporter om störningar och avbrott samt integritetsincidenter som inkommer till myndigheten. I händelse av mer omfattande eller principiellt intressanta incidenter kan PTS komma att inleda händelsestyrd tillsyn, som regel inriktad på att granska orsakerna till den inträffade händelsen och tillhandahållarens arbete för att undvika att liknande händelser inträffar igen.

PTS följer även upp de större tillhandahållarnas arbete med att hantera och dra lärdomar av inträffade incidenter genom en planlagd årlig tillsyn, som omfattar samtliga de inrapporterade störningar och avbrott samt integritetsincidenter under det gångna året som inte redan har granskats inom ramen för händelsestyrd tillsyn. Tillsynen kan även omfatta granskning av tillhandahållarnas rutiner för incidentrapportering.

Den årliga tillsynen inleds under första kvartalet 2020 och bedrivs huvudsakligen genom inhämtning av skriftliga underlag och möten med de större tillhandahållarna.

### **3.2 Driftsäkerhet vid förläggning av sjökablar**

PTS samarbetar med de nordiska motsvarigheterna till myndigheten bland annat vad gäller tillsyn. Inom ramen för detta samarbete har det framkommit att den finska tillsynsmyndigheten har haft anledning att granska tillhandahållares hantering av sjökablar, efter att myndigheten noterat att dessa förbindelser förläggs på ett oskyddat sätt vid marknivå.

PTS finner mot bakgrund av detta att det finns skäl att granska de svenska motsvarigheterna till dessa förbindelser, dvs. i synnerhet vad gäller skyddet där sjökablar övergår till att bli förbindelser på land.

Förbindelser ska enligt PTS driftsäkerhetsföreskrifter alltid omfattas av en aktuell riskanalys. Tillhandahållaren är vidare skyldig att vidta de skyddsåtgärder som är nödvändiga med hänsyn till den risk för störning och avbrott som framkommit i riskanalysen. Såväl riskanalysen som tillhandahållarens bedömning av nivån på skyddsåtgärder ska dokumenteras. Mot bakgrund av reglerna om riskanalys och vidtagande av nödvändiga skyddsåtgärder avser PTS att granska hur ett urval av tillhandahållare ser till att dessa förbindelser har en rimlig driftsäkerhetsnivå. Tillsynen, som kommer att bedrivs genom skriftlig informationsinhämtning, eventuellt i kombination med inspektion på plats, inleds under andra kvartalet 2020.

### **3.3 Sårbarheter i Border Gateway Protocol (BGP)**

Border Gateway Protocol (BGP) är en central del av internets ryggrad. Protokollet används av bl.a. internet- och knutpunktsleverantörer för att vidarebefordra internettrafik över världen.

PTS har konstaterat att det föreligger kända sårbarheter i BGP. Säkerhetsbristerna i BGP kan leda till såväl driftstörningar som integritetsincidenter. Bakomliggande orsaker till incidenter kan vara avsiktliga attacker eller oavsiktlig felkonfiguration.

Sårbarheter och säkerhetsåtgärder kopplade till BGP, har särskilt uppmärksammats internationellt de senaste åren. PTS har hittills mottagit en incidentrapport avseende oavsiktlig felkonfiguration av BGP. Incidenten ledde till ett omfattande avbrott i kommunikationstjänster.

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 åtgärder som vidtas ska vara ägnade att skapa en säkerhetsnivå som, med beaktande av tillgänglig teknik och kostnaderna för att genomföra åtgärderna, är anpassad till risken för störningar och avbrott.

Tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster är skyldiga att dessutom säkerställa att uppgifter som behandlas i samband med tillhandahållandet av tjänsten skyddas.

Mot bakgrund av detta kommer PTS under 2020 inleda en tillsyn över ett urval av de större tillhandahållarna i syfte att granska att dessa har tillräcklig kunskap om sårbarheterna och vidtar lämpliga säkerhetsåtgärder.

Tillsynen kommer att bedrivas genom skriftlig informationsinhämtning i kombination med tillsynsmöten.

### **3.4 Skärpta säkerhetskrav för operatörer inför upphandling**

Den kommande utbyggnaden av 5G-näten kommer att ytterligare öka samhällets beroende av tillförlitliga elektroniska kommunikationsnät och -tjänster. För att omhänderta några av de risker som aktualiseras har PTS den 1 mars 2020 skärpt reglerna om driftsäkerhet. De uppdaterade reglerna innebär bl.a. att tillhandahållare ska genomföra riskanalyser inför upphandling, krav att tillhandahållare beaktar ytterligare hot i riskanalysen, ökade dokumentationskrav och förtydliganden kring åtkomst och behörighet. Reglerna är i linje med flera av de åtgärder som rekommenderas i EU:s verktyglåda med säkerhetsåtgärder för 5G.

Mot bakgrund av dessa nya krav planerar PTS att under 2020 inleda en tillsyn över ett urval av de större tillhandahållarna i syfte att granska om dessa efterlever de nya kraven.

### **3.5 Efterlevnad av krav på reservkraft och redundans**

Tjänstetillhandahållare som känner till hur många aktiva anslutningar som deras tillgångar betjänar, är skyldiga att klassificera sina tillgångar efter hur många aktiva anslutningar som kan omfattas av en störning eller avbrott till följd av att tillgången upphör att fungera normalt. Med utgångspunkt i tillgångarnas klassificering ska tjänstetillhandahållaren efterleva krav på redundans och reservkraft. Tillhandahållare av mobila kommunikationsnät och mobila kommunikationstjänster ska, utöver de generella kraven på reservkraft, även efterleva ett särskilt krav på reservkraft.

Reglerna om krav på reservkraft och redundans träder i kraft den 10 juni 2020. Om tillhandahållaren har vidtagit någon förändring av tillgången eller reservkraftsystemet, efter den 1 januari 2016, gäller kraven emellertid omedelbart. Mot bakgrund av dessa nya bestämmelser planerar PTS att senast under 2021 inleda en tillsyn över ett urval av de större tillhandahållarna i syfte att granska om dessa har anpassat sig till de nya reglerna om reservkraft och redundans.

Tillsynen kommer sannolikt att bedrivas genom skriftlig informationsinhämtning i kombination med tillsynsmöten.

### **3.6 Nya föreskrifter**

För närvarande pågår en översyn av regelverket för såväl driftsäkerhet som konfidentiell kommunikation. Ett nytt EU-direktiv, en kodex om elektronisk kommunikation, ska genomföras i Sverige genom en ny lag om elektroniska kommunikationer. PTS arbetar med att ta fram nya föreskrifter kopplade till den nya lagen. Den nya lagen och föreskrifterna är tänkta att träda i kraft i december 2020.

De nya bestämmelserna kan komma att innebära nya eller förändrade krav gentemot tillhandahållare. PTS planerar att genomföra tillsyn under 2021 med utgångspunkt i någon eller några av de nya kraven, i syfte att granska om tillhandahållarna efterlever regelverket.

Tillsynen kommer sannolikt att bedrivas genom skriftlig informationsinhämtning i kombination med tillsynsmöten.