PTS tillsynsplan 2019-2020 för säkra kommunikationsnät och -tjänster

Post- och telestyrelsen (PTS) är tillsynsmyndighet över sektorn elektronisk kommunikation. Myndigheten publicerar här sina planlagda tillsynsinsatser för 2019-2020 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 som 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, är tjänstetillhandahållare även skyldiga att rapportera inträffade integritetsincidenter till PTS och berörda abonnenter eller enskilda personer, samt att föra en förteckning över inträffade incidenter. 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

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

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.

3 Planlagd tillsyn 2019-2020

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 kommer att inledas under första kvartalet 2019 och bedrivas huvudsakligen genom inhämtning av skriftliga underlag och möten med de större tillhandahållarna.

3.2 Säkerhetsarbete hos små och medelstora tillhandahållare

PTS kan konstatera att majoriteten av incidentrapporterna inkommer från de större tillhandahållarna. Detta kan delvis förklaras av att en mer omfattande verksamhet även leder till fler integritetsincidenter och störningar och avbrott av betydande omfattning. Reglerna om incidentrapportering är dock utformade så att även händelser där endast en person är drabbad av en integritetsincident är rapporteringspliktiga, samt att även driftsäkerhetsincidenter hos mindre tillhandahållare ska rapporteras, främst genom kravet på rapportering vid ett visst procentuellt kapacitetsbortfall.

Mot bakgrund av det begränsade antalet incidentrapporter från mindre tillhandahållare misstänker PTS att flera av dessa tillhandahållare inte efterlever kraven på rapportering. Bristen på rapporter ger också PTS ett sämre underlag för bedömning av hur tillhandahållarna lever upp till bestämmelserna om krav på skydd av behandlade uppgifter och driftsäkerhet.

PTS har därför för avsikt att i början av 2019 inleda tillsyn med inriktning på att granska hur små och medelstora tillhandahållare av nät och tjänster lever upp till kraven på konfidentiell kommunikation och driftsäkerhet, samt hur de efterlever kraven på incidentrapportering.

Tillsynen kommer att bedrivas genom skriftlig informationsinhämtning från ett större antal små och medelstora tillhandahållare, eventuellt kombinerat med inspektioner på plats hos ett urval av dessa tillhandahållare.

3.3 Processer för riskanalyser

PTS anser att tillhandahållares arbete med riskanalyser är centralt för att kunna bedriva ett långsiktigt, kontinuerligt och systematiskt säkerhetsarbete. Till exempel ska tillhandahållare enligt 5 § i driftsäkerhetsföreskrifterna minst en gång per år analysera risken för att dokumenterade tillgångar och förbindelser orsakar störningar eller avbrott i de kommunikationsnät och kommunikationstjänster som denne tillhandahåller. Även enligt PTS föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter ska tjänstetillhandahållare analysera riskerna för att integritetsincidenter inträffar för informationsbehandlingstillgångar.

PTS har efter tidigare tillsyn funnit anledning att misstänka att tillhandahållares arbete med genomförande av riskanalyser kan förbättras. PTS kommer därför att bedriva tillsyn över riskanalysarbetet, där myndigheten bl.a. ska granska om tillsynsobjektens process för riskanalys innefattar de delar som framgår av PTS föreskrifter. I denna tillsyn ingår dock inte att granska vilka skyddsåtgärder som tillsynsobjekten vidtar eller planerar att vidta för att avhjälpa identifierade risker.

Tillsynen, som inletts i slutet av 2018 men i huvudsak bedrivs under 2019, kommer att genomföras genom skriftlig informationsinhämtning i kombination med möten med tillhandahållarna. Den planeras att omfatta ett urval av större tillhandahållare.

3.4 Driftsäkerhet vid förläggning av sjökablar

PTS samarbetar med de nordiska motsvarigheterna till myndigheten bl.a. 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 tillhandahållare ser till att dessa förbindelser har en rimlig driftsäkerhetsnivå. Tillsynen, som kommer att bedrivas genom skriftlig informationsinhämtning, eventuellt i kombination med inspektion på plats, inleds under tredje kvartalet 2019.

3.5 Sårbarheter i Border Gateway Protocol (BGP)

Tjänstetillhandahållare är skyldiga att säkerställa att uppgifter som behandlas i samband med tillhandahållandet av tjänsten skyddas. PTS har konstaterat att det föreligger kända sårbarheter i det routingprotokoll som tillämpas i de routrar som binder samman internet, Border Gateway Protocol (BGP). PTS har endast noterat någon enstaka nationell incident som inträffat som ett resultat av dessa sårbarheter, men det finns ett flertal incidenter som uppmärksammats internationellt. Mot bakgrund av detta kommer PTS under andra hälften av 2019 inleda en tillsyn över ett urval av de större tillhandahållarna i syfte att granska att dessa har tillräcklig kunskap om sårbarheterna och vidtar lämpliga åtgärder för att skydda information under överföring.

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

3.6 Tillhandahållarnas åtgärder för att säkerställa identitet på abonnenter vid kontakt med kundtjänst på distans

Tjänstetillhandahållare är skyldiga att vidta nödvändiga åtgärder för att hantera risken för integritetsincidenter.

PTS har konstaterat att flera incidentrapporter som inkommit till myndigheten rört att tillhandahållares medarbetare i kundtjänst inte på ett godtagbart sätt säkerställt att den som kontaktat kundtjänst är den som den utger sig för att vara och behörig, innan kundtjänstmedarbetaren t.ex. har lämnat ifrån sig uppgifter om en specifik abonnent eller gjort förändringar i abonnemanget som medfört att utomstående kunnat få del av abonnentens kommunikation.

Mot bakgrund av dessa incidenter kommer PTS under första kvartalet 2019 inleda en tillsyn över ett urval tillhandahållare för att granska hur deras kundtjänstmedarbetare verifierar identiteten på abonnenter innan man utför vissa åtgärder inom ramen för tjänsten, såsom t.ex. aktivering av sim-kort, nummerportering och vidarekoppling av samtal.

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