Enkät om driftsäkerhet och skydd för behandlade uppgifter (Enkät 1)

Denna enkät riktar sig till aktörer som tillhandahåller en eller flera allmänt tillgängliga elektroniska kommunikationstjänster. Om ni därutöver tillhandahåller ett eller flera allmänna kommunikationsnät ska ni också besvara denna enkät.

Om ni däremot enbart tillhandahåller en eller flera allmänna kommunikationsnät, men inte allmänt tillgängliga elektroniska kommunikationstjänster, ska ni istället besvara enkäten som enbart innehåller frågor om driftsäkerhet (Enkät 2).

Syftet med enkäten är att kartlägga små och medelstora aktörers efterlevnad av reglerna om driftsäkerhet och skydd för behandlade uppgifter (integritetsskydd) samt att ge PTS ökad kunskap om mindre och medelstora aktörers arbete inom dessa områden. Målet är att kunna dra generella slutsatser om aktörernas arbete med driftssäkerhet och skydd för behandlade uppgifter utifrån de samlade enkätsvaren.

Verksamhet och antal anställda

Var god ange:

Företagets namn:

Organisationsnummer:

Begrepp

Elektronisk kommunikationstjänst: tjänst som vanligen tillhandahålls mot ersättning och som helt eller huvudsakligen utgörs av överföring av signaler i elektroniska kommunikationsnät.

Allmänt kommunikationsnät: elektroniskt kommunikationsnät som helt eller huvudsakligen används för att tillhandahålla allmänt tillgängliga elektroniska kommunikationstjänster och som stödjer informationsöverföring mellan nätanslutningspunkter.

1. Vilken typ av verksamhet bedriver ni?

- ☐ Tillhandahåller en eller flera allmänt tillgängliga elektroniska kommunikationstjänster
- ☐ Tillhandahåller en eller flera allmänt tillgängliga elektroniska kommunikationstjänster samt ett eller flera allmänna kommunikationsnät
- ☐ Tillhandahåller enbart ett eller flera allmänna kommunikationsnät *(Om ni enbart tillhandahåller ett eller flera allmänna kommunikationsnät ska ni istället besvara enkäten om driftsäkerhet, Enkät 2)*

2. Hur många anställda finns i verksamheten ni bedriver enligt ovanstående fråga?

- ☐ 1 – 2
- ☐ 3 – 14
- ☐ 15 – 99
- ☐ 100 – 299
- ☐ 300 – 999
- ☐ 1.000 eller fler

Ansvariga för arbetet med driftsäkerhet och integritetsskydd

3. Har ni särskilt utpekade ansvariga för driftsäkerhetsarbetet?

- ☐ Ja
- ☐ Nej
- ☐ Vet ej

4. Har ni särskilt utpekade ansvariga för arbetet med skydd för behandlade uppgifter (integritetsskydd)?

- ☐ Ja
- ☐ Nej
- ☐ Vet ej

Driftsäkerhet

Begrepp

Tillgång: funktion som utgörs av en avgränsad del av ett kommunikationsnät eller 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. Exempel på funktioner som kan utgöra tillgångar är routrar, switchar, basstationer, media gateways etc.

Förbindelse: del av kommunikationsnät mellan två tillgångar eller mellan en tillgång och en anslutning till ett kommunikationsnät. En förbindelse behöver inte gå mellan tillhandahållarens egna tillgångar för att omfattas, utan bör till exempel kunna utgöras av en svartfiberleverantörs uthyrda förbindelser mellan en annan parts tillgångar.

Riskanalys

Av PTS föreskrifter, PTSFS 2015:2 5 §, framgår att en riskanalys ska innefatta åtminstone följande delar;

1. Identifiering av samtliga relevanta hot mot den aktuella tillgången eller förbindelsen. Hot relaterade till väder samt intrång och annan yttre påverkan ska alltid analyseras.
2. Kvalificerad bedömning av konsekvenser i händelse av att identifierade hot inträffar.
3. Kvalificerad bedömning av sannolikheten för att identifierade hot inträffar.
4. Kvalificerad sammanvägd bedömning av sannolikheten för att identifierade hot inträffar och de konsekvenser det kan medföra om de inträffar (riskbedömning).

5. Hur ofta eller när analyserar ni risken för att tillgångar och förbindelser orsakar störningar och avbrott i kommunikationsnät och kommunikationstjänster? Det är möjligt att ange ett eller flera svarsalternativ.

- ☐ Löpande, dock minst en gång per år
- ☐ Mer sällan än en gång per år
- ☐ Vid planerade förändringar som kan påverka driftsäkerheten i kommunikationsnäten och/eller kommunikationstjänsterna
- ☐ Efter att störningar eller avbrott av betydande omfattning har inträffat
- ☐ Vi genomför inte riskanalyser för störningar och avbrott i vår verksamhet

Skyddsåtgärder

6. Har ni vidtagit några skyddsåtgärder för att minska risken för störningar eller avbrott i kommunikationsnät och kommunikationstjänster?

- ☐ Ja, löpande
- ☐ Ja, men inte under det senaste året
- ☐ Nej
- ☐ Vet ej

7. Har ni vidtagit någon eller några av följande åtgärder?

- ☐ Åtgärder för att skydda tillgångar mot fysiska och logiska intrång och annan yttre påverkan
- ☐ Åtgärder för att skydda tillgångar och förbindelser mot nederbörd, vind, blixtnedslag, fukt, skadliga temperaturer, översvämningar, jordskred och brand
- ☐ Säkerställande av att tester utförs innan ni genomför förändringar i kommunikationsnät eller kommunikationstjänster som kan orsaka störning eller avbrott av betydande omfattning

Störningar eller avbrott (Driftsincidenter)

8. Har ni system för att kontinuerligt upptäcka störningar och avbrott i era nät och tjänster?

- ☐ Ja
- ☐ Nej
- ☐ Vet ej

9. Har ni beredskap dygnet runt för att ta emot larm kring störningar och avbrott och initiera relevanta åtgärder?

- ☐ Ja
- ☐ Nej
- ☐ Vet ej

10. Hur många störningar och avbrott i era nät eller tjänster har inträffat under det senaste året? Ange antalet abonnentstörningstimmar (dvs. antal timmar * antal abonnenter) i snitt per år. Var god uppskatta.

- ☐ 0
- ☐ 0 – 99
- ☐ 100 – 999
- ☐ 1.000 – 9.999
- ☐ 10.000 – 99.999
- ☐ 100.000 – 499.999
- ☐ 500.000 eller fler
- ☐ Vet ej

11. Har ni under det senaste året, haft minst en störning eller avbrott som har inneburit kapacitetsbortfall i era nät eller tjänster enligt något av följande;

(Kapacitetsbortfall bör kunna beräknas som t.ex. andelen berörda aktiva anslutningar i förhållande till totala antalet aktiva anslutningar för tjänsten, andelen misslyckade samtalsförsök eller minskning av bandbredd i jämförelse med total bandbredd)

- ☐ 50 % kapacitetsbortfall eller mer under minst en timme
- ☐ 30 % kapacitetsbortfall eller mer under minst två timmar
- ☐ 20 % kapacitetsbortfall eller mer under minst 6 timmar
- ☐ 10 % kapacitetsbortfall eller mer under minst 24 timmar
- ☐ Vet ej

Skydd för behandlade uppgifter (integritetsskydd)

Begrepp

Informationsbehandlingstillgångar: system, databaser och fysiska tillgångar som används för informationsbehandling.

Behandlade uppgifter: uppgifter som behandlas i samband med tillhandahållande av tjänsten enligt 6 kap. 3 § LEK. Med behandling avses t.ex. insamling, registrering, lagring och bearbetning. Uppgifter är t.ex. det innehåll som överförs i kommunikationstjänsten, abonnentuppgifter, trafikuppgifter och lokaliseringsuppgifter som kan kopplas till den överförda informationen, till abonnemangsinnehavare eller till de användare som kommunicerar. Uppgifterna ska normalt röra eller kunna hänföras till en abonnent eller användare för att omfattas.

Integritetsincident: 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. Begreppet integritetsincidenter är relativt brett och kan t.ex. handla om att en faktura skickas till fel person, förlust av uppgifter i samband med mjukvaruuppdateringar eller att uppgifter tillfälligt inte kan kommas åt p.g.a. en överbelastningsattack.

Riskanalys

12. Hur ofta eller när analyserar ni risken för att integritetsincidenter inträffar för era informationsbehandlingstillgångar? Det är möjligt att ange ett eller flera svarsalternativ.

- ☐ Löpande, dock minst en gång per år
- ☐ Mer sällan än en gång per år
- ☐ Efter att integritetsincidenter har inträffat
- ☐ Vi genomför inte riskanalyser för informationsbehandlingstillgångar i vår verksamhet

Skyddsåtgärder

13. Har ni vidtagit några skyddsåtgärder för att minska risken för att integritetsincidenter inträffar för era informationsbehandlingstillgångar?

- ☐ Ja
- ☐ Nej
- ☐ Vet ej

Åtkomst- och behörighetshantering

Av PTS föreskrifter, PTSFS 2014:1 5 §, framgår att åtkomst till behandlade uppgifter endast ska ges till den som behöver det för att utföra sina arbetsuppgifter, har relevant utbildning med hänsyn till de uppgifter denne hanterar, och har upplysts om tystnadsplikten i 6 kap. 20-21 §§ lagen (2003:389) om elektronisk kommunikation. Behörigheter ska tilldelas i enlighet med detta (6 §).

14. Har ni dokumenterade rutiner för tilldelning, ändring och uppföljning av behörigheter?

- ☐ Ja
- ☐ Nej
- ☐ Vet ej

15. Har ni system för identitets- och åtkomsthantering som säkerställer att åtkomst endast medges i enlighet med tilldelade behörigheter?

- ☐ Ja
- ☐ Nej
- ☐ Vet ej

Loggning

16. Dokumenterar ni all läsning, kopiering, ändring och utplåning av behandlade uppgifter samt åtkomst till de system som används för behandling av sådana uppgifter?

- ☐ Ja
- ☐ Nej
- ☐ Vet ej

17. Om ja, kontrollerar ni dessa loggar systematiskt och återkommande?

- ☐ Ja
- ☐ Nej
- ☐ Vet ej

Skydd mot utplåning och förlust

18. Har ni vidtagit åtgärder för att säkerställa att behandlade uppgifter, som varaktigt lagras, skyddas mot oavsiktlig eller otillåten utplåning eller förlust, t.ex. genom säkerhetskopiering?

- ☐ Ja
- ☐ Nej
- ☐ Vet ej

19. Placerar ni informationsbehandlingstillgångar, där behandlade uppgifter varaktigt lagras, i utrymmen som har skydd mot intrång? (fysiskt skydd)

- ☐ Ja
- ☐ Nej
- ☐ Vet ej

Integritetsincidenter

Av PTS föreskrifter, PTSFS 2014:1 10 §, framgår att det ska finnas dokumenterade rutiner för identifiering, intern rapportering, hantering och uppföljning av integritetsincidenter. Av 6 kap. 4a § LEK framgår att inträffade integritetsincidenter ska rapporteras till PTS.

20. Har ni rutiner som säkerställer att all personal som behandlar uppgifter (t.ex. abonnentuppgifter och innehåll i elektroniska meddelanden) känner till reglerna om integritetsincidenter och intern incidentrapportering?

- ☐ Ja
- ☐ Nej
- ☐ Vet ej

Dokumentation och uppföljning

Dokumentation

21. Vilket av följande har ni dokumentation över? Det är möjligt att ange ett eller flera svarsalternativ.

Inom driftsäkerhet

- ☐ Rutiner och processer för arbetet med driftsäkerhet
- ☐ Förteckning över samtliga tillgångar och förbindelser
- ☐ Genomförda riskanalyser avseende tillgångar och förbindelser
- ☐ Vidtagna skyddsåtgärder med anledning av identifierade risker
- ☐ Inget av alternativen

Inom integritetsskydd

- ☐ Rutiner och processer för arbetet med skydd för behandlade uppgifter (integritetsskydd)
- ☐ Förteckning över samtliga informationsbehandlingstillgångar
- ☐ Genomförda riskanalyser avseende informationsbehandlingstillgångar
- ☐ Vidtagna skyddsåtgärder med anledning av identifierade risker
- ☐ Inget av alternativen

Uppföljning

22. Vilket av nedanstående följer ni upp minst årligen? Det är möjligt att ange ett eller flera svarsalternativ.

Inom driftsäkerhet

- ☐ Förteckning över samtliga tillgångar och förbindelser
- ☐ Genomförda riskanalyser
- ☐ Inträffade driftsincidenter
- ☐ Inget av alternativen

Inom integritetsskydd

- ☐ Förteckning över samtliga informationsbehandlingstillgångar
- ☐ Genomförda riskanalyser
- ☐ Inträffade integritetsincidenter
- ☐ Inget av alternativen

Tack för ditt deltagande!