Vår referens: 21–10016 **Aktbilaga:** 7

Tillsyn av rapporterad driftsäkerhetsincident 2020 och säkerhetsåtgärder

Part

AddSecure AB (Add Secure), 556527–2001

Saken

Tillsyn enligt lagen (2003:389) om elektronisk kommunikation

Post- och telestyrelsens avgörande

Post- och telestyrelsen (PTS) avslutar ärendet utan vidare åtgärd.

Bakgrund

PTS har sedan 2013 genomfört en årlig granskning av de driftsäkerhetsincidenter och integritetsincidenter som tillhandahållarna rapporterar till PTS i enlighet med krav i lagen (2003:389) om elektronisk kommunikation (LEK). I år genomförs tillsynen på ett ändrat sätt, främst genom att bara ett urval av incidentärendena har granskats och att fler tillhandahållare än tidigare omfattas av tillsynen.

Tillsynen har i år avgränsats till de driftsstörningsincidenter där tillhandahållarna meddelat att specifika säkerhetsåtgärder kommer att vidtas. Utöver det har incidenter som beror på problem med reservkraft eller redundans inkluderats och slutligen också den incident som orsakats av ett angrepp i form av en överbelastningsattack. Gränsdragningen har i år inneburit att tillsynen omfattat åtta tillhandahållare och sexton olika incidentrapporter från dessa åtta bolag.

Den incidentrapport som Add Secure givit in och som ingår i tillsynen rör en överbelastningsattack.

Skäl för beslutet

För tillämpliga bestämmelser se bilaga 1.

PTS bedömning

PTS konstaterar att Add Secure har vidtagit lämpliga säkerhetsåtgärder utifrån den driftsäkerhetsincident som har granskats. PTS ser positivt på att incidenthanteringen leder till investeringar och långsiktiga säkerhetsåtgärder för en förbättrad driftsäkerhet i elektroniska kommunikationsnät och -tjänster.

De åtgärder som Add Secure har vidtagit efter incidenten har varit åtgärder som förbättrar nätarkitekturen, såsom separerad funktionalitet, segregation av trafik, förbättrad larmstruktur och övervakning. De tekniska åtgärderna har följts av förbättrade organisatoriska åtgärder, vilket PTS ser positivt på.

Emellertid är dessa åtgärder av grundläggande slag. Det leder sammantaget till att PTS uppmanar Add Secure att fokusera än mer på det förebyggande och riskbaserade säkerhetsarbetet. Se bestämmelserna i 3, 5, 9, 10 och 14 §§ i PTS föreskrifter om krav på driftsäkerhet, se bilaga 1.

Tillsynen har sammanfattningsvis visat att Add Secure efter incidenten har vidtagit lämpliga tekniska och organisatoriska åtgärder för att öka förmågan att stå emot en liknande överbelastningsattack. Add Secure har också angett att de arbetar riskbaserat i enlighet med informationssäkerhetsstandarden ISO-27000. Detta riskbaserade arbetssätt ligger i linje med PTS föreskrifter om hur driftsäkerhetsarbete ska bedrivas.

Det finns därmed inte längre anledning för PTS att fortsätta tillsynen. Tillsynen avslutas därför utan åtgärd.

Beslutet har fattats av enhetschefen Anna Montelius. I ärendets slutliga handläggning har även Therese Braathen (föredragande) och Erika Hersaeus deltagit.

Bilaga 1

Tillämpliga bestämmelser

Här finns bestämmelser återgivna i relevanta delar för denna tillsyn

Tillsyn
Enligt 7 kap. 1 § lagen (2003:389) om elektronisk kommunikation (LEK) ska tillsynsmyndigheten bland annat ha tillsyn över efterlevnaden av lagen och de föreskrifter som har meddelats med stöd av lagen. Vad PTS har rätt att ta del av under en tillsyn framgår av 7 kap 2–3 §§ LEK, och vilka medel som PTS har för att skapa regelefterlevnad framgår av 7 kap 3 a -5 §§ LEK.

Driftsäkerhet i allmänt tillgängliga elektroniska kommunikationer
Enligt 5 kap 6 b § LEK framgår bland annat att den som tillhandahåller 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.

PTS föreskrifter om hur driftsäkerhetsarbetet ska bedrivas
Skyldigheterna i 5 kap 6 b § LEK preciseras i PTS föreskrifter om krav på driftsäkerhet (PTSFS 2015:2, ändrade genom PTSFS 2020:1).

Övergripande driftsäkerhetsarbete
I 3 § PTSFS 2015:2 beskrivs tillhandahållarens övergripande driftsäkerhetsarbete. Det föreskrivs att säkerhetsarbetet ska bedrivas långsiktigt, kontinuerligt och systematiskt. Arbetet ska omfatta såväl normala driftsförhållanden som extraordinära händelser.

Föreskrift om riskbaserat säkerhetsarbete
Det framgår av 5 § PTSFS 2015:2 när en tillhandahållare ska genomföra riskanalyser, bl.a. efter inträffade incidenter, och också vad riskanalyserna ska omfatta. Tillhandahållaren ska beakta erfarenheter från inträffade incidenter och ska tillämpa processer som utgår från etablerad standard på området.

Planering för och hantering av inträffade händelser som kan orsaka störningar eller avbrott
Enligt 7 § PTSFS 2015:2 ska tillhandahållaren bland annat säkerställa att åtgärder vidtas för att undvika liknande incidenter, och att erfarenheter från inträffade incidenter beaktas vid genomförande av riskanalyser enligt 5 §.

Vid vidtagande av åtgärderna ska tillhandahållaren tillämpa processer som utgår från etablerad standard på området.

Åtgärder efter riskbedömning
Det framgår av 9 § PTSFS 2020:1 att tillhandahållaren ska vidta åtgärder som föreskrivs i 10—12 §§. Tillhandahållaren ska också vidta åtgärder som är nödvändiga med hänsyn till den risk för störning eller avbrott som framkommit i tillhandahållarens riskbedömning enligt 5 och 5 a §§. För samtliga åtgärder ska en proportionalitetsbedömning göras. I den ska hänsyn tas till riskbedömningen, kostnader och verksamhetens art och omfattning.

Intrång, sabotage och annan yttre påverkan
Enligt 10 § PTSFS 2020:1 ska tillhandahållaren vidta åtgärder för att skydda tillgångar mot fysiska och logiska intrång, sabotage och annan yttre påverkan.

Åtgärder avseende övervakning och beredskap
Enligt 14 § PTSFS 2015:2 ska tillhandahållaren ha system som kontinuerligt övervakar kommunikationstjänster och aktiva delar i tillhandahållarens kommunikationsnät. Systemen ska generera larm vid störningar eller avbrott. Tillhandahållaren ska ha beredskap dygnet runt för att ta emot larm och initiera relevanta åtgärder.

PTS Beslutat av: Anna Montelius