Vår referens: 20–12815 **Aktbilaga:** 24

Telenor Sverige aktiebolag,
556421–030

Underrättelse om misstanke om bristande säkerhets- och skyddsåtgärder för externt trafikutbyte (extern BGP) på internet

Saken

Underrättelse enligt 7 kap. 4 § lagen (2003:389) om elektronisk kommunikation (LEK)

Post- och telestyrelsens underrättelse

Telenor Sverige aktiebolag (Telenor) underrättas om Post- och telestyrelsens (PTS) misstanke att Telenor brister i efterlevnad av 5 kap. 6 b § och 6 kap. 3 § LEK, 3 och 14 §§ i PTS föreskrifter om krav på driftsäkerhet (PTSFS 2015:2) samt 3 § och 4 § tredje stycket i PTS föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter (PTSFS 2014:1).

Den misstänkta bristen, utifrån dessa gällande regler och i förhållande till de förekommande och identifierade riskerna relaterade till extern BGP [1], är att Telenor inte vidtar tillräckliga säkerhets- och skyddsåtgärder när det gäller övervakning och larmgenerering i bolagets externa trafikutbyten på internet.

För att leva upp till gällande regler behöver Telenor använda ett övervaknings- och larmgenereringsverktyg som i realtid och på ett tillförlitligt sätt upptäcker, genererar larm och ger detaljerade rapporter om inträffade BGP-kapningar, BGP-läckor och andra BGP-relaterade incidenter i bolagets externa trafikutbyten över internet.

Telenor ges tillfälle att yttra sig över denna underrättelse **senast den 15 augusti 2022**. I yttrandet bör Telenor ange vilka åtgärder som bolaget har vidtagit eller avser att vidta med anledning av underrättelsen, samt när dessa beräknas vara vidtagna.

[1] BGP är en förkortning av Border Gateway Protocol. I denna underrättelse avses med BGP specifikt externa trafikutbyten, extern BGP eller eBGP. I rfc4271 (ietf.org) diskuteras och definieras BGP och eBGP.

PTS bedömer att rimlig tid för att vidta ovan nämnda åtgärder är till och med **årsskiftet 2022–2023**.

Telenor bör även yttra sig över bedömningen av rimlig tid för att vidta åtgärderna samt över i vilka nät som åtgärder kommer att vidtas och när. Telenor bör ange skäl i det fall några av Telenors nät inte kommer att omfattas av eventuella åtgärder. Om Telenor inte yttrar sig kan PTS komma att fatta beslut på det underlag som står till myndighetens förfogande.

Bakgrund

Border Gateway Protocol (BGP)

Border Gateway Protocol (BGP) är en kritisk funktion för att realisera elektroniska kommunikationstjänster och ovanpåliggande tjänster på internet. BGP:s uppgift är att hitta den snabbaste och mest effektiva vägen för att leverera ett meddelande från ett nät på internet, s.k. autonomt systemnät (AS), till ett annat autonomt systemnät på internet.

Protokollet BGP implementeras i tillgångar[2] och realiserar tjänster för att utbyta trafik externt på internet av bl.a. internet- och knutpunktsleverantörer. BGP implementeras således och används i tillhandahållarnas tillgångar som utbyter trafik externt på internet. Det handlar om tillgångar som tillhandahållaren förfogar över och därmed ansvarar för säkerheten i. Det externa trafikutbytet kan också benämnas extern BGP, eBGP eller extern routing. När BGP-protokollet konstruerades för många år sedan togs ingen större hänsyn till säkerhetsaspekter, vilket har lett till att routingsystemet idag har vissa välkända, fundamentala brister när det gäller att säkerställa att informationen i systemet är korrekt och tillförlitlig. Det vill säga det saknas mekanismer i protokollet för att säkerställa autenticitet och riktighet av routingmeddelanden (eller routingannonseringar) samt för att validera ett autonomt systemnät (AS) befogenhet att annonsera ett visst prefix eller skicka vidare route-information. BGP saknar även mekanism för att validera autenticiteten (äktheten) i s.k. path attribute i routingannonseringar. BGP-infrastrukturen är därmed sårbar för olika typer av avsiktliga attacker och oavsiktliga konfigurationsförändringar.

Om felaktiga routingannonseringar accepteras av tillhandahållare (s.k. peers i peering) och/eller sprids vidare, så ändras vägarna för paketen på internet. Konsekvensen av det är att trafik skickas till fel autonomt systemnät. Från detta nät kan det välja att vidareförmedla trafiken till den riktiga samt slutgiltiga destinationen i

[2] t.ex. i s.k. edge routrar, core routrar (för internettillhandahållare/ISP:er), route-servrar (för tillhandahållare av internetknutpunkter)

syfte att undvika uppmärksamhet. Denna typ av attack kan användas för att avlyssna, ändra eller avbryta internettrafiken.

När nät- och tjänstetillhandahållare (internetoperatörer eller internetknutpunktsleverantörer) genomför externa trafikutbyten[3] på internet gör de det genom att koppla samman sitt nät med andra operatörers och företags autonoma nät. Det kan ske med exempelvis s.k. edge routers eller core routers eller route-server i det fall tillhandahållaren är en s.k. knutpunktsleverantör. Trafikutbyten mellan näten realiseras genom två metoder/tjänster: *peering* och *transit*. I både peering- och transit-tjänsterna är extern BGP nödvändigt. Med peering avses när två eller flera internetoperatörers autonoma nätverk kopplar direkt till varandra för att utbyta trafik och det är en tjänst som internetoperatörerna i regel inte tar betalt för. Med transit avses när en tillhandahållare som tjänst till andra tillhandahållare tillåter trafik till och från andras nät att korsa deras autonoma nät. En tillhandahållares transittjänst vidareför således trafik mellan andras autonoma nät och andra nätverk för att trafiken över internet ska nå fram. Den som tillhandahåller transit tar betalt för tjänsten.

Risker och hot samt betydelsen av åtgärder för ett säkert externt trafikutbyte

Enligt branschinitiativet Mutually Agreed Norms for Routing Security (MANRS)[4] inträffar dussintals BGP-incidenter på internet dagligen och det har inträffat ett antal välkända och allvarliga BGP-incidenter hittills. Åtgärder för att stärka routingsäkerheten på internet beskrivs som mer nödvändiga än någonsin enligt MANRS, än mer på grund av ett förändrat säkerhetspolitiskt läge.[5]

MANRS beskriver gemensamma normer och säkerhetsåtgärder som har en särskilt stor betydelse för att åstadkomma säkrare routing på internet (extern BGP).

Även Europeiska unionens cybersäkerhetsbyrå Enisa har givit ut en vägledning för en säkrare användning av BGP[6] och det regionala internetregistret och certifikatutfärdaren RIPE NCC beskriver varför RPKI är en nödvändig åtgärd för ett säkrare externt trafikutbyte.[7]

PTS tillsyn

PTS inledde den 1 oktober 2020 tillsyn över ett urval av tillhandahållare av elektroniska nät och tjänster för att granska tillhandahållarnas tekniska och

[3] Se definition av externt trafikutbyte I PTS-ER 2007:14 s.53

[4] MANRS – Mutually Agreed Norms for Routing Security

[5] Se bland annat: A Regional Look into BGP Incidents in 2020 (manrs.org), BGP Security in 2021 (manrs.org)

[6] 7 Steps to shore up the Border Gateway Protocol (BGP) — ENISA (europa.eu) och Did Ukraine suffer a BGP hijack and how can networks protect themselves? (manrs.org)

[7] Resource Public Key Infrastructure (RPKI) — RIPE Network Coordination Centre

organisatoriska säkerhetsåtgärder med anledning av kända sårbarheter förknippade med extern BGP. Telenor är ett av bolagen som omfattas av tillsynen.

I tillsynen har PTS utifrån gällande regler granskat bolagets riskanalys samt bolagets riskhantering och vidtagande av säkerhets- och skyddsåtgärder. I granskningen har PTS utgått ifrån branschöverenskommelser inom MANRS och också RIPE NCC:s beskrivning av varför RPKI är en nödvändig åtgärd. PTS har vidare granskat om bolaget följer samtliga sju angivna steg i Enisas vägledning för en säkrare användning av BGP. Dessa sju steg är: upprättande av förmåga att upptäcka avvikelser i externt trafikutbyte, filtrering av IP-prefix, filtrering utifrån BGP AS-Path, Bogon-filtrering[8], säkerställande av korrekt kontaktinformation i vedertagna allmänna routingdatabaser, TTL-säkerhet (GTSM) samt användning av RPKI.[9]

Under tillsynens gång har PTS följt upp bolagets säkerhetsarbete, riskanalys, vidtagna åtgärder och kontrollerat om utfästa åtgärder har genomförts utifrån bolagets angivna planering och införandetidpunkter.

Telenors uppgifter om sin övervaknings- och larmfunktionalitet avseende BGP-incidenter i externa trafikutbyten

Telenor har sammanfattningsvis uppgett följande:

Telenor uppgav under december 2020 att ett nytt övervakningssystem skulle implementeras för att skapa bättre granularitet i loggning och övervakning av BGP-avvikelser, och förbättrad förmåga att upptäcka om en tredje part felaktigt annonserar bolagets prefix. Arbetet uppgavs som prioriterat och införandetiden angavs till 2021. Telenor uppgav vidare att bolaget inte har någon övervakning av route-annonseringar av egna prefix för att upptäcka om andra felaktigt försöker routa trafik till tredje part. Telenor får löpande information från RIPE RIS om Telenors prefix har status *RPKI Invalid*. Telenor har också möjlighet att få så kallade *traps* från ett annat bolag vid BGP-kapningar av Telenors prefix, men bara från Tier1 och Tier2 som detta bolag har avtal med. Telenor är inte medlem i MANRS men följer långtgående MANRS regelverk och det kan vara aktuellt att bli medlem i och med den nya plattformen.

I oktober 2021 uppgav Telenor att tester pågick före införandet av det nya övervakningssystemet. Målet var att systemet skulle vara i drift under 2022.

I februari 2022 uppgav Telenor att arbetet med det nya övervakningssystemet inte längre är en prioriterad aktivitet och bolaget inte kan ange en tid för när driftsättning kommer ske. Telenor angav vidare att den långsiktiga planen är att implementera övervakningssystemet internt, vilket leder till förmåga att upptäcka avvikelser i iBGP.

[8] ”falska” IP-adresser på ett nätverk på internet – dvs. IP-adresser som exempelvis inte har allokerats eller delegerats från Internet Assigned Numbers Authority (IANA) eller en Regional Internet Registry

[9] Se fotnoter 7 – 13 för vidare läsning.

Vidare meddelade Telenor att bolaget bedriver ett intensivt, komplext och resurskrävande arbete med att utveckla ett nytt nät med anledning av PTS licenskrav för nya nät. Åtgärder som införs i det befintliga nätet blir kortlivade och tar resurser från utvecklingen av det nya nätet. Åtgärder behöver därför vara drivna av behov. Prioriteringar av åtgärder bygger på Telenors riskanalyser. Telenor gör avvägningar mellan vad som måste implementeras i nuvarande nät och vad som behöver implementeras i det nya nätet.

Tillämpliga bestämmelser

Av 7 kap. 4 § LEK framgår att om PTS finner skäl att misstänka att den som bedriver verksamhet enligt denna lag inte efterlever lagen eller de beslut om skyldigheter eller villkor eller de föreskrifter som har meddelats med stöd av lagen, ska myndigheten underrätta den som bedriver verksamheten om detta förhållande och ge denne möjlighet att yttra sig inom skälig tid.

Enligt 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 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.

Enligt 6 kap. 3 § LEK ska den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att uppgifter som behandlas i samband med tillhandahållandet av tjänsten skyddas. Den som tillhandahåller ett allmänt kommunikationsnät ska vidta de åtgärder som är nödvändiga för att upprätthålla detta skydd i nätet. Åtgärderna ska vara ägnade att säkerställa en säkerhetsnivå som, med beaktande av tillgänglig teknik och kostnaderna för att genomföra åtgärderna, är anpassad till risken för integritetsincidenter.

Enligt 2, 30 och 34 a §§ förordningen (2003:396) om elektronisk kommunikation (FEK) är PTS tillsynsmyndighet enligt LEK och myndigheten har bemyndigande att meddela föreskrifter om skyldigheter och åtgärder enligt 5 kap. 6 b § och 6 kap. 3 § LEK.

I 3 § PTSFS 2015:2 föreskrivs att tillhandahållarens säkerhetsarbete ska bedrivas långsiktigt, kontinuerligt och systematiskt. Arbetet ska omfatta såväl normala driftsförhållanden som extraordinära händelser.

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.

I 3 § PTSFS 2014:1 framgår att tillhandahållares säkerhetsarbete avseende behandlade uppgifter ska bedrivas långsiktigt, kontinuerligt och systematiskt.

I 4 § tredje stycket PTSFS 2014:1 framgår att tjänstetillhandahållaren ska vidta de skyddsåtgärder som föreskrivs i 6–9 §§ liksom andra nödvändiga skyddsåtgärder, på den nivå som är lämplig för att hantera de identifierade riskerna.

PTS bedömning

Extern BGP spelar en central roll för att säkerställa tillförlitliga och driftsäkra elektroniska nät och tjänster. Eftersom utnyttjande av sårbarheter och hot relaterade till BGP leder till allvarliga incidenter med dominoeffekter för andra internetleverantörer och för slutanvändare, behöver tillhandahållare arbeta aktivt med att vidta lämpliga säkerhets- och skyddsåtgärder i förhållande till föreliggande risker och sårbarheter relaterade till extern BGP, aktuella hot, tillgänglig teknik och branschens gemensamt utformade rekommendationer för säkrare externa trafikutbyten.

Incidenter i externa trafikutbyten på internet kan få mycket allvarliga konsekvenser. Incidenterna kan innefatta att kommunikationsströmmar omdirigeras till obehöriga eller att trafikmönster eller kommunikation avlyssnas, och de kan också leda till störningar och avbrott i elektroniska kommunikationstjänster. Konsekvenserna av sådana incidenter drabbar inte bara den drabbade tillhandahållaren, utan ännu mer enskilda konsumenter, företag och organisationer, andra internetoperatörer och även stater. Det är därför nödvändigt att tillhandahållare vidtar lämpliga åtgärder för att skydda det externa trafikutbytet mot utnyttjande av sårbarheter och mot avsiktliga BGP-kapningar eller oavsiktliga felkonfigureringar i extern BGP.

Telenor är en tillhandahållare av allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster. Telenor har ett ansvar enligt lag och föreskrifter att vidta lämpliga tekniska och organisatoriska åtgärder dels för att säkerställa att verksamheten uppfyller rimliga krav på driftsäkerhet, dels för att säkerställa att uppgifter som behandlas i samband med tillhandahållandet av tjänsterna skyddas. Vilka åtgärder som ska vidtas framgår av PTS föreskrifter om krav på driftsäkerhet (PTSFS 2015:2, ändrade genom 2020:1) och om skyddsåtgärder för behandlade uppgifter (PTSFS 2014:1).

Telenor har i tillsynen visat att de vidtar olika säkerhetsåtgärder för att motverka sårbarheter och hot relaterade till extern-BGP och bolaget lever upp till kraven i

gällande regler i dessa delar. PTS har dock identifierat en misstänkt brist i säkerhetsarbetet.

PTS har i sin bedömning lagt vikt vid vad MANRS,[10] RIPE NCC,[11] Enisa[12] har uttalat om vad som är vägledande normer och nödvändiga eller grundläggande åtgärder för routingsäkerhet.

Enisa anger i sin vägledning sju relevanta åtgärder för att motverka sårbarheter och hot i anledning av BGP. Telenor uppfyller flera av de sju stegen i sitt säkerhetsarbete. Den punkten i Enisas vägledning om att upprätta förmåga att upptäcka avvikelser i externt trafikutbyte är av relevans för PTS misstanke om brister i denna underrättelse.

För att uppnå en nödvändig säkerhets- och skyddsnivå som motverkar hot relaterade till sårbarheter i BGP, behövs enligt PTS bedömning en kombination av åtgärder i ett systematiskt och förebyggande säkerhetsarbete, såsom bl.a. användande av RPKI i både peering- och transittjänster (vilket Telenor har), och också realtidsövervakning och larm för felaktiga BGP-annonseringar i externa trafikutbyten på internet, utöver de åtgärder som Telenor redan vidtar.

Avsaknad av kontinuerlig och ändamålsenlig övervakning och larmfunktioner

Av 14 § PTSFS 2015:2 framgår ett krav på att tillhandahållaren ska ha system som kontinuerligt övervakar kommunikationstjänster och aktiva delar i tillhandahållarens kommunikationsnät, att systemen ska generera larm vid störningar eller avbrott, samt att tillhandahållaren ska ha beredskap dygnet runt för att ta emot larm och initiera relevanta åtgärder. PTS misstänker att Telenors nuvarande övervakningsförmåga över BGP-kapningar och liknande i externa trafikutbyten på internet inte lever upp till dessa krav. Misstanken är att Telenor har en otillräcklig förmåga att upptäcka och reagera på BGP-kapningar och BGP-läckor i Telenors nät och tjänster, samt en otillräcklig förmåga att dygnet runt kunna initiera relevanta åtgärder mot BGP-kapningar och BGP-läckor i bolagets externa trafikutbyten på internet.

PTS misstänker också att bristen innebär att bolaget inte vidtar nödvändiga åtgärder för skydd av uppgifter på den nivå som är lämplig för att hantera de identifierade riskerna i externa trafikutbyten i enlighet med 4 § tredje stycket PTSFS 2014:1. Skyddet av behandlade uppgifter behöver övervakas kontinuerligt och systematiskt, för att leva upp till en lämplig nivå med dagslägets kännedom om risker i och med BGP och den teknik som finns tillgänglig. PTS misstänker slutligen också att bristerna som har beskrivits ger en otillräcklig förmåga att kunna genomföra säkerhetsarbetet

[10] MANRS – Mutually Agreed Norms for Routing Security och MANRS Network Operators Actions v2.5.2
[11] Resource Public Key Infrastructure (RPKI) — RIPE Network Coordination Centre
[12] 7 Steps to shore up the Border Gateway Protocol (BGP) — ENISA (europa.eu)

mot kända risker och sårbarheter i och med BGP på ett långsiktigt, kontinuerligt och systematiskt sätt vilket krävs enligt 3 § PTSFS 2015:2 samt 3 § PTSFS 2014:1.

Det är enligt PTS bedömning inte tillräckligt att Telenor tar emot varningar eller förlitar sig på att en annan tillhandahållare (Tier1 eller Tier2 som Telenor har angett) arbetar för att upptäcka och minska konsekvenser av BGP-incidenter med Telenors prefix eller i Telenors externa trafikutbyten på internet. Telenor behöver självt övervaka, generera larm och ha dygnet runt beredskap vad avser egna prefix, tjänster och nät i enlighet med PTS föreskrifter. Det är inte heller tillräckligt att implementera övervakning endast för iBGP (internal BGP avser endast det egna autonoma systemnätet).

Den övervakning och larmfunktionalitet som är nödvändig med hänsyn till dagslägets risker och dagslägets tillgängliga teknik, ska så långt som möjligt reagera i realtid för att kunna upptäcka, och därefter ge förmåga att snabbt begränsa konsekvenser av framför allt BGP-kapningar och BGP-läckor i externa trafikutbyten. Övervakningsverktyget ska ge systemgenererade larm i realtid och det ska finnas beredskap dygnet runt för att agera på larmen, annars riskerar störningar och avbrott, eller kapad eller avlyssnad trafik, att förbli oupptäckt eller onödigt utdraget i tiden då åtgärder uteblir eller försenas.

För att uppnå kraven i 3 § och 14 § PTSFS 2015:2 och 3 § och 4 § tredje stycket PTSFS 2014:1 behöver Telenor därför införa ett tillförlitligt övervakningssystem som så långt som möjligt kan reagera i realtid och som genererar larm och bevakas såväl för iBGP som för eBGP.

PTS har i bedömningen även beaktat Telenors förutsättningar och riskerna, även i förhållande till att Telenor nu bygger ett nytt nät, samt kostnaderna i förhållande till den tillgängliga tekniken.

Telenor får tillfälle att yttra sig

PTS finner sammanfattningsvis att myndigheten enligt 7 kap. 4 § LEK ska underrätta Telenor om att myndigheten misstänker att Telenor agerar i strid med 5 kap. 6 b § och 6 kap. 3 § LEK samt 3 och 14 §§ i PTS föreskrifter om krav på driftsäkerhet (PTSFS 2015:2) och slutligen även 3 § och 4 § tredje stycket i PTS föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter (PTSFS 2014:1).

Telenor ges tillfälle att yttra sig över denna underrättelse **senast den 15 augusti 2022**.

När tiden för att inkomma med yttrande har löpt ut kan PTS med stöd av 7 kap. 5 § LEK komma att meddela föreläggande som behövs för att Telenor ska vidta nödvändiga åtgärder för rättelse. Eventuellt föreläggande kan komma att förenas

med vite. Om Telenor inte alls hörs av kan PTS ändå komma att fatta beslut på det underlag som står till myndighetens förfogande.

Ett beslut om underrättelse enligt 7 kap. 4 § LEK får enligt 8 kap. 21 § samma lag inte överklagas.

Johanna Eklund

Underrättelsen har beslutats av tf enhetschefen Johanna Eklund

Föredragande har varit Therese Braathen. I ärendets slutliga handläggning har även Erika Hersaeus och verksjuristen Emma Edsjö deltagit.