Vår referens: 20–11180 **Aktbilaga:** 32

Tillsyn över säkerhetsarbete i externt trafikutbyte (extern BGP) på internet

Part

Telia Company AB, 556103–4249

Saken

Tillsyn enligt lagen (2003:389) om elektronisk kommunikation

Post- och telestyrelsens beslut

Post- och telestyrelsen (PTS) avslutar ärendet mot Telia Company AB (Telia) utan vidare åtgärd.

Bakgrund

Border Gateway Protocol (BGP)

BGP[1] 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. 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

[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.

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

Post- och telestyrelsen
Postadress: Box 6101, 102 32 Stockholm
Besöksadress: Hälsingegatan 38
Telefon: 08-678 55 00
E-post: pts@pts.se
www.pts.se

autonomt systemnäts (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) 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 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), och det regionala internetregistret och certifikatutfärdaren RIPE NCC beskriver varför RPKI är en nödvändig åtgärd för ett säkrare externt trafikutbyte.[6]

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

Europeiska unionens cybersäkerhetsbyrå Enisa har dessutom givit ut en vägledning med sju specifika steg i arbetet för en säkrare användning av BGP[7]. Enisas sju steg består av följande: 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]

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 organisatoriska säkerhetsarbete med anledning av kända sårbarheter förknippade med extern BGP. Telia 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. Under tillsynens gång har PTS följt upp säkerhetsarbete, vidtagna åtgärder och kontrollerat om eventuella utfästa åtgärder har genomförts utifrån bolagets angivna införandetidpunkter.

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

[7] 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)

[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.

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.

Av 9 § PTSFS 2015:2, ändrad genom 2020:1, framgår att tillhandahållaren ska vidta de åtgärder som föreskrivs i 10—12 §§, samt de ytterligare åtgärder som är nödvändiga med hänsyn till den risk för störning eller avbrott som framkommit i tillhandahållarens riskbedömning enligt 5 och 5 a § §. Vidare framgår bl.a. att åtgärderna ska vidtas på den nivå som är proportionerlig med hänsyn till riskbedömningen, de kostnader som är förenade med åtgärden samt verksamhetens art och omfattning.

Enligt 10 § PTSFS 2015:2, ändrad genom 2020:1 ska tillhandahållaren vidta åtgärder för att skydda tillgångar mot fysiska och logiska intrång, sabotage och annan ytTelia påverkan.

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

Betydelsen av säkerhetsåtgärder i externa trafikutbyten

Extern BGP spelar en central roll för att säkerställa tillförlitliga och driftsäkra elektroniska nät och tjänster. Utnyttjanden eller andra händelser orsakade av sårbarheter och hot relaterade till BGP leder till allvarliga incidenter med dominoeffekter för andra internetleverantörer och för slutanvändare. Tillhandahållare behöver på grund av detta 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.

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.

Bolagets säkerhetsarbete och vidtagna åtgärder

Telia har i tillsynen på ett bra sätt redogjort för sitt arbete med att identifiera relevanta aktuella sårbarheter samt hot mot extern BGP, upprättat riskanalys över dessa och visat att bolaget arbetar långsiktigt, kontinuerligt och systematiskt i säkerhetsarbetet och med åtgärder för att motverka de kända riskerna och sårbarheterna i externa trafikutbyten.

PTS bedömer att bolagets redovisade säkerhetsarbete och vidtagna åtgärder lever upp till 3 § och 14 § PTSFS 2015:2, 9–10 §§ PTSFS 2015:2, ändrade genom PTSFS 2020:1, samt 3 och 4 §§ PTSFS 2014:1.

Mot bakgrund av det ovanstående finns det inte skäl att fortsätta tillsynen och den avslutas därför utan åtgärd.

Johanna Eklund

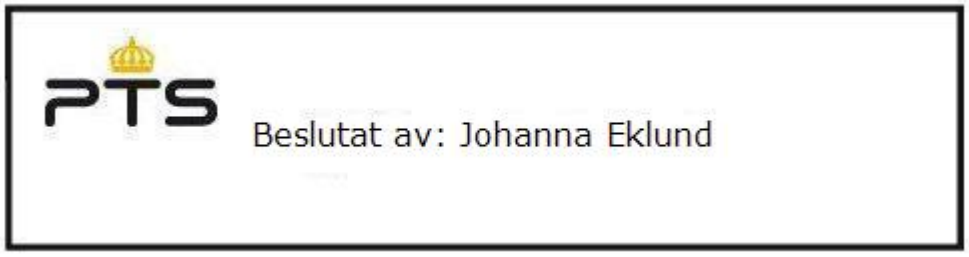
Underrättelsen har beslutats av tf enhetschefen Johanna Eklund

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

[10] MANRS for IXPs och MANRS – Mutually Agreed Norms for Routing Security

[11] Resource Public Key Infrastructure (RPKI) — RIPE Network Coordination CenTelia

[12] 7 Steps to shore up the Border Gateway Protocol (BGP) — ENISA (europa.eu)


PTS
Beslutat av: Johanna Eklund