Vår referens: 20–11178 **Aktbilaga:** 21

Netnod Internet Exchange AB,
556534–0014

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

Netnod Internet Exchange AB (Netnod) underrättas om Post- och telestyrelsens (PTS) misstanke att Netnod 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) och 9–10 §§ i PTSFS 2015:2, ändrade genom PTSFS 2020:1, samt 3 § och 4 § tredje stycket i PTS föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter (PTSFS 2014:1).

De misstänkta bristerna, utifrån dessa gällande regler och i förhållande till de förekommande och identifierade riskerna relaterade till extern BGP [1] i externa trafikutbyten på internet, är att Netnod:

1. inte vidtar tillräckliga säkerhets- och skyddsåtgärder i bolagets tillhandahållande av externt trafikutbyte i transittjänster.

2. inte vidtar tillräckliga säkerhets- och skyddsåtgärder när det gäller övervakning och larmgenerering i bolagets externa trafikutbyten i peering- och transittjänster.

[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.

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

För att leva upp till gällande regler behöver Netnod:

1. Införa och använda Resource Public Key Infrastructure (RPKI)[2] (kryptografiskt valideringsbara routinguppgiftsannonseringar/-meddelanden) även i bolagets tillhandahållande av transittjänst, för att filtrera bort felaktiga routingmeddelanden eller påståenden.

2. 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.

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

I yttrandet bör Netnod ange vilka åtgärder som bolaget har vidtagit eller avser att vidta med anledning av underrättelsen, samt när dessa beräknas vara vidtagna.

PTS bedömer att rimlig tid för att vidta ovan nämnda åtgärder är till och med **årsskiftet 2022–2023**. Netnod bör yttra sig över bedömningen av rimlig tid för att vidta åtgärderna. Om Netnod inte yttrar sig eller vidtar rättelse inom angiven rättelsetid 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[3] 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-

[2] RPKI definieras i RFC6810 med titeln *The Resource Public Key Infrastructure (RPKI) to Router Protocol* och finns beskrivet i RFC6480 med titeln *An Infrastructure to Support Secure Internet Routing.*

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

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 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[4] 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.

Säkerhetsåtgärden Resource Public Key Infrastructure (RPKI)

Resource Public Key Infrastructure, RPKI[5], har tagits fram som det globala ramverket och säkerhetslösningen av det tekniska internetsamfundet i syfte att kunna säkerställa autenticitet och riktighet i BGP-annonseringar och därmed förbättra routingsäkerheten.

RPKI är en funktionalitet som ger tillhandahållare möjlighet att skapa kryptografiskt signerade samt valideringsbara uttalanden om BGP-annonseringar. Dessa uttalanden kallas för Route

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

[5] RFC 6480 - An Infrastructure to Support Secure Internet Routing (ietf.org)

Origin Authorisations (ROA[6]). Ett ROA är ett certifikat som talar om vilket autonomt system (AS), nät på internet som en tillhandahållare förfogar över, som är auktoriserat att originera en viss sammanhängande IP-adressmängd (s.k. prefix eller adressutrymme). Det vill säga RPKI tillstyrker kopplingen mellan prefix, autonomt systemnät och innehavaren av aktuella prefix. Certifikaten bevisar kryptografiskt prefixinnehavarens rättighet att annonsera sina prefix och kan kryptografiskt valideras.

För att tillämpa RPKI behöver en tillhandahållare vidta två åtgärder.[7] Den första är att tillhandahållaren efterfrågar ett kryptografiskt certifikat över sina prefix hos RIPE NCC[8]. Den andra åtgärden är att tillhandahållarens utrustning som realiserar extern BGP, t.ex. edge och coreroutrar, installeras med och tillämpar RPKI-mjukvara. Genom tillhandahållares tillämpning av RPKI-mjukvaran för sitt autonoma nät[9] valideras riktigheten och autenticiteten av genomförda BGP-annonseringar (“Valid”, “Invalid”, “Unknown”).

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

Enligt branschinitiativet Mutually Agreed Norms for Routing Security (MANRS)[10] 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.[11]

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

Även Europeiska unionens cybersäkerhetsbyrå Enisa har givit ut en vägledning för en säkrare användning av BGP[12] och det regionala internetregistret och certifikatutfärdaren RIPE NCC beskriver varför RPKI är en nödvändig åtgärd för ett säkrare externt trafikutbyte.[13]

[6] Managing ROAs — RIPE Network Coordination Centre

[7] Managing ROAs — RIPE Network Coordination Centre

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

[9] BGP Origin Validation — RIPE Network Coordination Centre

[10] MANRS – Mutually Agreed Norms for Routing Security

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

[12] 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)

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

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 säkerhetsåtgärder med anledning av kända sårbarheter förknippade med extern BGP. Netnod är ett av bolagen som omfattas av tillsynen. Netnod är en internetknutpunktsleverantör (IXP). Netnod har hand om Sveriges och de nordiska ländernas anslutning till internet och hanterar DNS. Netnod sköter en av internets rotservrar.

I tillsynen har PTS utifrån gällande regler granskat bolagets riskanalys samt bolagets riskhantering och vidtagande av säkerhets- och skyddsåtgärder. I granskningen har PTS beaktat ifrån branschöverenskommelser inom MANRS, beaktat MANRS åtgärdspaket om grundläggande säkerhetsåtgärder för IXPs[14], 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[15], säkerställande av korrekt kontaktinformation i vedertagna allmänna routingdatabaser, TTL-säkerhet (GTSM) samt användning av RPKI.[16]

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.

Netnods uppgifter angående införande och användning av RPKI i transittjänst

Netnod har inledningsvis under tillsynen, i oktober 2020, uppgett att RPKI, vid sidan av att det tillämpas i bolagets peeringtjänst, även kommer att införas och användas i bolagets transittjänst och att införandet skulle ske under det första kvartalet 2021.

Netnod inkom, efter fråga från PTS efter första kvartalet 2021, med uppgifter om en försening, på grund av försening av en stabil leverans av RPKI-mjukvaran från leverantör, samt med en ny planerad sluttid för införandet. Netnod angav då att RPKI kommer att vara infört under det tredje kvartalet 2021.

Efter ytterligare fråga om införandet från PTS under det tredje kvartalet 2021 inkom Netnod med en ny tid för införande. Netnod angav då att bolaget sedan oktober 2021 har RPKI-programvara tillgänglig och att RPKI kommer att vara infört i transittjänst under det andra

[14] MANRS for IXPs

[15] ”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

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

kvartalet 2022. Netnod informerade dock samtidigt att åtgärden avseende RPKI i transittjänst inte är högt prioriterad eftersom Netnod inte anser sig vara en större tillhandahållare av transittjänst.

I januari 2022 angav Netnod slutligen och sammanfattningsvis följande. Netnod uppnår tillräcklig routingsäkerhet genom ROA på sina egna prefix och att validering görs i route-servrar för bolagets peeringtjänster sedan flera år. Transittjänst ingår inte i Netnods huvudsakliga tjänster. Netnods transittjänstkunder som använder egna prefix ska se till att ROA finns på deras egna prefix. Programvaran för RPKI finns tillgänglig hos Netnod sedan oktober 2021, men Netnod angav i detta läge att Netnods hårdvara för transit inte är dimensionerad för att hantera aktuell informationsmängd. RPKI ska installeras i transit så fort det går, men annan utvecklingsverksamhet prioriteras högre.

Netnods uppgifter om sin övervaknings- och larmfunktionalitet avseende BGP-incidenter

Netnod har inledningsvis under tillsynen, i oktober 2020, uppgett att bolaget inom kort avser att implementera ett nytt, mer tillförlitligt och snabbare övervaknings-system. Övervaknings- och larmfunktionaliteten kommer i och med det att förbättras och effektivare kunna upptäcka BGP-kapningar. Netnod uppgav också att det nya övervakningssystemet kommer ta in extern routinginformation utöver data från den egna routinginfrastrukturen. Netnod angav vidare att, med det nya systemet, kommer bolaget att kunna ställa in samt erhålla larm mer frekvent än med dagens övervakningstjänst och öka mängden larm, och därmed skapa en förbättrad övervakning av BGP-kapningar som avser Netnods prefix.

Netnod uppgav vidare, i svar till PTS under första respektive tredje kvartalet 2021, att det nya övervakningssystemet inte har införts enligt planeringen och att införandet inte är prioriterat utan skjuts på framtiden eftersom bolaget redan använder andra övervakningslösningar.

I januari 2022 angav Netnod slutligen och sammanfattningsvis följande. Det nuvarande övervakningssystemet ger Netnod en rapport om falska annonseringar på veckobasis och att det kan leda till ett larm. Netnod planerar ett införande av nytt övervakningsverktyg. Det nya verktyget innebär även möjlighet till automatisk mitigering, mer finmaskighet och bättre kontroll av inställningar i verktyget, i jämförelse med nuvarande verktygets grövre kontroll. Det nya systemet ska ersätta det nuvarande, men Netnod kan inte motivera en prioritering och inte ange ett datum p.g.a. en mängd faktorer. När det gäller implementering har Netnod angett att det kommer att införas på sikt men finns tillgängligt för bolaget i februari 2022.

Det är möjligt att även ytterligare verktyg kommer att implementeras på sikt. Netnod påtalar vidare att en falsk annonsering påverkar alla Netnods driftställen. Men också att i grunden är både det nuvarande och det nya systemet övervakningssystem och inget annat. Det nuvarande systemet ger tillräcklig säkerhet vid routing.

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.

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 yttre 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

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.

Netnod är en internetknutpunktsleverantör och som sådan tillhandahållare av allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster. Netnod 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).

Netnod 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 några misstänkta brister i säkerhetsarbetet.

PTS har i sin bedömning lagt vikt vid vad MANRS,[17] RIPE NCC,[18] Enisa[19] har uttalat om vad som är vägledande normer och nödvändiga eller grundläggande åtgärder för routingsäkerhet.

Det PTS fäster särskilt avseende vid, utifrån Enisas vägledning, är Enisas angivna åtgärder om att upprätta förmåga att upptäcka avvikelser i externt trafikutbyte, filtrera IP-prefix samt använda RPKI.

För att uppnå en nödvändig säkerhets- och skyddsnivå som motverkar risker för att hot relaterade till sårbarheter i BGP realiseras, behövs enligt PTS bedömning en kombination av förebyggande säkerhetsarbete, såsom bl.a. användande av RPKI i både peering- och transittjänster, och realtidsövervakning och larm för felaktiga BGP-annonseringar i externa trafikutbyten, utöver de åtgärder som Netnod redan vidtar.

Misstänkta brister enligt 9 och 10 §§ PTSFS 2015:2, ändrade genom PTSFS 2020:1 samt 3 och 14 § i PTSFS 2015:2

Enligt 3 § PTSFS 2015:2 ska tillhandahållarens säkerhetsarbete bedrivas långsiktigt, kontinuerligt och systematiskt.

Enligt 9 och 10 §§ PTSFS 2015:2, ändrade genom PTSFS 2020:1, ska tillhandahållaren vidta åtgärder för att skydda tillgångar mot fysiska och logiska intrång, sabotage och annan yttre påverkan.

I 14 § PTSFS 2015:2 framgår kravet på att tillhandahållaren ska ha system som kontinuerligt övervakar kommunikationstjänster och aktiva delar i tillhandahållarens kommunikationsnät och att det ska genereras larm vid störningar eller avbrott.

Avsaknad av användning av RPKI i transittjänster

BGP-kapningar och BGP-läckor i tillhandahållares nät och tjänster är enligt PTS att jämställa med sådan yttre påverkan som tillhandahållare ska vidta åtgärder för att skydda sina tillgångar mot enligt reglerna i 9 § och 10 § PTSFS 2015:2, ändade genom PTSFS 2020:1. RPKI är den säkerhetslösning som har tagits fram för att kunna säkerställa autenticitet och riktighet i BGP-annonseringar och därmed förbättra routingsäkerhet. Enligt ENISA:s

[17] MANRS for IXPs
och MANRS – Mutually Agreed Norms for Routing Security
[18] Resource Public Key Infrastructure (RPKI) — RIPE Network Coordination Centre
[19] 7 Steps to shore up the Border Gateway Protocol (BGP) — ENISA (europa.eu)

vägledning om routingsäkerhet, vilket är i enlighet med PTS bedömning, ska tillhandahållare av allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster, samt andra organisationer som sköter operationell drift av ett autonomt systemnät, AS, implementera RPKI.

Netnod använder RPKI i peeringtjänster, vilket PTS ser positivt på.

Användning av RPKI även i transittjänst, skulle ge Netnod förmåga att filtrera bort felaktiga routingmeddelanden även för trafik som av Netnod endast tillåts passera genom Netnods nät i transit. PTS anser att även sådan trafik ska skyddas av Netnod i Netnods nät och tjänster. Det är inte tillräckligt att Netnods transittjänstkunder som använder egna prefix ska se till att ROA finns på deras egna prefix. Att installera RPKI-mjukvara i de egna BGP-tillgångarna för att detektera och filtrera oönskad trafik i det egna nätet, så att inkorrekt adressering kastas bort även i Netnods transittjänster, krävs alltså för att Netnod ska leva upp till kraven enligt 9–10 §§ PTSFS 2015:2. Netnod har också, enligt egna uppgifter, mjukvara för RPKI tillgänglig.

Avsaknad av kontinuerlig och ändamålsenlig övervakning och larmfunktioner

Netnods nuvarande övervakningssystem har enligt Netnods uppgifter en grov övervakningsförmåga, som ger Netnod rapport om BGP-incidenter i det egna nätet en gång per vecka. Netnod saknar därmed förmåga att upptäcka och reagera på BGP-kapningar och BGP-läckor i realtid. Netnod har även uppgett att det nuvarande övervakningsverktyget inte har hög tillförlitlighet eftersom det har en begränsad användning av routinginformation från externa routingdatabaser.

Ett sådant övervakningsverktyg som Netnod använder i nuläget kan enligt PTS bedömning inte anses uppfylla kraven på övervakningssystem i 14 § PTSFS 2015:2. En veckovis rapport om BGP-avvikelser och -incidenter kan inte motsvara föreskriftskravet på kontinuerlig övervakning. Den nuvarande åtgärden ger inte Netnod tillräcklig förmåga att kunna agera kontinuerligt och motverka konsekvenser av bland annat BGP-kapningar och BGP-läckor. PTS misstänker därför att Netnods nuvarande övervakningsförmåga inte lever upp till kraven om övervakning, larm och beredskap i 14 § PTSFS 2015:2.

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. 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 14 § PTSFS 2015:2 behöver Netnod införa det planerade och för Netnod tillgängliga övervaknings- och larmsystemet eller annat jämförbart sådant. När det gäller det av Netnod angivna planerade nya övervakningsverktyget finns programvaran tillgänglig på marknaden som opensource-programvara. För Netnod krävs således att programvaran installeras, konfigureras och börjar tillämpas för Netnods tjänster i enlighet med gällande bestämmelser.

Misstänkta brister enligt 3 § PTSFS 2015:2 och 3–4 §§ PTSFS 2014:1

PTS misstänker att Netnod genom ovanstående brister inte heller efterlever reglerna i 3 § PTSFS 2015:2 och 3–4 §§ PTSFS 2014:1 av följande skäl.

Netnod har sedan oktober 2021 programvara för RPKI tillgänglig, men har skjutit upp införandet av RPKI i transittjänst. Netnod upplyste PTS först i januari 2022 om att bolagets hårdvara inte är dimensionerad för de nuvarande informationsmängderna i transittjänst och att bolaget därför inte kan vidta åtgärden med RPKI i transittjänst med prioritet.

Netnod har också uppgett att det övervakningssystem som Netnod idag använder endast ger en rapport per vecka om BGP-incidenter i det egna nätet, och det tar endast in begränsad routinginformation från externa routingdatabaser, samt att ett nytt övervakningssystem finns tillgängligt för bolaget sedan februari 2022, men att ett utbyte till det mer tillförlitliga övervakningssystemet inte prioriteras högt.

Genom dessa förhållanden misstänker PTS att Netnod inte uppfyller kraven på ett kontinuerligt, långsiktigt och systematiskt säkerhetsarbete enligt 3 § PTSFS 2015:2 och 3 § PTSFS 2014:1.

Enligt PTS bedömning kan Netnod genom dessa förhållanden inte heller ha vidtagit nödvändiga skyddsåtgärder 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 och den teknik som finns tillgänglig.

Sammanfattande bedömning

PTS misstänker således sammanfattningsvis att Netnod inte uppfyller kraven enligt reglerna om driftssäkerhet och skydd av uppgifter som åligger tillhandahållare av elektroniska när och tjänster att följa. För att uppfylla kraven behöver Netnod införa de två säkerhets- och skyddsåtgärder som PTS anger i underrättelsen. PTS har i bedömningen även beaktat Netnods förutsättningar och kostnaderna i förhållande till den tillgängliga tekniken. Från och med oktober 2021 har Netnod angett att bolaget har programvara tillgänglig för att införa

RPKI i transittjänster. När det gäller det mer tillförlitliga övervakningssystemet som kan upptäcka BGP-kapningar i realtid har Netnod angett att det kommer att införas på sikt och finns tillgängligt för bolaget i februari 2022.

Netnod får tillfälle att yttra sig

PTS finner sammanfattningsvis att myndigheten enligt 7 kap. 4 § LEK ska underrätta Netnod om att myndigheten misstänker att Netnod 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 9–10 §§ i PTSFS 2015:2, ändrade genom PTSFS 2020:1 och slutligen även 3 § och 4 § tredje stycket i PTS föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter (PTSFS 2014:1).

Netnod 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 Netnod ska vidta nödvändiga åtgärder för rättelse. Eventuellt föreläggande kan komma att förenas med vite. Om Netnod 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 Erika Hersaeus. I ärendets slutliga handläggning har även Therese Braathen och verksjuristen Emma Edsjö.