RIIGI INFOSÜSTEEMI AMET

OHUHINNANG[1] *Juuni 2020*

Marsruutimisprotokolli BGP riskid ja nende maandamise võimalused

Internetis andmete juhtimiseks kasutatav marsruutimisprotokoll BGP (Border Gateway Protocol) on loomult ebaturvaline ja selle puuduste tõttu on toimunud kümneid tuhandeid intsidente, paljud neist ülemaailmse mõjuga. Üks värskemaid näiteid on 9. juunil IBMi pilveteenust tabanud BGP kaaperdamine, mis põhjustas tunde kestnud teenusekatkestuse. On lahendusi, mille kasutamine muudab BGP tunduvalt turvalisemaks, kuid paraku on Eesti nende rakendamisel Euroopa Liidu viimaste seas.

BGP – mis see on ja kuidas toimib?

BGP on marsruutimisprotokoll, mida kasutatakse erinevate autonoomsete süsteemide vahel marsruutimisinfo vahetamiseks. Autonoomsed süsteemid omakorda sisaldavad infot ühe või rohkema IP-prefixi ehk IP-võrgu kohta. BGP-st sõltub, kas meie andmed jõuavad turvaliselt ühest autonoomsest süsteemist teise.

BGP on justkui interneti teekaart, aga selle rolli ja vajaduse selgitamiseks sobib ka võrdlus postiteenusega. Pärast seda, kui kirja saatja on lasknud ümbriku postkasti, valib postiettevõte sellele märgitud aadressi ja postifirma kasutuses oleva info põhjal, millise tee kaudu saab kirja adressaadini toimetada.

Kui keegi soovib edastada andmeid ühes autonoomses süsteemis asuvast IP-võrgu seadmest teises autonoomses süsteemis asuvasse IP-võrgu seadmesse, siis, analoogselt postiettevõttega, on vaja esmalt infot selle kohta, millised on võimalikud teed, mida mööda saaks selle info kohale toimetada. BGP ongi loodud, et vahetada sellist info erinevate autonoomsete süsteemide vahel. Vastavalt saadud infole koostatakse analoogselt postitettevõttega nn teekaart ja valitakse andmete kohale toimetamiseks sobilik tee.

Kuna internet on võrkude võrk, mis koosneb kümnetest tuhandetest väiksematest võrkudest, liiguvad andmed enamasti erinevate autonoomsete süsteemide vahel. Igas sellises süsteemis peab olema vähemalt üks marsruuter, mis suhtleb BGP protokolli alusel teiste autonoomsete

[1] KüTS'i paragrahv 12:
(2) Riigi Infosüsteemi Amet teostab küberturvalisuse tagamiseks Eesti internetiprotokolli aadressiruumis olevate ning Eesti maatunnusega seotud domeenide vaatlust, analüüsib süsteemide turvalisust ohustavaid riske ning nende mõju riigile, ühiskonnale ja süsteemide turvalisusele.
(3) Riigi Infosüsteemi Amet edastab isikutele küberintsidendi ennetamiseks ja lahendamiseks ohuteateid, mis võimaldavad rakendada küberintsidendi mõju vältivaid või vähendavaid abinõusid.

süsteemide marsruuteritega. Autonoomsed süsteemid pole alati üks-ühele ühenduses, lisaks sellele on olemas ka interneti sõlmpunktid, kus üks autonoomne süsteem saab vahetada infot korraga mitme teise autonoomse süsteemiga.

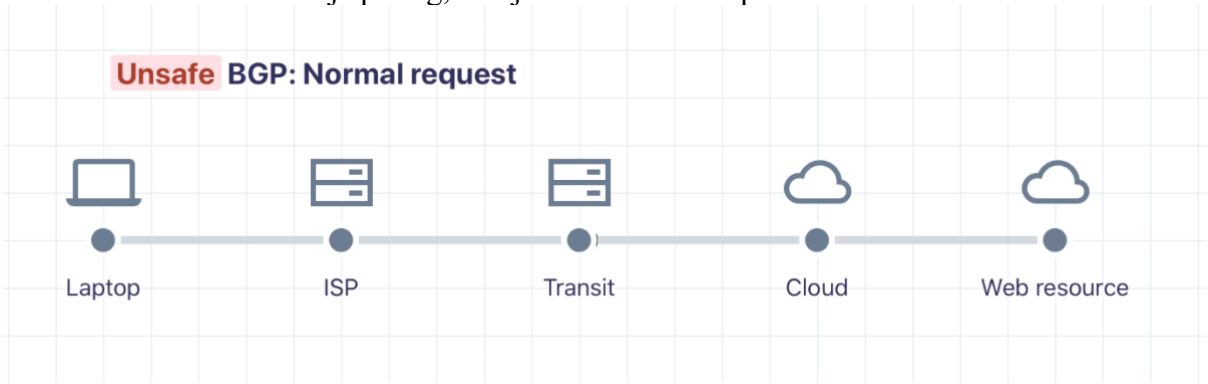
Internetti ühendatud autonoomsete süsteemide sõlmpunktid paiknevad üle maailma, Tänu sellistele sõlmpunktidele on tagatud võimalike teede paljusus ja ühe tee katkemisel saab alati valida järgmise, mille kaudu andmed kohale toimetada. Seni, kuni kõik osalised jagavad tõest infot, jõuavad andmed soovitud sihtpunkti. Probleemid algavad hetkest, mil üks marsruuter saadab teisele valeinfot.

BGP turvariskid

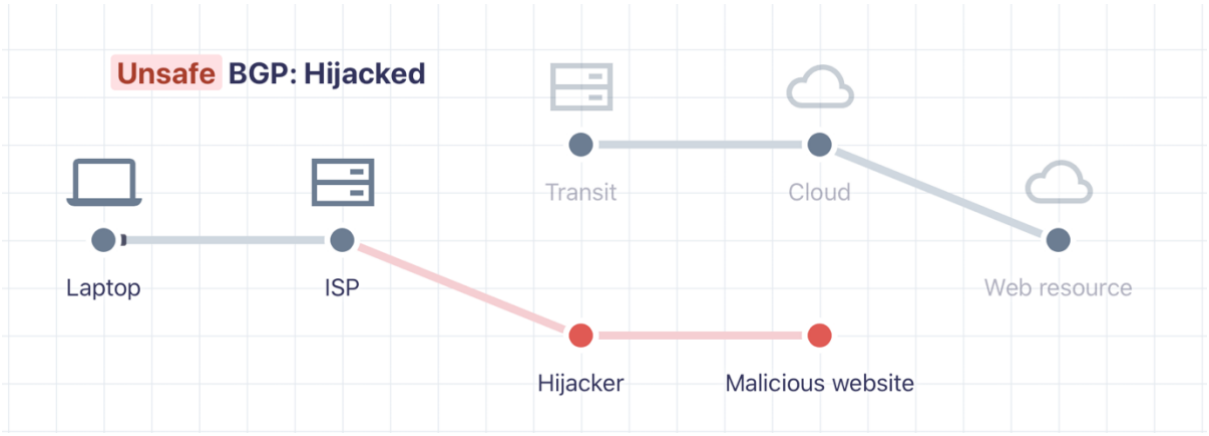
BGP loodi rohkem kui 25 aastat tagasi ja selle autorite fookuses oli lihtsus, töökindlus ja kasutusmugavus. Turvalisus toonaste prioriteetide hulka ei kuulnud, mistõttu oli BGP algselt seadistusvigade ja rünnakute ees kaitsetu.

Üks levinuim probleem on BGP kaaperdamine (BGP *hijack*). Selle käigus annab üks sõlmpunkt marsruutimistabeli kaudu temaga otseühenduses olevatele sõlmedele valeinfot andmete edastamise teede kohta või väidab, et talle kuuluvad IP-aadressid, mis tegelikult kuuluvad teistele. Ilma turvaprotokollideta võib selline väärinfo levida loetud minutitega üle maailma, liikudes ühelt autonoomselt süsteemilt teisele. Kui see juhtub, üritavad eksiteele aetud seadmed suunata andmeid mööda valesid või olematuid radu. Tulemuseks võivad olla teenusekatkestused, pettused või andmevargused.

Joonis 1: Selline näeb välja päring, mis jõuab edukalt sihtpunkti.



Joonis 2: Nii liigub päring, mis BGP haavatavuse tõttu poolel teel kaaperdati: kasutaja jõuab soovitud lehe asemel kaaperdaja soovitud lehele.



BGP põhineb usaldusel: ruuterid avaldavad info võimalike andmeteede kohta ja teised ruuterid usaldavad enamasti pimesi saadud informatsiooni ning levitavad seda kontrollimata edasi. Üldjuhul ongi saadud marsruutimisinfo õige, aga tuleb ette ka suure mõju ja kuluga vigu. Enamasti on süüdi seadistusvead ja inimlikud eksimused, kuid ajalugu tunneb ka märksa tõsisemaid pahatahtlikke kaaperdamisi, mille eesmärk on krüptoraha- või andmevargus.

Olulisemad intsidendid

Suur osa Euroopa mobiilsest andmesidest suunati läbi Hiina telekomifirma. 6. juunil 2019 lekkis andmekeskuseid haldava Šveitsi firma Safe Host sisemine marsruutimistabel. Selmet lekkinud marsruutimisinfot ignoreerida, kuulutas Hiina internetiteenuse pakkuja China Telecom selle põhjal Safe Hosti andmeteed turvamata BGP-sid kasutades enda omaks. Selle tagajärjel suunati suur osa Euroopa mobiilsest andmesidest läbi China Telecomi taristu, mis tähendas, et paljude Euroopa mobiilioperaatorite klientide andmed liikusid läbi Hiina. Selle ajal kogesid kliendid tavapärasest aeglasemat liiklust, kuid suurem probleem on aga võimalik andmekorje, mida Hiina telekomiettevõte selle intsidendi käigus teha võis. Kui enamasti vältavad marsruutimisintsidendid vaid loetud minutid, siis antud intsident kestis üle kahe tunni.

Osa USA-sisesest internetiliiklusest käis läbi Hiina. 2018. aasta juulis selgus, et China Telecom on 2,5 aastat vale marsruutimisinfo alusel juhtinud osa USA-sisesest internetiliiklusest läbi Hiina. Näiteks, Los Angelest saadetud andmed liikusid esmalt Hangzhousse ja alles pärast seda sihtpunkti Washingtonis.

Kurjategijad kaaperdasid liikluse krüptoraha-lehele: 2018. aasta aprillis kasutasid kurjategijad ära BGP nõrkust, et suunata need, kes soovisid minna krüptoraha-lehele myetherwallet.com, ümber sellega sarnanevale libalehele. Kui kasutajad sisestasid oma kasutajanime ja parooli, kandsid kurjategijad ohvrite kontol olnud krüptoraha enda kontrolli all olevale kontole.

Google'sse ja Facebooki läbi Vene Föderatsiooni: 2017. aasta detsembris suunati BGP-kaaperdamise tagajärjel üle 200 tuntud veebilehe (teiste seas Google, Facebook, Microsoft ja Apple) liiklus läbi Vene Föderatsiooni autonoomse süsteemi, mis enne seda intsidenti oli

aastaid kasutuseta seisnud. See juhtum kestis umbes tund aega ja tõstatas kahtluse, et intsidendi põhjustanud firma salvestas andmevoo ümbersuunamisega saadud andmed.

Türgist sai interneti sõlmpunkt: 2004. aasta jõululaupäeva hommikul saatis Türgi internetiteenuse pakkuja TTNet BGP kaudu välja marsruutimisinfo, mis sisuliselt väitis, et TTNet on parim tee peaaegu kõige jaoks, mis internetis liigub. Kuna teised teenusepakkujad seda väidet ei kontrollinud, vaid edastasid seda järgmistele teenusepakkujatele, suunatigi mitme tunni jooksul enamus globaalsest internetiliiklusest läbi Türgi. TTNeti taristu ei olnud hüppeliselt kasvanud koormuseks valmis, mistõttu ei pääsenud suur osa internetikasutajatest mitme tunni jooksul soovitud lehekülgedele.

Pakistani telekom võttis maha YouTube'i: 2008. aasta veebruaris andis Pakistani valitsus riiklikule telekomifirmale käsu blokeerida Pakistani territooriumil ligipääs YouTube'le. Telekomifirma muutis marsruutimisinfot nii, et kõik, kes soovisid külastada populaarset videoplatvormi, suunati lehele, mis teatas, et YouTube on blokeeritud. Paraku saatsid Pakistani telekomi võrguseadmed uuendatud marsruutimisinfo BGP kaudu teistele internetiteenuse-pakkujatele, kes ei kontrollinud seda, vaid edastasid omakorda järgmistele telekomidele. Tulemus: YouTube polnud kahe tunni jooksul ülemaailmselt kättesaadav.

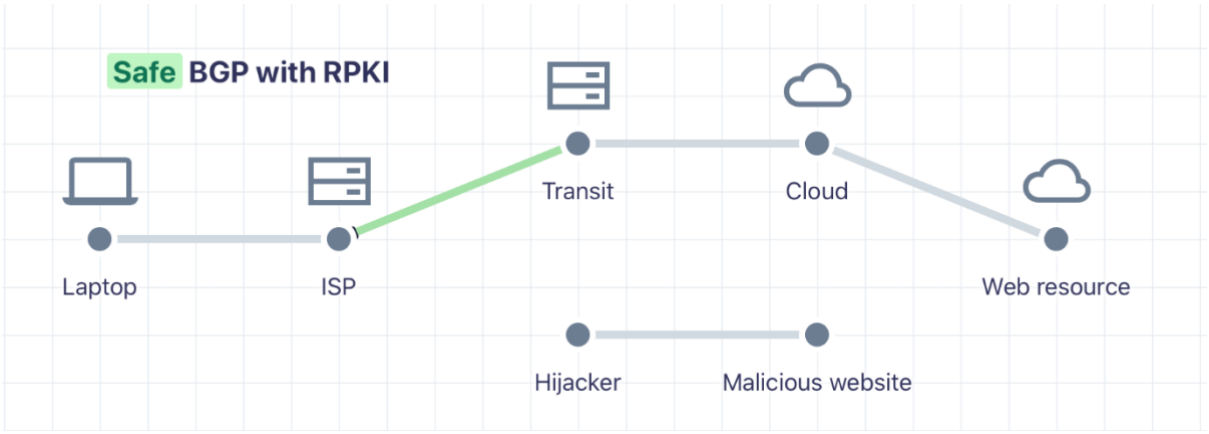
RIA soovitused: kuidas muuta BGP turvalisemaks

Nagu need juhtumid kinnitavad, pole BGP vaikimisi turvaline. Võrguliikluse monitoorimine, sellest anomaaliate otsimine, partneritega oma marsruutimispraktikate jagamine ja prefiksite filtreerimine aitavad turvalisuse tõstmisele kaasa, kuid määrava tähtsusega on siin BGP marsruutide valideerimine.

Üks tunnustatumaid ja levinumaid marsruutimisinfo valideerimislahendusi on RPKI (*Resource Public Key Infrastructure*), mida soovitame rakendada kõigil Eesti ettevõtetel, kes omavad autonoomset süsteemi.

RPKI abil saab autonoomse süsteemi omanik ROA kirje (Route Originate Autorization) abil väljendada seost enda autonoomse süsteemi ja talle kuuluva prefixi vahel ning seda digiallkirjaga kinnitada. See võimaldab omakorda marsruuteritel, mis on seadistatud marsruutimise infot RPKI abil kontrollima, valed ruutingud välja filtreerida.

Joonis 3: BGP kaaperdamiskatse pärast RPKI rakendamist.



Mida teha, et allkirjastada ROA kirjed?

Kuna meie piirkonnas on regionaalne internetiregister (RIR) RIPE, kasutame nende usaldusahelat. Allkirjastamine toimub läbi RIPE LIRi portaali ja see võtab mõned minutid.

- Suundu aadressile lirportal.ripe.net
- Logi oma RIPE NCC kontoga sisse.
- Lehe päises vali Manage IP-S and ASN > LIR portal > Resources > RPKI Dashboard.
- Järgi ekraanile ilmuvaid juhised.
- Vastates küsimusele, kas, kas soovid kasutada enda või RIPE sertifitseerimislahendust (CA), soovitame valida viimase. Kuna sertifikaate hoiab niikuinii RIPE, ei anna enda sertifikaadi kasutamine märkimisväärselt juurde ei võimaluste ega riskide kontekstis.
- Avanevas aknas on tulp autonoomsete süsteemide (AS) numbritest ja prefiksitest. Vali kõik prefiksid ja vajuta nupul „Create ROA for selected BGP Announcements".
- Kinnita oma valikud.
- Sellele järgneb RIPE-poolne kontroll ja test. Kui selle käigus probleeme ei ilme, on kahe päeva pärast digiallkirjastatud ROA kirje tehtud ja pärast seda saavad teised autonoomsed süsteemid teie autonoomse süsteemi suunas viitavaid ruutinguid valideerida.

Mida teha, et ka teie marsruuterid valideeriks ruutinguid?

Ruutingute valideerimiseks soovitame kasutada RIPE valideerimislahendust rpki-validator.ripe.net.
Paigaldamise juhendi leiab: https://labs.ripe.net/Members/tashi_phuntsho_3/how-to-install-an-rpki-validator.
Marsruuterite seadistuse näidised on leitavad: https://www.ripe.net/manage-ips-and-asns/resource-management/certification/router-configuration

Täpsustavate küsimuste korral võid pöörduda ka CERT-EE poole: cert@cert.ee

RPKI rakendamisega kaasnevad riskid

Olulisi riske RPKI rakendamisega ei kaasne. Seadistades süsteemi selliselt, et valideerimislahenduse katkemisel aktsepteeritakse sissetulevad ruutingud, ei kaasne

käideldavuse riski. Valideerimislahenduse katkemisel võetakse vastu kõik ruutingud ehk säilib RPKI rakendamise eelne olukord.

Kokkuvõtteks

RPKI pole uus tehnoloogia, kuid paraku ei kasutata seda BGP turvamisel nii laialdaselt kui võiks. CERT-EE-le laekunud info kohaselt on ka Eesti sideteenuste pakkujate IP-aadresse kuulutatud välja valedest võrkudest, kuid sellele vaatamata oleme siiani RPKI rakendamisel Euroopas viimaste seas ja see teeb meid BGP kaaperdamiste suhtes väga haavatavaks. Samamoodi jätkates võib Eestit aina tõenäolisemalt tabada suure mõjuga BGP nõrkusest tulenev intsident.