Kaitse oma WiFi võrku

9 aastat tagasi - 31.07.2017 Autor: Martin Grüner

Tänapäeval on raske leida kodu või kontorit, kus poleks WiFi ruuterit. Traadita internet on saanud sama tavapäraseks, kui televiisor.

Koduse võrgu üles seadmine on muutunud nii lihtsaks, et selleks pole vaja isegi tehniku abi. Üldjuhul piisab WiFi võrgu loomiseks ruuteri võrgukaabli ja vooluvõrguga ühendamisest. 4G ruuterit pole vaja isegi võrgukaabliga ühendada, piisab ainult pistiku seina lükkamisest. Kuna ruuteri ühendamine on niivõrd lihtne, jäetakse tihti tähelepanuta koduse võrguga kaasnevad turvariskid. Vaatame järgnevalt kuidas oma kodus või kontoris juhtmevaba võrk võimalikult turvaliseks muuta.

Miks turvata oma WiFi võrku?

Koduse WiFi võrgu kaitseta jätmine võib esmapilgul tunduda ebaoluline ja isegi mõistlik lahendus. Sul ega su külalistel pole vaja telefonide ja arvutite võrku ühendamiseks parooli sisse trükkida, mis on ju mugav.

Mugav on see tõesti, kuid mitte ainult heatahtlikele külalistele. Turvamata võrku võivad ühendada ka naabrid ja möödujad. Isegi, kui nende tegevus pole otseselt pahatahtlik koormavad nad su ruuterit, mistõttu on su internet tavapärasest aeglasem. Internetikiiruse langus on tegelikult kõige väiksem mure, mille soovimatud seadmed su WiFi võrguga kaasa võivad tulla. Viirusega nakatunud arvuti võib nakatada teisi sinna ühendatud arvuteid ilma, et kasutaja sellest midagi teaks (kuidas levivad viirused olen pikemalt kirjutanud **siin**).

Turvamata kodune WiFi on täpselt sama ohtlik, kui turvamata avalikuks kasutamiseks mõeldud võrk. Avalike WiFi võrkude kasutamine on piisavalt turvatundlik teema, et olen sellest kirjutanud artikli “**Turvalisus avalikus WiFi võrgus**”.

Kui avalikus WiFi võrgus on oht langeda õngitsemise või viiruse rünnaku ohvriks, siis oma võrgu kaitseta jätmisel on veel üks suur risk. Nimelt oled seaduse meelest vastutav oma võrgus toimuva eest. Korrakaitsjad tulevad kõigepealt koputama just sellele uksele, kust illegaalseid materjale jagatakse. Edasi pead juba ise tõestama, et süüdistusega seotud polnud. Igal juhul tähendab see palju

potensiaalseid probleeme, muuhulgas su kodus leiduvate arvutite, telefonide ja teiste andmekandjate konfiskeerimist ning potensiaalselt pikka kohtuteed. Lihtsam on seda kõike vältida oma võrgu turvamisega.

Viimane lõik võib tunduda paranoiana – keegi ei sõida ju mööda linna ringi turvamata WiFi võrke otsides, et sealt näiteks lastepornot levitada. Paraku on risk täiesti reaalne, kuna kurjategijad just nimelt seda teevad. Üks kindlamaid viise internetis oma identiteeti varjata on leida suvaline avatud võrk, soovitatavalt oma kodust võimalikult kaugel, kus siis kiirelt ühe korraga valgustkartvad teod toime panna. Sellest ei jää praktiliselt mingit jälge maha (ehk ainult märge uuest masinast ruuteri logidesse), ning kahtlus langeb täielikult internetiühenduse omanikule.

Muuda kõik tehaseseaded

Tehaseseadeteks on ruuteri puhul **võrgu nimi**, **võrgu parool** ning **ruuteri administreerimisliidese kasutajanimi ja parool**. Võrgu turvalisuse tagamiseks ei tohiks mitte ükski neist olla vaikimisi pärit tehaseseadest.

Kõigi tehaseseadete muutmine on oluline, kuna internetis on leitavad kõigi ruuterite haldusliideste vaikimisi paroolid. Vaikimisi seadetes ruuterisse sisse murdmine on ainult ühe guugeldamise kaugusel – sellega saab hakkama isegi laps (ei tasu kunagi alahinnata tänapäeva noorte tehnikateadlikkust). Tõsi, õigesti seadistatud ruuteri haldusliidesele pääseb ligi ainult olles juba võrku ühendatud. See on väike lohutus, kuna vaikimisi ei pruugi ruuter olla turvalisuse vaatepunktist õigesti seadistatud. Samuti võib olla võimalik, et su WiFi võrgu parooli saab ära arvata vaikimisi nime põhjal.

See probleem on näiteks Thomson’i ruuteritega, mida jagas oma klientidele pikka aega Telia. Oluline on märkida, et see ei puuduta kõiki nende ruutere, ainult valitud Thomson’i omi. Kuidas tunda ära lihtsalt haavatavat Thomson’i ruuterit? Nad on äratuntavad võrgu nime “ThomsonXXXXX” järgu, kus X-ide asemel on numbreid ja suuri tähti. Sisestades sõnale Thomson järgneva numbrite ja tähtede kombinatsiooni siia leiad suure tõenäosusega võrgu parooli.

PS! Eelnev ei tähenda, et Thomson’i ruuterid, isegi antud mudelid, oleksid oma ülejäänutest olemuselt ebaturvalisemad. Ohtlikud on nad ainult juhul, kui jätad vahetamata võrgu nime ja parooli. Kui vahetad kasvõi ainult parooli ei ole seda võimalik võrgu nime põhjal genereerida. Vaikimisi paroole on antud juhul võimalik genereerida ainult seetõttu, et nimi ja parool on loodud seotud valemi alusel.

Thomson pole ainuke ruuterite tootja, kelle vaikimisi paroole on võimalik lihtsalt ära arvata. Ei tasu kunagi eeldada, et sinu ruuter on vaikimisi turvaline – parooli muutmine võtab ainult hetke.

Kuidad vahetada paroole ja võrgu nime?

WiFi võrgu nime ja parooli vahetamiseks tuleb sisse logida ruuteri administreerimisliidesesse. Selleks pead kõigepealt arvuti või nutitelefoniga ühendama ruuteri võrku vaikimisi parooliga. Vaikimisi võrgu nime ning parooli leiad enamasti ruuteri pealt või kaasatulevast manuaalist.

Kui oled ühendunud ruuteri võrku pead avama haldusliidese veebilehitsejas. Selleks pead veebilehitseja aadressiribale trükkima vastava IP aadressi. Õige IP aadressi leiad enamasti ruuteri manuaalist. Kui ruuteri manuaalis seda mainitud pole (see kipub tihti juhtuma internetiteenuse pakkuja poolt klientidele renditavate ruuteritega), leiad selle internetist. Otsi lihtsalt “Ruuteri nimi (mille leiad pakendilt) admin panel IP”.

Kui oled aadressiribale trükkinud õige IP aadressi avaneb haldusliidesse logimise vaade. Sisse saad logida ruuteri administraatori kasutajanime ja parooliga, mille leiad samuti kas ruuterilt või kaasatulevast manuaalist.

Paraku on edasi tulev vaade igal ruuteril erinev. Universaalselt klikk-kliki põhist juhist pole WiFi parooli ning nime muutmiseks võimalik teha. Soovitan lihtsalt kõik menüü elemendid läbi klikkida, kuni leiad võrgu nime (SSID) ning parooli muutmise koha. Ruuteri kasutajanime ja prooli saad muuta reeglina kas “kasutaja” sektsioonist.

Arvestama peab, et ruuteri haldusliidesed on reeglina inglise keeles. Menüü linkide läbi klikkimisel tuleb kindlasti siiski vaadata, mida see teeb, mitte pimesi kõiki nuppe vajutama. See eeldab, et oled inglise keelega kodus. Kui see nii pole tasub pöörduda abi saamiseks ka inglise keelt rääkiva inimese või IT tehnika hooldusteenust pakkuva ettevõtte pole.

Telia pakub täpseid juhendeid oma seadmete haldamiseks oma kodulehel “Online abi” sektsioonis.

Starmanil pakutavate ruuterite seadistamise juhendi leiab samuti nende kodulehelt.

Kui oled oma seatud WiFi parooli või administeeerimisliidese logimisandmed unustanud on igal ruuteril nupp tehaseseadete taastamiseks.

Pane võrgule parool ja õige krüpteering

Parooli seadmisel pead valima ka algoritmi, millega liiklus krüpteeritakse. WiFi protokolli puhul on tegemist standardiga, mis paneb paika kasutatavad krüpteeringu algoritmid. Kui WiFi krüpteeringud poleks standardsed ei oleks sul võimalik ühendada igasse WiFi võrku, kuna su võrgukaart ei pruugiks osata sellega lihtsalt suhelda. Standardse krüpteeringu negatiivne pool on, et need kipuvad kiirelt ajale jalgu jääma.

WiFi krütpeeringu standardid on “**WEP**”, “**WPA**” ja “**WPA2**”. Alati tuleks kasutada kõige tugevamat võimaliku krüpteeringut. Eelmainitutest on tugevaim WPA2, mille peaksid alati valima. Kõik uuemad ruuterid toetavad WPA2 krüpteeringut. Kui sul peaks olema väga vana ruuter, mis seda ei toeta, tuleks see ideaalis välja vahetada. Kui välja vahetamine pole võimalik, tuleks kasutada WPA krüpteeringut.

WEP algoritmiga krüpteeritud võrk on praktiliselt avatud. WEP (Wired Equivalent Privacy) standard pärineb eelmisest aastatuhandest (1999), kuid murti lahti juba paari järgneva aasta jooksul. WEP algoritmiga kaitstud võrgu parooli saab lahti murda mõne minutiga ilma, et selleks peaks mingeid erilisi teadmisi olema.

Soovikorral võid seda ise proovida kasutades AirCrack nimelist tarkvara. AirCrack on saadaval kõigile nii Windows’ile, Linux’ile, kui Mac’ile. Loomlikult tohib seda teha ainult enda võrguga veendumaks, et WEP on tõesti ebaturvaline.

WPA ning WPA2 tähendavad vastavalt “Wi-Fi Protected Access” ja “Wi-Fi Protected Access 2”. Kuigi nimed on sarnased ei tähenda, et algoritmid seda oleks. WPA ning WPA2 on tehniliselt täiesti erinevad algoritmid. WPA2 on turvalisem ja kiirem, kui seda on WPA.

Võimalik, et algoritmi valikus on rohkem valikuid, kui 3. Näiteks võivad seal olla *WPA2 TKIP*, *WPA2 AES* ja *WPA2 TKIP/AES* (või *WPA2 MIXED*). Sellise valiku korral tuleks valida **WPA2 AES**, mis on turvaliseim ja kiireim variant. Kõik tänapäevased seadmed ka toetavad seda. Selle võimalik kitsaskoht on vanemad seadmed, mis ei pruugi osata antud krüpteeringuga midagi peale hakata. Kui mõni su vanem seade ei näe WPA2 AES seades võrku või ei oska sinna ühendada võib kasutada WPA2 MIXED varianti. Viimane on küll väga ebatõenäoline, see võib juhtuda ainult enne 2004. aastat välja lastud võrguseadmega. Kui valikus on lihtsalt WPA2 on see suure tõenäosusega WPA2 AES krüpteering.

Uuenda vajadusel ruuteri tarkvara

Ruuter võib tunduda lihtsalt kastina, mis tekitab WiFi’t, kuid tegelikult on seal sees palju tarkvara. Nagu igas teises programmis, võib ka selles tarkvaras esineda turvaauke. Kui tootja peaks selle avatama väljastab ta enamasti turvapaiga, mille pead käsitsi installeerima. Turvapaiku saad enamasti installeerida haldusliidese kaudu, kuhu logimisest kirjutasin eelmises **peatükis**. Telia võimaldab enda väljastatud ruuterite tarkvara uuendada ka iseteeninduse kaudu. **Turvalisuse tagamiseks peab ruuteri tarkvara alati uusimale versioonile uuendama.** Tihti on just ruuteri uuendamata tarkvara nõrgaks kohaks arvutivõrgus, kust häkker (või ussviirus) end sisse vingerdada saab.

Ruuteri tarkvara uuendamiseks on ka teine põhjus. See võib lisada uusi põnevaid võimalusi, mida vanemas tarkvara versioonis pole. Tarkvarauuendus võib su interneti isegi kiiremaks muuta.

Kui su ruuteril pole haldusliideses uuendusfunktsiooni peaksid aeg-ajalt tootja kodulehelt kontrollima, ega ruuteri tarkvarast uut versiooni tulnud pole. Kui uus versioon ruuteri tarkvarast (*router firmware* inglise keeles) peaks saadaval olema, tuleks see manuaalselt installeerida. Manuaalne uuendus võib olla parajalt keeruline, kuid juhendid on enamasti kas tootja kodulehel või internetis. Suure tõenäosusega leiad YouTubest samm-sammult õpetusvideo. Kui sa siiski end seda tehes kindlalt ei tunne, võib pöörduda spetsialisti poole. Suure tõenöosusega saavad kõik arvutihooldust pakkuvad ettevõtted hakkama ka ruuteri tarkvara uuendamisega. Kindlasti ei tohiks tarkvarauuendust tegemata jätta lihtsalt sellepärast, et see keeruline tundub.

Kortermajas eelista 5 Ghz võrku

5 Ghz WiFi võrgu eelistamiseks on mitu põhjust. Esiteks on see märgatavalt kiirem, kui tavapärane 2.4 Ghz WiFi. Samuti ei häiri kattuvad võrgud 5 Ghz WiFi’t nii palju, mis muudab selle märgatavalt kiiremaks. 5 Ghz WiFi suurimaks miinuseks on väiksem raadius. Turvalisuse vaatepunktist on see vastupidi positiivne – kui su WiFi ei levi kaugemale su korterist ei saa keegi väljaspoolt sinna ühendada. Kui WiFi’t ei levi, ei saa seda ka rünnata!

Soovitatavalt paiguta ruuter võimalikult kodu keskele, et kogu su korter oleks WiFi ühendusega kaetud, kuid see ei lekiks minimaalselt välja.

Ruuteri haldusliidesest saab enamasti valida, kas see edastab 5 Ghz või 2.4 Ghz WiFi signaali. Paraku ei toeta enamik Eesti internetiteenuse pakkujate poolt

väljastatud ruutere 5 Ghz võrku. Kui ruuteri seadetest seda valida ei saa, tähendab see suure tõenäosusega, et su ruuteril puudub 5 Ghz WiFi võimekus.

5 Ghz võrgu soovitus ei ole universaalne. Suure korteri puhul ei pruugi 5 Ghz võrk ulatuda igasse tuppa, mis juhul tuleks kasutada kas 2.4 Ghz WiFi't või WiFi võrgu laiendajat. Samuti ei läbi 5 Ghz võrk väga hästi seinu, mistõttu võib näiteks vanalinnas see probleemseks muutuda.

Kodust pikemaks ajaks lahkudes võta ruuter vooluvõrgust välja

Kui lähed kodust pikemaks ajaks ära, tasub ruuter seinast välja tõmmata. Vähemalt võiks kinni keerata WiFi. Nii ei saa keegi su äraoleku ajal su võrku kasutada ega seal midagi potensiaalselt kurja korda saata.

Võrgu peitmine

Enamasti on ruuteritel võimalus võrku peita. Peidetud võrgu korral ei edasta ruuter võrgu nime ning see ei ilmu arvutite/telefonide WiFi võrkude nimekirjas. See võib tunduda hea turvameetmena, kuid tegelikult ei takista see ründajat üldse. Vastava tarkvaraga näeb potensiaalselt pahatahtlik kasutaja kõiki WiFi võrke oma ümbruses, ka peidetuid. Võrgu peitmine muudab selle kasutamise sulle ja su külalistele ebamugavamaks pakkumata reaalset kaitset. **Võrgu peitmine pole alternatiiv ruuteri seinast tõmbamisele**.

Keela võrguväline ligipääs ruuteri haldusliidesele

Ruuter võib vaikimis seadetes lubada ligipääsu oma kontrollpaneelile ka internetist. Seda ei tohiks kunagi lubada – kontrollpaneelile peaks ligi saama ainult juba võrku ühendatud olles. Samuti on paljudel ruuteritel "välise abi" funktsioon, mis võimaldab osasid seadeid väga lihtsalt üle interneti muuta. Ka see on potensiaalselt haavatav ning tuleks kinni keerata. Kui kasutad oma internetiteenuse pakkuja väljastatud ruuterit saavad klienditoe töötajad sellele suure tõenäosusega ligi ka siis, kui oled välise abi funktsiooni välja lülitanud. Pole vaja karta, et see näiteks Telia veebipõhised tööriistad kasutuks muudaks.

Välise ligipääsu seadete nimed ruuteri kontrollpaneelis on "*remote acces*" ja "*remote help*". Need pole päris samad asjad, kuid mõlemad tuleks turvalisuse huvides deaktiveerida.

Seadmepõhised ligipääsupiirangud

Igal võrguseadmel on unikaalne kood nimega MAC aadress. Kui IP aadress muutub sõltuvalt võrgust, kuhu seade ühendatud on, siis MAC aadress jääb alati samaks. Paljusid ruutereid saab seadistada lubama ühendust ainul eelseadistatud MAC aadressidelt. Nii saavad su WiFi võrku ühendada ainult sinu arvuti, telefon, mängukonsool jms.

Seadmepõhise ligipääsu piirang on üsnagi efektiivne, kuid kindlasti mitte lollikindel turvameede. Kui häkker peaks teada saama su arvuti MAC aadressi saab ta seda simuleerida. MAC aadressi tuvastamine pole sugugi keeriline, selleks piisab samasse avaliku võrku ühendamisest. Samuti on MAC aadressi põhine piirang tüütu, kui su külalised peaks tahtma võrku kasutada.

Koduses võrgus on seadmepõhised ligipääsupiirangud ilmselt juuksekarva lõhki ajamine. Kontoris seevastu võib olla hea idee lubada WiFi’t kasutada ainult ettevõttele kuuluvatel arvutitel.

Kokkuvõte

Wifi turvamine pole keeruline. Su võrk on suure tõenäosusega piisavalt turvaline, kui järgnevad tingimused on täidetud:

1. WiFi võrgu vaikimisi nimi, parool ning administreerimisliidese vaikimisi kasutajanimi ja parool on vahetatud
2. WiFi on kaitstud parooli ja WEP2 AES krüpteeringuga
3. Ruuteri tarkvara on uuendatud uusimale versioonile
4. WiFi ei levi su kodust või kontorist (palju) kaugemale
5. Ruuteri “*remote access*” ja/või “*remote help*” featuurid on välja lülitatud

Artikkel on pärit Netsec.ee blogist

- Lahendused

- Andmeside
- Turvalisus
- Võrguseadmed

Pilt


Free
Wi Fi