Näin lukitset langattoman lähiverkkosi

*Kotiisi voidaan murtautua muualtakin kuin ovesta tai ikkunasta. Tietoturvayhtiö Check Pointin maajohtaja **Jukka Saarenmaa** kertoo, miten suojaat langattoman lähiverkkosi kutsumattomilta vierailta.*

Helsinki 27.1.2014 – Langaton lähiverkko eli WLAN, toiselta nimeltään Wi-Fi, on kätevä, koska sen kautta voi liittää kaikki verkkoyhteyttä käyttävät laitteet sekä nettiin että viestimään keskenään. Sitä käyttävät niin puhelimet, tietokoneet ja smart tv:t kuin tulostimet ja uusimmat kamerat, ehkä piakkoin jopa älykkäät jääkaapit.

Lähiverkon jättäminen suojaamatta on sama kuin antaisi murtovarkaalle kotiavaimen. Kutsumaton vieras voi napata tärkeät tietosi tai käyttää laitteitasi rikollisiin tarkoitusperiinsä. Kaikeksi onneksi verkko on suhteellisen helppoa lukita.

Reitittimen eli WLAN-tukiaseman asetuksia pääsee rukkaamaan verkon kautta ylläpitokäyttöliittymässä, jonka osoite selviää reitittimen käyttöohjeesta. Käyttöliittymä on yleensä suojattu salasanalla, jonka vaihtaminen on ensimmäinen, mitä kannattaa tehdä.

1. Vaihda salasana

Oletussalasanan käyttö on huono idea laitteesta riippumatta. Vaihda langattoman lähiverkon reitittimen salasana laitteen ylläpitokäyttöliittymässä. Jos reitittimessäsi on omat asetukset verkon vieraskäyttäjille, vaihda myös tämä salasana. Valitse vahva salasana, jossa on sekä isoja että pieniä kirjaimia, numeroita ja symboleja. Vältä kaikkea helposti arvattavaa, kuten nimiä, syntymäaikoja ja maailman kenties yleisintä salasanaa 1234567.

2. Vaihda verkon nimi

Myös verkon ulospäin näkyvä nimi eli SSID kannattaa vaihtaa, koska alkuperäinen nimi voi kertoa ulkopuoliselle tarkkailijalle, minkätyyppinen verkkosi on. Kyberrosvo voi myös päätellä, että koska olet jättänyt verkkosi nimen vaihtamatta, et varmaan ole vaihtanut sen salasanaakaan. Verkon nimen voi myös piilottaa, mutta sillä ei ole suurta suojaavaa vaikutusta, koska asiansa osaava hakkeri löytää piilotetun nimen helposti.

3. Suojaa tukiasemat salauksella

Valitse verkossasi kulkevan datan suojaksi vahvin salaus, jonka reitittimesi tarjoaa. Vanhin menetelmä WEP (Wired Equivalent Privacy) on täynnä turvallisuusaukkoja, joten valitse WPA (WiFi Protected Acces) tai vielä mieluummin WPA2, joka on edeltäjäänsä vankempi. WPA2 käyttää enkryptauksessa AES-algoritmiä (Advanced Encryption Standard), mutta kaikki tukiasemat ja vanhimmat langattomat laitteet eivät tue sitä.

4. Ota MAC-osoitteen suodatus käyttöön

Joka tietokoneella on yksilöllinen MAC (Media Access Control) -osoite. Jos reititin tukee MAC-suodatusta, sille voi antaa listan sallittujen laitteiden MAC-osoitteista. Kun suodatus on päällä,

reititin päästää verkkoon vain listassa mainitut laitteet. Ohjeet MAC-osoitteiden etsimiseen löytyvät tarvittaessa verkkohaulla, ellei niitä ole annettu reitittimen käyttöohjeissa.

5. Poista etähallinta käytöstä

Joitakin reitittimiä on mahdollista ohjata mistä tahansa etähallintana (Remote Administration). Jos tähän ei ole välttämätöntä tarvetta, ominaisuus kannattaa ottaa pois käytöstä. Etähallinta on kyberrosvolle takaovi langattoman lähiverkon sisältöön.

Lisätietoja:

Check Point Software Technologies Finland Oy, maajohtaja Jukka Saarenmaa, p. 040 744 9531, jukka.saarenmaa@checkpoint.com

Seuraa Check Pointia sosiaalisessa mediassa:
Twitter: www.twitter.com/checkpointsw
Facebook: https://www.facebook.com/checkpointsoftware
YouTube: http://www.youtube.com/user/CPGlobal

Check Point Software Technologies Ltd.
Check Point Software Technologies Ltd. (www.CheckPoint.com) on maailman johtava internetin turvallisuuden asiantuntija, joka tarjoaa asiakkailleen tinkimättömän suojan kaikenlaisia tietoturvauhkia vastaan vähentäen tietoturvan monimutkaisuutta ja alentaen sen kokonaiskustannuksia. Check Point on ollut alan edelläkävijä patentoituun tekniikkaan perustuvasta Firewall-1-palomuuristaan lähtien. Tällä hetkellä Check Point kehittää innovaatioita Software Blade -arkkitehtuurin pohjalta tarjoten joustavia ja yksinkertaisia ratkaisuja, jotka voidaan räätälöidä vastaamaan täsmällisesti minkä tahansa organisaation turvallisuustarpeita. Check Point on alan ainoa palveluntarjoaja, joka ylittää teknologian ja näkee turvallisuuden liiketoimintaprosessin osana. Check Point 3D Security turvaa yrityksen tietovarannot yhdistämällä ainutlaatuisella tavalla ihmiset ja tietoturvakäytännöt sekä niiden valvonnan. Näin tietoturvatoiminnot saadaan vastaamaan organisaation liiketoiminnan tarpeita. Check Pointin asiakkaina on kymmeniä tuhansia erikokoisia yrityksiä, mukaan lukien kaikki Fortune- ja Global 100 -yritykset. Check Pointin palkitut ZoneAlarm-ratkaisut suojaavat miljoonia kuluttajia tietomurroilta, vakoiluohjelmilta ja identiteettivarkauksilta.