TIETOSUOJAVALTUUTETUN TOIMISTO

KOTI-WLANIN SUOJAAMINEN

Päivitetty 27.07.2010

www.tietosuoja.fi

KOTI-WLANIN SUOJAAMINEN

Langattomat lähiverkot mahdollistavat tietokoneiden välisen tiedonsiirron radioaaltojen avulla. Jatkuvasti yleistyvät WiFi-tuotteet toimivat lupavapaalla 2.4GHz taajuusalueella ja niitä saa pystyttää kuka tahansa. WLAN-teknologioilla rakennettuja verkkoja käytettäessä on kuitenkin syytä uhrata hetki langattoman verkon suojaamistarpeen arviointiin.

Langattoman lähiverkon kantama voi esteistä riippuen olla jopa 100 metriä, jolloin se ylettyy helposti monien eri tahojen ulottuville. Koska verkon kantavuutta on vaikeaa rajoittaa tai suunnata on tietoverkon väärinkäytön tai salakuuntelun riski normaalia lankaverkkoa suurempi. WiFi-tuotteet sisältävät sisäänrakennettuja suojamekanismeja salakuuntelua ja väärinkäyttöä vastaan, mutta ne pitää ottaa erikseen käyttöön. Tässä minioppaassa keskitytään yksityisen kotikäyttäjän kannalta merkittävimpiin WiFi-verkkojen suojausominaisuuksien käyttöönottoon.

Muista että kuka tahansa voi käyttää avointa ja suojaamatonta WiFi-verkkoa. Jos WiFi-verkko on liitetty Internetiin voi pahimmassa tapauksessa joku ulkopuolinen alkaa käyttämään verkkoliittymää rikolliseen toimintaan tai muuhun asiattomaan toimintaan. Tällaisesta toiminnasta syntyvät verkkojäljet johtavat tällöin avoimen verkon omistajaan!

Jos sinulla kotikäyttäjänä ei ole erityistä syytä pitää WiFi-verkkoasi kaikkien käytettävissä on viisainta suojata WiFi-verkko WPA- tai WPA2-salausmenetelmällä.

Langattoman lähiverkon suojaamistekniikat

WLAN-verkkojen suojaaminen pohjautuu pääsynvalvontaan sekä verkossa liikkuvan tiedon salakirjoittamiseen. Kotikäytössä pääsyä langattomaan verkkoon hallitaan salasanalla, jota ilman verkkoon ei voi kytkeytyä. Langattoman lähiverkon radioliikenteen salakuuntelua torjutaan salakirjoittamalla radioteitse kulkeva tieto käyttäen erilaisia salausalgoritmeja. WLAN-verkoissa käytettyjä suojausmekanismeja, jotka sisältävät sekä pääsynvalvonnan että salakirjoituksen ovat WEP (Wired-Equivalent Privacy), WPA (WiFi Protected Access) ja WPA2.

WEP-salaus löytyy jokaisesta WiFi-tukiasemasta, mutta sen tarjoama turvataso on tänä päivänä riittämätön. WEP-salaus on kuitenkin tyhjää parempi, sillä sen käyttöönotto viestittää selvästi että kyseinen langaton verkko ei ole tarkoitettu yleiseen käyttöön. WEP-salauksenkin murtaminen on rikos.

WPA ja WPA2 salaukset löytyvät kaikista tuoreemmista WiFi-tukiasemista ja ne tarjoavat hyvällä salasanalla varustettuna tällä hetkellä parasta salausta WiFi-verkkoihin.

Useat WiFi-tukiasemat tarjoavat lisäksi mahdollisuuden WiFi-verkon tunnisteen piilottamiseen (Hidden SSID) sekä verkkoon kytkettävien verkkolaitteiden erittelyyn (MAC-suodatus), mutta nämä menetelmät ovat kierrettävissä ja toimivat ainoastaan hidasteena mahdolliselle tunkeutujalle.

Kun pystytät WiFi-verkkoa kotiisi

- o Lue ostamasi WiFi-tukiasemasi käyttöohjeet
- o Mieti minne kaikkialle pystyttämäsi langaton verkko tulee kantamaan
- o Jos sinulla ei ole erityistä syytä pitää WiFi-verkkoasi kenen tahansa käytettävissä, aseta tukiasemasi käyttämään WPA tai WPA2-salausta
- o Valitse verkkosi salasana huolella. Vältä sanakirjoista löytyviä sanoja sekä pidä huoli että salasanasi on riittävän pitkä, vähintään 8 merkkinen.
- o Vaihda salasanasi säännöllisesti
- o Tutustu laajakaistaliittymäsi käyttösopimukseen. Jotkut operaattorit saattavat asettaa rajoituksia laajakaistaliittymänsä langattomalle käytölle.

Kun haluat käyttää WiFi-verkkoa

- o Pidä huoli että tietokoneesi palomuuri sekä virussuojaus ovat kunnossa!
- o Pyydä WiFi-verkon haltijalta tai ylläpitäjältä lupa käyttää verkkoa
- o Jos verkossa käytetään salausta pyydä myös verkon salasana
- o Älä ryhdy käyttämään tuntemattomia langattomia verkkoja, vaikka ne olisivatkin suojattuja – salausmenetelmät suojaavat vain verkon radioliikennettä, verkon salakuuntelu on vielä mahdollista tukiaseman päässä!

Vahva salasana…

- o ei ole sana millään kielellä eikä löydy minkään kielen sanakirjoista
- o sisältää sekaisin numeroita sekä pieniä ja isoja kirjaimia
- o ennen kaikkea on niin pitkä kuin vain suinkin mahdollista, vähintään 8 merkkiä mutta mielellään 14-127 merkkinen

Sanastoa

WLAN (Wireless Local Area Network)
Radioaalloilla toimiva langaton lähiverkko. Tarkemmat ominaisuudet ja nopeudet perustuvat kansainvälisen standardointiorganisaatio IEEE:n 802.11 määrityksiin. Yleisimmät Suomessa käytössä olevat 802.11-määrityksen ovat 802.11b (11 Mbps nimellisnopeudella toimiva langaton verkko), 802.11g (54 Mbps nimellisnopeudella toimiva langaton verkko) sekä 802.11i (WPA ja WPA2-suojausmekanismit).

WiFi (Wireless Fidelity)
Kansainvälisen Wi-Fi Alliancen yleisnimi tietoliikennelaitteille, jotka noudattavat IEEE 802.11-määrityksen mukaisia WLAN-standardeja.

SSID (Service Set Identifier)
Langattoman lähiverkon tunniste.

MAC (Media Access Control)
Verkkokortin oma yksilöllinen postiosoite, jota verkkokortit käyttävät tiedon välittämiseen toisilleen.

WEP (Wireless Equivalent Privacy)
WLANin alkuperäinen suojausmekanismi. Salakirjoittaa radioteillä kulkevan tiedon. WEP-salauksesta löytyneiden virheiden takia sitä ei voida enää pitää tehokkaana suojauskeinona.

WPA (Wifi Protected Access)
WEP:n korvaajaksi pikaisesti laadittu suojaus.

WPA2 (Wifi Protected Access 2)
Tuorein WLANin suojausmekanismi. Kotikäyttäjän näkökulmasta WPA, jossa käytetään tiedon salaukseen Yhdysvaltojen kansallista salausstandardia.

Lisätietoa

- Turvallisesti nettiin, Tietoturvaopas, http://www.tietoturvaopas.fi
- Laajakaistan ostajan opas, Viestintävirasto, http://www.ficora.fi/index/palvelut/palvelutaiheittain/puhelinjalaajakaista/ostajanoppaat/ostajanopaslk.html