



DATAOMBUDSMANNENS BYRÅ

SKYDDA HEMMA-WLAN

Uppdaterad 27.07.2010

www.tietosuoja.fi

SKYDDA HEMMA-WLAN

Trådlösa lokala nätverk möjliggör dataöverföring mellan datorer med hjälp av radiovågor. WiFi-produkter som fungerar på det licensfria frekvensområdet 2,4 GHz blir allt vanligare och får sättas upp av vem som helst. Då man använder nätverk uppbyggda med WLAN-teknik är det dock skäl att ägna en stund åt att utvärdera det trådlösa nätverkets skyddsbehov.

Ett trådlöst nätverk kan beroende på fysiska hinder nå en räckvidd upp till 100 meter och kan på så sätt bli tillgängligt för många olika parter. Eftersom det är svårt att begränsa eller rikta nätets räckvidd blir risken för missbruk eller avlyssning av nätverket större än för kabelnätverk. WiFi-produkter har inbyggda skyddsmekanismer mot avlyssning och missbruk, men dessa bör tas i bruk särskilt. Denna miniguide koncentrerar sig på WiFi-nätverkens mest relevanta skyddsmekanismer för privata hemanvändare.

Kom ihåg att vem som helst kan använda ett öppet och oskyddat WiFi-nätverk. Om WiFi-nätverket är anslutet till Internet kan i värsta fall någon utomstående använda nätanslutningen för kriminell eller obehörig verksamhet. Spåren efter sådan verksamhet leder då till ägaren av nätverket!

Ifall du som hemanvändare inte har särskilda skäl att hålla ditt WiFi-nätverk öppet för alla är det klokast att skydda WiFi-nätverket med WPA- eller WPA2- krypteringsmetoden.

Skyddstekniker för trådlösa lokala nätverk

Skyddet för WLAN-nätverk grundar sig på accessövervakning och kryptering av data som rör sig i nätet. Vid hemmabruk kontrolleras accessen till trådlösa nätverk med ett lösenord som krävs för anslutning till nätverket. Avlyssning av det trådlösa nätverkets radiotrafik bekämpas genom att kryptera information som rör sig i etern med hjälp av olika krypteringsalgoritmer. Till skyddsmekanismer som används i WLAN-nätverk och som innehåller både accessövervakning och kryptering hör WEP (Wired-Equivalent Privacy), WPA (WiFi Protected Access) och WPA2.

Varje WiFi-stödstation har WEP- kryptering, men dess säkerhetsnivå är otillräcklig i dagens läge. WEP-kryptering är dock bättre än ingenting, då man med hjälp av den klart signalerar att nätverket i fråga inte är avsett för allmänt bruk. Dekryptering av en WEP-kodning/kryptering är ett brott.

WPA och WPA2 finns i alla nyare WiFi-stödstationer och i kombination med ett bra lösenord erbjuder de för tillfället det bästa skyddet för WiFi-nätverk.

Många WiFi-stödstationer erbjuder möjlighet att gömma WiFi-nätverkets ID (Hidden SSID) samt separering av apparater anslutna till nätverket (MAC-filtrering), men dessa metoder kan kringgå och utgör endast dröjsmål vid möjliga intrång.

När du bygger upp ett WiFi-nät i ditt hem

- Läs igenom WiFi-stödstationens bruksanvisning.
- Fundera på vilken räckvidd ditt trådlösa nät kommer att ha.
- Om du inte har något särskilt skäl att upplåta ditt WiFi-nät åt vem som helst bör du ställa in din stödstation att använda WPA eller WPA2-kryptering.
- Välj ditt lösenord till nätet omsorgsfullt. Undvik ord som finns i lexikon och se till att lösenordet är tillräckligt långt, minst 8 tecken.
- Byt lösenord regelbundet.
- Bekanta dig med användaravtalet till din bredbandsanslutning. En del operatörer kan begränsa användandet av trådlös förbindelse i sitt bredband.

När du vill använda WiFi-nät

- Se till att brandmur och virussydd i din dator är i ordning!
- Anhåll om tillstånd att använda WiFi-nätet av innehavaren eller den nätansvariga.
- Om kryptering används i nätet, be också om nätets lösenord.
- Börja inte använda okända trådlösa nät fast de är skyddade - skyddsmetoderna rör endast nätets radiotrafik, det är möjligt att avlyssna ännu i stödstationen.

Ett starkt lösenord ...

- är inte ett ord på något språk och finns inte i något språklexikon
- innehåller en blandning av siffror samt små och stora bokstäver
- är framför allt så långt som möjligt, minst 8 tecken men gärna 14–127 tecken.

Några begrepp

WLAN (Wireless Local Area Network)

Trådlöst lokalt nätverk som fungerar med radiovågor. Mer preciserade egenskaper och hastigheter enligt specifikationerna beror på den internationella standardiseringsorganisationens standard IEEE 802.11. De vanligaste 802.11-definitionerna i Finland är 802.11b (trådlöst nät som fungerar på den nominella hastigheten 11 Mbps), 802.11g (trådlöst nät som fungerar på den nominella hastigheten 54Mbps) samt 802.11i (WPA och WPA2-skyddsmekanismerna).

WiFi (Wireless Fidelity)

Internationella WiFi Alliance allmänna namn på apparater för datakommunikation som lyder under WLAN-standarder med IEEE 802.11-definitioner.

SSID (Service Set Identifier)

ID för ett trådlöst lokalt nätverk.

MAC (Media Access Control)

Nätkortets individuella postadress, som nätkortet använder för dataöverföring sinsemellan.

WEP (Wireless Equivalent Privacy)

Den ursprungliga skyddsmekanismen för WLAN. Krypterar radiosänd information. Kan inte längre anses som ett säkert skydd p.g.a. fel som detekterats i WEP-krypteringen.

WPA (Wifi Protected Access)

Skydd som konstruerats snabbt för att ersätta WEP.

WPA2 (Wifi Protected Access 2)

Den senaste skyddsmekanismen för WLAN. Ur hemanvändarens synvinkel WPA som använder Förenta Staternas nationella standard för kryptering.

Ytterligare information:

- Tryggt på nätet, Guide om datasäkerhet, http://www.tietoturvakoulu.fi/ru_aloitus.htm
- Guide för köparen – bredbandsförbindelse, Kommunikationsverket, <http://www.ficora.fi/sv/index/palvelut/palvelutaiheittain/puhelinjalaajakaista/ostajanoppaat/ostajanopask.html>