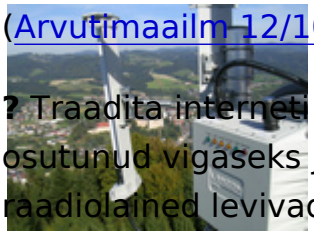
WLAN ärikeskkonnas – risk või võimalus?

14 aastat tagasi - 22.04.2011 Autor: Ando Urbas

(Arvutimaailm 12/10)



? Traadita interneti kasutamist on firmades peljatud, sest mitu turvaalgoritmi on osutunud vigaseks ja füüsiliselt pole võimalik ligipääsu võrgule piirata – raadiolained levivad, kuhu tahavad.

! Kui WLANi seadmeid ja tarkvara õigesti hallata, siis saab ka traadita võrgu piisavalt turvaliseks, et ohtu ärikasutajale sellest ei teki.

Traadita internet teeb elu mugavaks nii kontorikeskkonnas kui ka tööstushoonetes – sülearvutid pääsevad võrku koosolekuruumis ja kohvinurga diivanil, toomis- või laohoones võib juhtmete pärast muretsemata seadmeid ümber paigutada. Kuid WiFi võrke on aastaid kimbutanud turvalisusprobleemid, vahel ka levi- ja stabiilsusküsimused. Kuidas ehitada ärikeskkonda turvaline ja stabiilne traadita võrguühendus?

Esimene mure on turvalisus. Vaevalt, et keegi enam WEP turvaalgoritmi kasutab, mis on vaid minutitega lahtimurtav, ent ka laialt levinud WPA-PSK (TKIP) süsteemis on selged nõrkused ning lihtsa või lühikese parooli korral ei valmista sellegi lahtimurdmine suurt probleemi. Ainukesena on praeguseks veel häkkimiskindlaks osutunud WPA2 koos CCMP algoritmiga, kuid kes teab, mis homme juhtub. Kuid turvaalgoritmi nõrkused pole kaugeltki mitte ainuke mure WiFi turvalisuses.

Suurim mure peitub võtmehalduses – kes teab firmas WiFi parooli? Niikaua, kuni kogu firma WLANi võrk kasutab vaid ühte parooli, mida siis IT-administraator käib igale poole sisestamas, ei saa süsteemi turvaliseks pidada. Iga saladus lekib kunagi. Kujutage nüüd ette, mis juhtub, kui töölt lahkub mõni inimene või varastatakse sülearvuti – vaene administraator peaks kõik WLANi seadmed läbi jooksma ja paroolid ära vahetama.

Kasutajapõhine autentimine

Toimivaks turvalisuseks tuleb iga WLANi kasutaja eraldi autentida. Seda saab teha 802.1x ja RAIDUS/EAP autentimisserveriga, mille funktsionaalsus on sisse ehitatud igasse Windows Serveri platvormi (IAS, Internet Authentication Service).

See loob keskse halduskeskkonna, WiFi võrgule ligipääs muutub personaliseerituks, jälgitavaks, lihtsalt administreeritavaks. Ühe üldise ligipääsukoodi asemel on igal töötajal/seadmel oma, olgu siis tegu parooli- või sertifikaadipõhise autentimisega.

Kui tekib probleem mõne kasutaja või tema seadmega (näiteks sülearvuti vargus), on nüüd lihtne piirata vaid selle kasutaja õiguseid ilma, et peaks kogu infrastruktuuri üle vaatama. Lisaks saab eri kasutajatele võimaldada ligipääsu erinevatele võrguosadele (müügiosakond ei pääse ligi raamatupidamise võrgule jne), piirata teenuste kasutamist (teatud programmide või veebilehekülgede blokeering) ning jälgida, millise ruuteri levialas mõni kasutaja oma sülearvutiga parasjagu viibib.

Virtualiseerimine on abiks

Sageli tekib probleeme sellega, et kõik WLAN-seadmed ei toeta soovitud turvalisuse taset. Eriti tööstuskeskkonnas võib leiduda vanu, aga kalleid seadmeid, mis ei saa hakkama näiteks millegi muuga kui 64bitise WEP võrguga. Äriklassi WLAN-seadmega on sellisel juhul võimalik luua mitu virtuaalset WiFi võrku. Kasutaja näeb erinevaid SSID-nimega võrke, igaühel oma turvalisuse tase. Erinevate SSIDdega ühendatud kliendid saab eraldada virtuaalsetesse võrkudesse (VLAN) ning rakendada neile erinevaid ligipääsusüsteeme.

Nii on lihtne luua ka firmat külastavatele inimestele eraldi võrguligipääs, mis on samas põhivõrgust täielikult eraldatud ning mille parooli võib muuta kas või mitu korda tunnis.

Ühe raadiomooduliga seadmetega saab luua üldjuhul kuni kaheksa erineva SSIDga võrku, kahe raadiomooduliga aga juba 16. Kahe raadiomooduliga seadmed on tavaliselt ka kahesageduslikud ehk üks nendest võib töötada 2,4 GHz sagedusalas vanemate arvutite ja seadmete tarbeks, teine 5 GHz sagedusalas, kus on üldjuhul kordades vähem segajaid, rohkem üksteist mittesegavaid kanaleid, mille vahel valida ja mis võimaldab vastava toega seadmetele kokkuvõttes kiiremat netiühendust.

Kuidas riistvaraliselt hallata?

Juba paari WLAN-seadme, rääkimata siis kümne või paarikümne korral kerkib teravalt üles küsimus nende kesksest haldusest. Kui kõike ülaltoodut saab veel enam-vähem teostada ka hoolikalt valitud koduste seadmetega ning seeläbi kenakese kopika säästa, siis keskseid haldussüsteeme pakuvad vaid äriklassi seadmed.

Äriklassi võrguseadmete korral on võimalik ühest arvutist ühe programmida jälgida ja hallata kõikide seadmete tööd. Näiteks teha püsivara uuendusi, saata kõigile korraga seadetemuudatused (paroolivahetus) või jälgida, kas kõik on töökorras.

Tõelise edu tagab aga riistvaraline WLAN-kontroller, mis jälgib ja juhib kõigi WiFi ruuterite tööd, pakub keskse halduskeskkonna kõigile WLAN-seadmetele ja jälgib kogu võrgu turvalisust. Näiteks annab teada võõraste WiFi-klientide või pääsupunktide (AP) ilmumisest võrku või sissemurdmiskatsetest. Samuti vahetab see informatsiooni seadmete vahel ja optimeerib raadiosageduste kasutamist – alates vabade kanalite jälgimisest kuni rändlusteenuse parameetrite muutmiseni, et kogu WLAN-võrgu koormust ühtlasemalt jagada.
Kõrgeima turvalisuse taseme korral ei ole üheski WiFi ruuteris salvestatud mitte ühtegi seadistust, parooli ega sertifikaati – iga alglaadimise käigus saadab seadistuse ruuteri mällu WLANi kontroller. See tagab, et mingeid andmeid ei leki isegi mõne WiFi ruuteri füüsilise varguse korral.

ANDO URBAS

- Lahendused

- Võrguseadmed
- Andmeside