Jak úspěšně zabezpečit WLAN?

Vložil/a Mira [1], 24 Březen, 2005 - 19:38

- Security [2]
- WiFi & Wireless [3]

Kratičký článek o tom, jak zabezpečit WiFi síť. Všude se píše o napadnutelnosti WIFI, o tom jak lze obejít WEP nebo nyní již dokonce i WPA atd ... ale nikde se již nepíše o tom, jak takovou síť co nejvíce zabezpečit aby se útoky eliminovaly na minimum.

O WiFi (Wireless Fidelity) se již nějaký pátek zajímám. Nechci tvrdit, že jsem expert, to ne, ale zajímám se o nové a nové věci.

Všude na internetu najdete plno článků o tom, jak je zabezpečení WLAN (Wireless Local Area Network) lehce prolomitelné. Ale existuje málo článků, které by se zabývaly tím užitečnějším - jak zabezpečit, jak omezit útoky od hackerů atd...

Bohužel bezdrátové sítě mají oproti svým kabelovým kolegům jednu zásadní nevýhodu - nelze dostatečně omezit prostor, kde lze signál zachytávat a kde ne.

Pár rad:

Když si koupíte AP (Access Point) - přijdete domů :) nebo do firmy ... AP zapojíte (co jiného byste s ním také dělali že ano) ... většina AP má bohužel standartně webovské admin rozhraní - každý ví že přenos na portu 80 se dá snadno zachytit jakýmkoliv snifferem (např. Cain & Abel [4]) ... lepší AP lze konfigurovat např přes www rozhraní ale pouze přes LAN - nikoliv přes WLAN, což je už bezpečnější. Ještě líp jsou na tom AP které se konfigurují přes RS 232 nebo dokonce SSH nebo WinBOX což je Windowsáckej prográmek, kterým se konfigurují stanice založené na RouterOS Mikrotik [5].

Takže podle toho, za jakým účelem AP pořizujete se také dívejte jak lze AP spravovat ... není vždy pravda že v jednoduchosti je dokonalost ... vzdálená správa AP přes nezabezpečené protokoly je ošidná.

Pokud máte omezené finanční prostředky, je jasné že sáhnete po levnějším řešení, které je vybaveno pouze web rozhraním ... takové AP užijete asi v domácnosti, rozhodně nedoporučuji pro firmy, ba dokonce pro velké společnosti a když už tak:

1. ihned změňte administrátorské jméno, heslo !!!**A TAKÉ STANDARTNÍ IP ADRESU**!!!
2. vypněte vysílání SSID - ikdyž je jasné že jsou programy které SSID bez problému odhalí, je to první krok k ukrytí Vaší sítě před amatéry ...
3. Zapnětě nejvyšší požnou podporu šifrování (64, 128, 256 bitů) - zvolte nejvyšší možnou, kterou podporují všechny klientské karty. Je jasné že WEP lze prolomit, ale lepší malá ochrana než žádná. Pravidelně měňte klíč a distribujte ho mezi klienty (nikoliv emailem ale jiným humánním způsobem, který je bezpečnější)
4. Některá zařízení již mají podporu *WPA* (*WiFI Protected Access*) - je to nový bezpečnostní mechanismus ratifikovaný WiFI Aliancí - využívá stejný šifrovací mechanismus jako *WEP* (128 b) ale obsahuje dočasné *TKIP* (Temporal Key Integrity Protocol) klíče - ty se mění každých 10 000 packetů - to už ale na SP někde ale asi zaznělo. BACHA ! *WPA* musí podporovat všechna zařízení v síti ...
5. Již teď by měla být síť amatérem nenapadnutelná - ale v dnešním světě nejsou jen amatéři, že? Proto jdeme dále ...
6. Filtrování MAC adres - odhalit MAC adresu nějakého zařízení není zase tak jednoduché jako

odhalit 64b WEP klíč, ale jde to. To ale není důvod, proč tuto funkci nezapínat ... ale i tohle má své pro a proti ... filtrování MAC adres je dobré tam, kte nepoužíváte roaming ... nebo kde máte jen jedno AP - zde musíte pořád udržovat platný seznam ... např. prodáte kartu tak ji musíte smazat ze seznamu a přidat tam jinou kterou třeba koupíte. To je ale jasné... nevýhodou je, že při použití roamingu již na dvou nebo třech AP musíte udržovat aktuální seznam MAC adres - a to je jak víte šílenost hrabat se v číslech a pořád něco přepisovat ... záleží také, jak často se například ve firmě mění HW atd ... pro použití doma je to bezúdržbová záležitost :-)

7. *Denial of Service* (DoS) - tyto útoky sice nepatří v pravém slova smyslu mezi průniky do sítě, ale mohou se vysíláním nesmyslných požadavků postarat o výpadek sítě (vyřazení sítě z provozu) - takže pokud Vaše AP má možnost zapnout ochranu před DoS - rozhodně ji zapněte !!
8. Pokud máte firmu, dejte si pozor, aby si někdo ze zaměstnanců nevměstnal do sítě vlasní AP a neposílal si internet třeba domů :) pak by se mohlo stát že se Vám někdo napíchne do sítě a zneužije citlivá data - v tomto případě kdyby útočník využíval Vaše připojení k internetu, je to ta lepší varianta ... mohlo to dopadnout hůř :)
9. ANTÉNY :: Amatéři s oblibou na svých AP zbytečně používají vysoce ziskové antény (viděl jsem i na 200 metrů 18 dbi všesměrovku :) v nezarušeném prostředí) - čím nižší zisk tím nižší dosah - dalo by se amatérsky říct ... neberu ISP kteří potřebují dostat signál co nejdál :-) ale proč používat všesměrovou anténu na vysílání jedním směrem ? (pokud potřebujete spojení pouze jedním směrem, zkuste se poohlédnout po nějakých směrových anténách - sektorovky, panelovky, paraboly, yaginy a v nejhorším případě síta) ... když omezíte vysílání na co možná nejužší směr, máte jistotu že se na Vás nenapíchne nikdo "zezadu" ... no a pokud zjistíte útočníka, víte ze kterého směru se připojuje (ikdyž to asi nebude moc platné)
10. Nikomu nesdělujte svá hesla, MAC adresy nebo šifrovací klíče ... pokud dovolítě vašemu kamarádovi aby si na Vaši síť napíchnul notebook a pařil na netu, po jeho odchodu změňte šifrovací klíč !!
11. ROZDĚLTE LAN A WLAN - pokud máte doma nebo spíše ve firmě sítě LAN a WLAN - pokud to jen jde, oddělte je od sebe ... máte zase vyšší jistotu že ten kdo napadne bezdrát, nebude mít přístup k drátům :-)
12. Nic nepodceňte - mohu Vám říct, že pokud si takhle síť zabezpečíte, nikdo se na Vás nabourávat nebude ... pokud se útočník dostane přes jeden kopec .. čeká ho další ... nabourání se do takové sítě není otázka pár minut, ale hodin, dnů ba i týdnů ... a věřte mi že to nikoho nebude bavit jen pro to aby se k vám dostal kvůli internetu zadarmo ... takže taková síť je relativně hodně bezpečná a nikdo se do takové sítě nebude lámat, pokud nebude přesně vědět po čem jde ... přestane se o vaši síť zajímat a půjde zase o dům dál :o)
13. řiďte se body 1 - 12

A pokud se Vám i přes tato opatření někdo do sítě vlámal nebo pokud se Vám zdá že po dočtení tohoto článku nejste ani o chlup chytřejší a myslíte si že tento článek je škvár, poproste admina o výmaz :)
V opačném případě díky za pozornost a za kladné hodnocení
Poprvé pro SP M. Šraga (webmaster@sraga.cz [6])

URL článku:
https://security-portal.cz/clanky/jak-%C3%BAsp%C4%9B%C5%A1n%C4%9B-zabezpe%C4%8Dit-wlan

Odkazy:
[1] https://security-portal.cz/users/mira
[2] https://security-portal.cz/category/tagy/security
[3] https://security-portal.cz/category/tagy/wifi-wireless
[4] http://www.oxid.it
[5] http://www.routeros.cz/
[6] mailto:webmaster@sraga.cz