Triky hackerů bezdrátových sítí

"Dobrý den, pojďte dál - dveře jsou otevřené!" Řekli byste to nějakému cizinci? Vaše komponenty WLAN to však dělají. Nabízejí nezvaným hostům přístup k vašim nejtajnějším datům.

Margit Kuther

Bezdrátové sítě nabízí skvělou mobilitu a pohodlí: díky nim už nemusíte sedět v kanceláři, ale můžete se s Wi-Fi notebookem například uvelebit na terase a pracovat tam, tedy pokud máte osvíceného zaměstnavatele a terasu. Tato svoboda však má i stinné stránky. Na rozdíl od drátové komunikace může každá Wi-Fi stanice v dosahu váš signál odchytávat. Ať už z ulice, nebo z bytu naproti. V tomto článku se dozvíte, jaké slabiny WLAN sítě ukrývají.

Hackeři na cestách: Co je dovoleno, bývá i často využíváno. Hackeři se soustředí na špionáž v cizích WLAN sítích nebo se snaží do takových systémů proniknout kvůli surfování. Jak to tito čmuchalové dělají, to se dozvíte v části "Útoky" (od strany XX).

V džungli paragrafů: WLAN je otevřený. Můžeme se do něho podívat? Hacker nepozorovaně využije počítač k surfování a tajně uloží dětskou pornografii. Kdo za to bude odpovědný? V rámečku na straně XX se k tomuto problému vyjádří právník.

Zamkněte svoji bezdrátovou síť': Zbavte se nevítaných hostů tak, že svoji síť izolujete. Část "Bezpečnost" (od strany XX) prozradí, jak postupovat. V síti byste měli provést všechna zmíněná bezpečnostní opatření, jelikož udělat jen nějaká by byla fušeřina. Absolutně bezpečný systém sice neexistuje, ale naše tipy by měly váš soukromý WLAN celkem spolehlivě ochránit.

Nebezpečí

Pokud nově instalujete bezdrátovou síť, už v tu chvíli zvete cizí osoby k nahlédnutí. Příčina jednoduchého přístupu spočívá v samotné technologii WLAN, ale rozvněž v defaultním nastavení bezdrátových komponent.

1. WLAN používá stejné standardy

WLAN stojí na několika standardech. V současné době je to v sektoru 5 GHz norma IEEE 802.11a s teoretickou propustností 54 Mb/s. Ve frekvenčním pásmu 2,4 GHz to jsou známé standardy IEEE 802.11b a jeho rychlejší následovník 802.11g. Varianta "g" je zpětně kompatibilní s 11b, takže si většina komponent WLAN rozumí. Norma IEEE 802.11a není kompatibilní s verzemi 11b a 11g a z důvodu legislativní regulace nebyla donedávna v České republice použitelná. Od 1. 9. 2005 je však rozhodnutím ČTU povolen provoz zařízení standardu IEEE 802.11a/h v pásmu 5470-5725 MHz (norma ETSI) bez omezení a v pásmu 5150-5350 MHz (norma FCC) pouze uvnitř budov.

Ochranná opatření: Kdo přestoupí na IEEE 802.11a, profituje z toho, že v naší zemi se hackeři specializovali na pronikání do IEEE 802.11b/g. Dokonalou ochranu to však nepředstavuje, protože hackerské programy pro sítě 11a samozřejmě existují.

Přestup z "bégéčkové" Wi-Fi na "áčkovou" ale přesto nemůžeme úplně doporučit. Přijdete totiž o výhodu mobility a o možnost pohodlně komunikovat na různých místech s ostatními sítěmi WLAN. Klidně zůstaňte u IEEE 802.11b nebo 11g, chraňte svoji síť jiným způsobem.

Všestranné využití

Kdo by nechtěl jeden ze standardů IEEE 802.11a nebo 11b/g, pro toho mají někteří výrobci na výběr komponenty, které zvládají všechny tři normy. K nim se počítá například USB adaptér DWL-G122 od D-Linku, zhruba za 1 200 Kč. Takových univerzálních adaptérů však není na trhu tolik a navíc jsou obvykle dražší než srovnatelné komponenty IEEE 802.11b/g.

2. Otevřeno od výrobce

Když chce WLAN klient (adaptér) přistoupit k bezdrátové síti, pošle požadavek na Access Point. V zásadě existují dva způsoby oprávnění přístupu, které jsou aktivovány v menu "Přístup", "Bezpečnost", nebo "Access". U autentizace "Open Key" oprávní Access Point každého klienta, který se chce přihlásit. U autentizace "Share Key" již musí klient překonat několik překážek. Zde jsou totiž aktivována některá přístupová omezení, jako kódování dat.

Když zřizujete bezdrátovou síť poprvé, je zpravidla otevřená, protože téměř všechny Access Pointy a všechny adaptéry jsou od výrobce konfigurovány jako otevřené. Výrobci totiž chtějí uživatelům, kteří se většinou v sítích příliš nevyznají, surfování bez kabelu co nejvíce zjednodušit. Kdo toto nastavení ponechá otevřené, posílá svá data do éteru nechráněná a nabízí cizím účastníkům téměř volný přístup do PC systémů sítě.

Ochranné opatření: V bezpečnostní nabídce zvolte "Shared Key", abyste bezdrátovou síť ochránili před vetřelci.

Autentizace "both"

Některé Access Pointy nabízejí mód "both" (anglicky "oba") nebo "Open Key/Shared Key". Pokud je tento způsob provozu aktivován, zpřístupní Access Point bezdrátovou síť jak pro klienty, které se přihlašují přes "Open Key", tak pro ty, kteří používají "Shared Key". Z bezpečnostních důvodů se raději rozhodněte pro "Shared Key".

3. Access Pointy se jmenují stejně

Volali jste někdy v plném metru na někoho "Karle"? Pravděpodobně se otočila polovina lidí. Stejně se chovají i Access Pointy. Výrobci většinou nechávají zapnutý standardní SSID (Service Set Identifier) jako "Any", "Default", nebo "Wlan", případně do něj vloží vlastní název jako "Netgear". Zkušený hacker tak rychle získá přístupové jméno. Pokud hacker vypátrá i výrobce Access Pointu, potom rychlý pohled na jeho webovou stránku prozradí i přednastavené hodnoty SSID. Výrobci bezdrátových komponent totiž většinou přiřazují svým produktům vždy jeden a tentýž SSID.

Ochranné opatření: Svému Access Pointu vždy přidělte nové jméno (viz tip 13).

4. Access Point prozrazuje své jméno

Access Point se hlásí Wi-Fi klientům standardním způsobem. Název bezdrátové sítě (SSID) vysílá tak, aby byl srozumitelný pro všechny komponenty. Zveřejnění SSID tak zjednodušuje potenciálním vetřelcům přístup do sítě: prozradí cizímu klientu, například notebooku Wi-Fi, nejen to, že se nachází v síti a jak se jmenuje. Zájemci zjistí i kanál, na němž datový transfer probíhá.

Ochranné opatření: Zabraňte vysílání SSID (viz Tip 14).

SSID: Každá bezdrátová síť se dá jednoznačně určit přes identifikaci sítě nebo Service Set Identifier. Aby se mohli klienti WLAN přihlásit k Access Pointu,

potřebují SSID. To se konfiguruje v základní stanici (Access Point) a zanese se do softwaru klientů, kteří chtějí přistoupit k Access Pointu.

5. Dosah bezdrátové sítě

Sedíte na terase a bezdrátově vyměňujete data s počítačem v kanceláři. Data však putují nejen do kuchyně, ale například i do sousedního bytu nebo na ulici. Anténa vysílá radiové vlny zpravidla kruhově. Ve volném prostoru mohou doputovat až do vzdálenosti tří set metrů. Pokud musí radiové vlny překonávat překážky jako například zdi, potom síla signálu strmě klesá. V takovém případě se radiové vlny v závislosti na materiálu, jímž musí projít (beton, kov.) dostanou na zhruba 10 až 30 metrů. Jakmile ale překonají hranice vašeho bytu, může je na obecném prostranství kdokoliv odchytávat.

Ochranné opatření: Omezte dosah své bezdrátové sítě (viz tip 16). Bezdrátovou síť vypínejte, když ji nepotřebujete (viz tip 17).

Vysílací výkon

Efektivní izotropní výkon vysílání (EIRP - Effective Isotropic Radiated Power) Wi-Fi přístrojů v pásmu 2,4 GHz nesmí v EU překročit 100 miliwattů EIRP (20 dBm). EIRP je vysílací výkon, jímž musíte zásobovat anténu vysílající rovnoměrně do všech prostorových směrů (izotropně), aby přístroj ve vzdáleném poli dosahoval stejné síly jako u směrové antény.

dBm jsou decibely ve vztahu k miliwattům. V praxi to znamená, že zohledňovaný výkon vysílání vyplývá z výkonu zařízení WLAN po odečtení všech ztrát, jako tlumení v kabelech, plus směrový zisk antény.

Kdo si anténu postavil sám a nemůže měření provést, měl by se v okruhu svých známých poohlédnout po nějakém odborníkovi, třeba radioamatérovi. Ten by pak snad mohl říci, zda je výkon takové externí antény v povoleném rozsahu.

Útoky

Čmuchalové se snaží proniknout do cizích bezdrátových sítí, aby mohli zdarma surfovat nebo si prohlížet cizí data. Předvedeme vám pár triků, které používají, abyste měli přehled, jakým nebezpečím je vaše bezdrátová síť vystavena.

Když hacker pronikne do vaší sítě, může se po ní pohybovat, jak chce. Je to stejné, jako kdybyste dovolili cizinci připojit se přímo k vašemu notebooku, surfovat pomocí něj na internetu, dívat se na vaše data a stahovat cokoliv na váš počítač. Nebezpečí se skrývá i v e-mailových serverech: hackeři mohou například zneužít vaši identitu k rozesílání spamu. I když přítomnost vetřelce v síti objevíte, zjistíte v nejlepším případě jeho IP a MAC adresu - chytit ho je téměř nemožné.

6. Snadný průnik

Kdo chce rychle surfovat na internetu pomocí cizí bezdrátové sítě, jde většinou tou nejjednodušší cestou - najde si systém bez kódování. Zde se hodí zmínit citát z jednoho hackerského fóra: "Scan Tool ukazuje, jestli je síť, kterou chytáš, zakódovaná nebo ne. Pokud je, najdi si jinou. A pokud zakódována není. musí se ukázat síť, přes kterou se teď můžeš připojit. Pak bys měl využít její přístup na internet."

Používáte-li bezdrátovou síť, musíte s hackery a dalšími vetřelci počítat úplně všude. Nepotřebují žádné drahé vybavení. Bohatě jim stačí notebook. A Wi-Fi se již stalo standardní funkcí mobilních počítačů.

Potřebné pátrací nástroje najdete na internetu během okamžiku. Vyrazíte-li na procházku s Wi-Fi notebookem nebo PDA, rychle najdete (hlavně v centrech větších měst nebo na sídlištích) špatně chráněné bezdrátové sítě a může se zkusit na ně napojit. Existuje pro to pojem: warxing. "War" znamená "Wireless Access Revolution", "X" naznačuje způsob pohybu: chůze (walking), řízení (driving), létání (flying). Warwalking třeba označuje člověka, který se na slídění po nezabezpečených bezdrátových sítích vydal pěšky. A na Wardriving je potřeba dopravní prostředek, většinou auto.

Ochranné opatření: Svoji bezdrátovou síť bezpodmínečně izolujte (viz část "Bezpečnost" od strany XX).

7. Skenery vyhledávající bezdrátové sítě

Hackeři pročesávají éter pomocí speciálních vyhledávačů. Jejich cílem jsou informace, s jejichž pomocí proniknou do cizích sítí. K těmto informacím patří třeba to, zda je síť zakódována nebo ne (viz tip 2), kdo je výrobce Access Pointu (tip 3), SSID (tip 4), síla signálu (tip 5) a MAC adresa (tip 15).

Mezi nejpoužívanější patří aktivní vyhledávače pro Windows, s nimiž se pracuje velmi snadno. Aktivní skenery vysílají v pravidelných odstupech "requestové" pakety do éteru a hledají Access Pointy, který je pošle zpátky.

Komunikace probíhá zhruba následovně: skenery volají přes každý kanál: "Haló, je tam někdo?" Pokud je nějaký otevřený Access Point slyší, odpoví: "Ano, tady je bezdrátová síť xxx", xxx zde znamená SSID Access Pointu. Aktivní skenery mohou vypátrat pouze Access Pointy, které posílají zpět datové pakety speciálně jim. Nejznámějším aktivním skenerem je **Network Stumbler** (na CD, viz rámeček dole).

Pasivní skenery pracují skrytě a jsou efektivnější. Neposílají malé pakety, nýbrž lapají všechny datové pakety, které se pohybují v éteru. Pasivní skenování je možné pouze v případě, kdy může pátrající WLAN adaptér přejít do módu "Monitor". Adaptér pak pošle všechny pakety, které odchytává, dále na ovladač - i takové, které nejsou určeny jemu. Nejznámějším pasivním skenerem bezdrátových sítí je Kismet. Ten však funguje pouze pod Linuxem.

Ochranné opatření: Otestujte svoji Wi-Fi síť (viz rámeček na straně XX). Zakódujte ji (viz tip 12). Bezpodmínečně změňte jméno výrobce (viz tip 13). Vypněte odesílání SSID (viz tip 14). Zredukujte sílu signálu (viz tipy 16 a 17).

8. Naslouchání a zaznamenávání dat

Když se hacker dostane do sítě, může pomocí softwaru pro analyzování sítí sledovat, ukládat a analyzovat datový provoz. Takovým nástrojem je třeba Ethereal (rámeček dole na této stránce).

Ochranné opatření: Otestujte svoji bezdrátovou síť (rámeček na straně 50). Zakódujte důležitá data na pevném disku, například pomocí softwaru **Steganos Safe 8.0** (*www.steganos.com*, 29,90 eur).

9. Prolomení šifrování WEP

Před vetřelci nejste úplně chráněni, ani když bezdrátovou síť zašifrujete pomocí WEP. WEP je totiž letitý bezpečnostní standard, který jej již dlouhou dobu prolomený.

Crack-Tools na WEP klíče potřebují podle způsobu práce něco mezi několika dny a pár minutami. K rychlým programům v tomto směru patří například linuxový **Chopchop** od firmy Korek. WEP kódování vykáže pouze ty, kteří se do cizí bezdrátové sítě dostali nedopatřením a rozhodně do ní nechtěli proniknout.

Ochranné opatření: Novější šifrování je účinnější (viz tip 12).

10. Podsunutý WLAN klient

Přístup na bezdrátovou síť povolujete pouze těm, jejichž MAC adresa je Access Pointu známa. Ale i v tomto případě se vám tam může vplížit nechtěný klient, jakmile získá pomocí WLAN skeneru MAC adresu legitimního uživatele sítě. Tuto adresu pak potenciální vetřelec přiřadí svým komponentám.

U některých bezdrátových adaptérů se dá MAC adresa změnit softwarově nebo upgradem firmwaru. Pro hackery však existují jednodušší programy jako **Smac** (viz rámeček na této straně), které běží pod Windows a mění MAC adresu rozhraní bezdrátové sítě. WLAN adaptér přitom zůstává nezměněn, pakety však dostanou jiného odesílatele.

Ochranné opatření: Otestujte svoji bezdrátovou síť (viz rámeček na straně XX). Zabezpečte svoji síť pomocí jiného postupu (viz část "Bezpečnost").

11. Směrové antény: delší dosah

Každý prvek bezdrátové sítě má anténu. Většinou se jedná o všesměrový zářič, jehož signálové vlny se rozšiřují rovnoměrně kolem antény. Jinak to však vypadá u směrových antén. Ty totiž zvyšují dosah v určitém směru. Hackeři takové antény využívají k tomu, aby zjistili směr, v němž leží Access Point. Směrová anténa vás však může naopak před hackery chránit, pokud necháte vlny vysílat pouze určitým směrem.

Směrové antény můžete koupit kdekoliv, ale kutilové se základními znalostmi o technice antén si je mohou postavit i sami. Jako výchozí materiál poslouží plechovky. Velmi oblíbené jsou plechovky od Kosteleckých párků. Sadu k výrobě antény z tohoto domovního odpadu můžete dokonce koupit, například na *www.wifishop.cz*. Balení čipsů Pringles se hodí méně, i když i takové antény se objevují.

Bezpečnost

Vetřelci mohou číhat všude. Vy však rozhodujete o tom, zda vaše bezdrátová síť nežádané hosty pustí dovnitř nebo je vykáže ven. Na následujících řádcích se dozvíte, jak svůj WLAN zabezpečit.

12. Aktivujte šifrování

Pro bezdrátové sítě existuje několik způsobů šifrování: WEP, WPA, TKIP (dříve WPA2) a AES, přičemž WEP se překonává nejlehčeji a AES je v dnešní době stále ještě bezpečné.

Při šifrování zakóduje vysílač datové pakety, přijímač je zase odšifruje. Vysílač i přijímač tedy musejí používat stejnou techniku zabezpečení.

Vzhledem k tomu, že ne všechny komponenty WLAN zvládají AES, TKIP a WPA, zbývá často jen WEP, který znají všechny. Takže přinejmenším WEP byste měli v komunikačním programu Access Pointu a ve WLAN klientu aktivovat, a sice ve 128bitovém šifrování.

I když WEP pro hackery nepředstavuje žádnou větší překážku, alespoň vás uchrání před těmi, kteří se do vašeho vysílacího okruhu dostali bez zlých úmyslů. Navíc by to mělo zadržet vetřelce, kteří chtějí přes váš systém rychle surfovat na internetu. Na to si totiž raději rovnou najdou nechráněnou bezdrátovou síť.

13. Individuální název

SSID je jméno bezdrátové sítě, které potřebuje klient znát pro přihlášení. Výrobci většinou dodávají Access Pointy se standardním SSID. Názvy obvykle znějí "ANY", "Default", "WLAN" nebo nesou jméno výrobce, jako třeba "Netgear". Nezvaným hostům ztížíte přístup, pokud v konfiguračním programu svého Access Pointu použijete individuální jméno. To by totiž nemělo být tak snadné uhádnout.

14. Název sítě musí zůstat utajen

Nepříjemných vetřelců se zbavíte až v případě, kdy svému Access Pointu zakážete, aby nové jméno vysílal do éteru, kde ho mohou vidět všichni.

V konfiguračním menu vyhledejte možnost "uzavřená síť" a aktivujte ji. Pokud taková možnost chybí, podívejte se na položku většinou nazvanou "SSID Broadcast" a přepněte ji na "Disable". Nyní se mohou na Access Point přihlásit pouze klienti, kteří budou mít SSID zaneseno v softwarovém nastavení WLAN.

15. Využívejte MAC adresu klientu

Identifikace Media Access Control je hardwarová adresa síťových komponent. Je implementována do komponent a jednoznačně je identifikuje v síti. MAC adresa bývá zpravidla vytištěna přímo na síťovém adaptéru. Každý Access Point může jednotlivé klienty volat přímo jménem (MAC adresou). Proto zaneste MAC adresu každého klienta do komunikačního softwaru Access Pointu. Klienty, které Access Point nezná, nepustí dál.

Tuto kontrolu přístupu používejte v každém případě, i když není stoprocentní (viz tip 10). Minimálně počítače soukromých osob by měly být tímto opatřením chráněné. Kdo by totiž musel získávat MAC adresu oprávněného klienta, a tu pak pomocí cizího maskovaného klienta (ilegálně) podstrkávat Access Pointu, očekává, že systém obsahuje důležitá data. Nejčastější vetřelce by tak měl tento způsob ochrany odradit.

16. Omezte dosah bezdrátové sítě

Co se nedostane za plot vaší zahrady, zůstane čmuchalům skryto. Některé komponenty WLAN jsou dodávány s omezovačem dosahu. U některých přístrojů je v přenosovém softwaru záložka "Radio" a možnost "Redukce vysílacího výkonu". Zde pak určíte, o kolik decibelů má být signál ztlumen. Optimální hodnotu získáte testováním.

Pokud vysílací výkon nelze snížit softwarově, může pomoci změna pozice. Vyberte místo, které se nalézá co nejvíce uprostřed bytu a ne na jeho okraji, třeba u okna.

17. Vypínejte WLAN

Kdo nic neslyší, nemůže nic najít. I když není váš WLAN aktivní, vysílá Access Point pravidelné signály, aby se mohl klient připojit. Svoji bezdrátovou síť byste proto měli nechat mlčet, dokud nebude v akci.

Některé Access Pointy jsou vybaveny vypínači. Někdy se v menu WLAN softwaru nachází položka pro vypnutí. Další možnost představuje jednoduše vytažení kabelu Access Pointu ze zásuvky.

Přehled programů WLAN

Width1Width3Width1286Width3Width944Width3Width1618Width3Width2927Width3Width1280Width3Width1157ProduktCenaSystémInternetJazykStranaWidth1Width3Width1286Width3Width944Width3Width1618Width3Width2927Width3Width1280Width3Width1157

ChochopzdarmaLinuxwww.netstumbler.organglicky49Width1Width3Width1286Width3Width944Width3Width1618Width3Width2927Width3Width1280Width3Width1157

Ethereal 0.10.11zdarmaWin 95/98/ME, NT4, 2000, XPwww.ethereal.comanglicky49Width1Width3Width1286Width3Width944Width3Width1618Width3Width2927Width3Width1280Width3Width1157

Network Stumbler 0.4.0zdarmaWIN 2000, XPwww.netstumbler.organglicky49Width1Width3Width1286Width3Width944Width3Width1618Width3Width2927Width3Width1280Width3Width1157

Smac 1.2 1)15 dolarůWIN 2000, XP, 2003www.klcconsulting.net/smacanglicky49Width1Width3Width1286Width3Width944Width3Width1618Width3Width2927Width3Width1280Width3Width1157

Steganos Safe 8.030 euroWin 95/98/ME, NT4, 2000, XPwww.steganos.deněmecky49Width1Width3Width1286Width3Width944Width3Width1618Width3Width2927Width3Width1280Width3Width1157

Winpcap 3.1 Beta 4zdarmaWin 95/98/ME, NT4, 2000, XP, Server 2003www.winpcap.organglicky50Width1Width3Width1286Width3Width944Width3Width1618Width3Width2927Width3Width1280Width3Width1157

1) Demoverze ukazuje pouze aktivní adaptéry sítě a přiděluje pouze adresu "0C0C0C0C0C01".

Bezpečnostní nástroje: zničte hackery jejich vlastními zbraněmi

Většina programů, které vetřelci používají pro získávání přístupu do cizích počítačů, jsou původně bezpečnostní nástroje síťových administrátorů. Kdo je používá k tomuto účelu a pouze pro vlastní bezdrátovou síť, nedělá nic nezákonného. Buďte o krok před hackery a sami testujte, zda je vaše bezdrátová síť bezpečná. A to pomocí nástrojů, které používají samotní hackeři.

Network Stumbler

S freewarem v anglickém jazyce (na CD) můžete otestovat, jaké informace vaše bezdrátová síť vyzrazuje. Pak budete vědět, jaká bezpečnostní opatření provést (viz část "Bezpečnost", od strany XX)

Network Stumbler nejprve skenuje jednotlivé Wi-Fi kanály. Následně zobrazí nalezené bezdrátové sítě. Zpravidla by se mělo jednat o váš Access Point. Pro bezpečnost dat je v první řadě nejdůležitější položka "Filters, Encryption Off". Tady byste žádné komponenty vidět neměli. Pokud ano, musíte aktivovat jejich šifrování (viz tipy 2 a 12).

Pokud nástroj zjistí výrobce karty, měli byste přezkoušet identifikaci sítě (SSID, viz tipy 3 a 13). Neměl by se zde objevit ani SSID (viz tipy 4 a 14).

Ethereal

Freeware v anglickém jazyce zkoumá síť a hledá problémy tak, že ukládá přenos dat a analyzuje je. Když svoji síť otestujete, zjistíte, které informace by případní vetřelci mohli získat. Než Ethereal nainstalujete, musíte nejdříve nahrát ovladač Capture jako Winpcap (na CD, zdarma, anglicky).

V Etherealu pak pod "Capture, Interface" zvolíte pro záznam WLAN adaptér. V menu "Capture Filters" upřesníte výběrová kritéria datového proudu. Pomocí "Capture, Start" zaznamenáte datové pakety. Kliknutí na "Stop" pak zobrazí záznamy v trojdílném okně. Rady, jak program používat, najdete na *www.ethereal.com*.

Smac

Pomocí tohoto softwaru (cena plné verze činí 15 dolarů) můžete vyzkoušet, zda je vaše bezdrátová síť bezpečná i v případě, kdy do ní vpašujete WLAN komponentu s falešnou MAC adresou. Je-li Smac spuštěn, vidíte svůj WLAN klient a pod "Active MAC" jeho MAC adresu. Pod položkou "New Spoofed MAC Adress" mu můžete přiřadit novou MAC adresu. V našem případě zvolíme MAC adresu nějakého klienta, který má oprávnění k přístupu. Kliknutí na "Update MAC" převezme nastavení. Když chcete později adresu vrátit, aktivujte ji pomocí "Remove MAC". Dávejte pozor: po každé změně nastavení musí být komponenta deaktivována a zase aktivována, aby Windows změnu zaregistrovaly.

Legální nebo ilegální: Co (ne)smíte dělat

Využití cizí bezdrátové sítě může být jak zákonné, tak nezákonné. Záleží na tom, co vetřelec dělá.

PC WORLD: *Jedná se u otevřeně přístupných dat nějaké bezdrátové sítě o trestný hacking?*

Advokát: Trestný hacking ne, neboť ten předpokládá překonání zabezpečení. Může se zde ale jednat o trestné zásahy do dat. Trestná je každá změna dat bez svolení oprávněné osoby.

PC WORLD: *Mohu znalosti získané z otevřeně přístupné bezdrátové sítě předat třetí straně?*

Advokát: Osobní údaje nesmějí být ukládány nebo předávány dál. Ale i předání podnikatelských údajů může mít za následek nárok na náhradu škod.

PC WORLD: *Je povoleno dostat se na internet přes cizí, otevřenou bezdrátovou síť kvůli surfování. Nebo je to trestný čin?*

Advokát: Pokud je bezdrátová síť otevřená, nesplňuje využití neoprávněnou osobou skutkovou podstatu žádného trestného činu. Dochází k tomu v případě, kdy se provozovatel sítě technicky zajistil proti jejímu neoprávněnému užívání, například pokud vyžaduje zadání hesla. Kdo takovou zábranu překoná, dopouští se i při jinak legálním surfování trestného činu kvůli "získání neoprávněného plnění" a může počítat s odnětím svobody do výše jednoho roku. Navíc má provozovatel sítě nárok na odškodnění.

PC WORLD: *Co se z právního hlediska stane, když nějaký vetřelec ukládá přes moji otevřenou bezdrátovou síť dětskou pornografii bez mého vědomí na můj počítač?*

Advokát: Z pohledu trestního práva není provozovatel WLAN zodpovědný, dokud o těchto událostech neví. Když však orgány činné v trestním řízení začnou v těchto případech s vyšetřováním, dostane se do jejich zorného pole nejdříve zpravidla provozovatel WLANu jako vlastník IP adresy. Odsouzení pouze na základě zjištění IP adresy je ale nepravděpodobné. Vyšetřování se spíše rozšíří na neoprávněného uživatele WLAN. V praxi jsou tato vyšetřování v poslední době stále úspěšnější.

PC WORLD: *Mohu oklamat klienta WLAN cizí bezdrátové sítě tím, že mu podstrčím svoje WLAN PC jako Access Point?*

Advokát: Ne, i zde se jedná o nepovolenou záměnu cizích dat, protože k tomuto "podsunutí" musí být odpovídající data klienta změněna. Navíc zde připadá v úvahu i trestné získání neoprávněného plnění.