Bezdrátově a bezpečně snadno a rychle

Konfigurace vlastní bezdrátové sítě je otázkou zhruba deseti minut. Horší už je to s bezpečností. Řada uživatelů zabezpečení své sítě podceňuje nebo na něj zapomíná. To se však nemusí vyplatit. *Jiří Macich ml., jirka.macich@macich.net*

V domácnostech se nám množí technika, kterou rádi propojujeme. Kdo by dnes dobrovolně seděl za stolním počítačem, když si může vzít notebook do postele? Jenže kabely jsou nepohodlné a estetice příbytku rozhodně nepřidají. Naštěstí je tu dnes už technicky i cenově dostupná technologie Wi-Fi.

Proč dbát na bezpečnost bezdrátové sítě

Asi nejmenším rizikem je to, že za vaše peníze budou surfovat i nadšení sousedé, k nimž přesahuje pokrytí vaší otevřené sítě. Nemusí to však být jen sousedé, ale i náhodní kolemjdoucí. V zahraničí jsou již známí tzv. Wi-Fi turisté, kteří cestují po městě a hledají bezplatné připojení k internetu přes špatně zabezpečenou Wi-Fi síť. Pro někoho je to adrenalin, pro někoho vítaná úspora.

OCHRANA: Windows Firewall poskytne základní ochranu nejen před útoky z internetu, ale i z vaší domácí sítě.

Vyskytly se však už i případy, kdy přes nezabezpečenou síť docházelo k trestné činnosti, jako je šíření dětské pornografie nebo pirátských kopií počítačových programů (abyste se tedy nedivili, až vám jednoho krásného dne vtrhne do bytu zásahová jednotka). Existuje i možnost útoku na vaše data.

Možná se domníváte, že je to celé přitažené za vlasy, ale za klidný spánek nic nedáte. Základní zabezpečení proti nezvaným hostům není nijak komplikované a nepředstavuje žádné další náklady.

Dobře se zamaskujte a změňte tovární nastavení

Je nevhodné ponechávat síť zbytečně na očích. To platí i o venkovních anténách, které nebývají zrovna levné. Určitě byste nebyli rádi, kdyby vinou nějakého nenechavce skončila vaše anténa ve sběrných surovinách. My však máme tentokrát na mysli maskování samotné sítě, nikoliv jejích fyzických komponent.

Zvolte tedy takovou anténu a takový výkon, aby pokrytí nemělo zbytečně velký přesah na nepotřebné území. Z protějšího domu by se útočníkovi určitě lépe hackovalo než na vaší pohovce v obýváku.

Změňte SSID svého access pointu. Jde o označení, kterým se váš přístupový bod identifikuje. Doporučuje se, aby podle SSID nebylo možné odvodit totožnost konkrétního vlastníka sítě, abyste se vyhnuli eventuálnímu cílenému útoku. Zní to asi trochu paranoidně, ale za změnu nic nedáte, tak proč ji neprovést.

Ideální je zároveň skrýt svůj access point, aby se síť náhodným kolemjdoucím nezobrazovala v seznamu dostupných sítí, tedy pokud to není vzhledem k povaze vaší sítě nutné.

Šifrování komunikace: WEP už je jen na okrasu

Šifrování pomocí základní technologie WEP je stále ještě hodně rozšířené, ale je už vyloženě riskantní. Dokáže sice odradit hledače otevřených sítí, kteří nemají schopnosti či zájem prolamovat nějakou ochranu, ale sofistikovanějšímu útoku neodolá. WEP šifrování je velmi snadno překonatelné – pomocí některého z mnoha návodů kolujících po internetu to za pár minut zvládne i hacker amatér.

Podstatně lépe je na tom o několik let mladší WPA, či ještě novější WPA2 v kombinaci s PSK autentizací. Toto šifrování je pro většinu účelů více méně dostačující a jeho podpora je dosti široká. Pro domácí bezdrátové sítě je WPA2-PSK relativně ideální a u nových zařízení by s jeho podporou neměl nastat žádný problém. Pro větší firemní sítě se ovšem doporučuje WPA2 s autentizací 802.1x.

Sebelepší šifrování však není k ničemu, nepoužijete-li silné heslo – klíč, který je nutné zadat při připojení k chráněné síti. Vyplatí se opravdu dlouhý klíč, obsahující změť různých podporovaných znaků, velkých i malých písmen a čísel. Uvědomte si, že jméno vašeho psa není pro souseda chtivého internetu zase tak nepřekonatelným heslem. Trochu větší práce při nastavení sítě se později může vyplatit. Lze jen doporučit i občasnou změnu klíče.

Filtrování MAC adres: Nepovolaným vstup zakázán

Lepší routery umožňují filtrování MAC adres zařízení, která vpustí do sítě nebo kterým naopak přístup odříznou. Pokud nepotřebujete často do sítě připojovat nějaká „hostující zařízení“ (například notebook vaší návštěvy), vyplatí se seznam akceptovatelných MAC adres omezit jen na vaše zařízení. Jednoduše si – tedy pokud to váš síťový hardware podporuje – vytvoříte jakýsi whitelist.

Funkce opačná, na bázi blacklistu, nemá při prevenci takový význam. Je totiž nepravděpodobné, že byste znali MAC adresy zaří- →

NÁZEV SÍTĚ: Změnit SSID a schovat access point může být při výběru vhodného zařízení opravdu snadné.

ŠIFROVÁNÍ: Vyberte si tu správnou ochranu pro svou síť. Nezapomeňte ani na silný klíč.

→ zení všech sousedů a nenechavců ve vašem okolí. Blacklist se naopak hodí v okamžiku, kdy už byl nějaký problém s narušením sítě.

Filtrování MAC adres je možné použít i tehdy, když nechcete, aby z nějakého důvodu měla do sítě přístup i vaše konkrétní zařízení. Zahrnutím do blacklistu předejdete nechtěnému připojení ze strany jiných uživatelů.

Nejslabším článkem je člověk

Největší hrozba pro dnešní počítače se nachází mezi klávesnicí a židlí. Toto tvrzení je sice už otřepané, ale bohužel natolik pravdivé, že je opět musíme zdůraznit. Nejen čtenáři Chipu pak jistě vědí, že pro bezpečí bezdrátové sítě je nutné i klasické dodržování běžných pravidel, zejména při práci s internetem.

Když už budete u nastavování routeru a access pointu, rozhodně nezapomeňte změnit přihlašovací údaje do administračního rozhraní. Zní to sice možná až směšně, ale obrovské procento uživatelů to nedělá a na tovární nastavení můžete hodně rychle doplatit. Společnost Symantec před časem upozornila, že řada routerů používaných v domácích sítích je právě z tohoto důvodu v nebezpečí a spolu s nimi i celá síť. Případný útočník může skrze javascriptový kód umístěný na jakékoliv webové stránce snadno získat přístup k nastavení routeru a podle potřeby jej upravovat včetně vypnutí firewallu či zrušení šifrování.

SÍTĚ: Ve vašem okolí může být mnoho sítí. Ne do všech je však možné vstoupit. Jak je tomu v případě té vaší?

Dobře si také promyslete, jaké výsady dáte uživatelům vaší sítě. Opravdu musí všichni zaměstnanci znát přístupové heslo do administračního rozhraní vašeho routeru? Je nezbytné, aby vaše ratolesti měly ve Windows práva administrátorů a mohly tak pohodlně měnit nastavení? Takových rozhodnutí je více, a pokud včas zvolíte nějakou rozumnou „bezpečnostní politiku", můžete si ušetřit různé starosti. To samozřejmě platí obecně a nejde o specifikum bezdrátové sítě.

Bohužel jsou zde značně omezující možnosti správy práv uživatelů a pokročilé práce v síti v levných edicích Windows XP i Windows Vista pro domácí užití.

Vyberte si hardware a můžete začít

Jak tedy konkrétně zabezpečit malou domácí síť? Pokud ještě nemáte srdce své sítě, router kombinovaný s access pointem a případně i modemem, začněte výběrem správného typu. Zjistěte si, co všechno umí a zda podporuje zabezpečovací funkce, které hodláte ve své síti použít. Nejen z důvodu bezpečnosti se vyplatí sáhnout raději po osvědčené značce než po nějakém cenově lákavém low-endu.

Při první zkoušce své sítě nenasazujte rovnou ten nejtěžší kalibr. Raději si nejprve zkuste, zda všechna zařízení fungují tak, jak mají. Jestli se řádně připojí k internetu, mohou mezi sebou sdílet požadované soubory, mají správně přidělené IP adresy a podobně. Pokud je vše v pořádku, neváhejte s uzavřením sítě. Zvolte takový způsob šifrování, jaký bez obtíží podporují všechna zařízení v síti – ideálně dnes WPA2-PSK. Nastavte dostatečně silný klíč a zvažte naše další doporučení.

Samozřejmě ani poté nezapomínejte na všechny základní bezpečnostní poučky, kvalitní a pravidelně aktualizovaný antivir, instalování důležitých záplat a podobně. Je lepší být trochu paranoidní uživatel než uživatel, který přišel o data nebo o peníze.

Jiří Macich ml.

Jak nastavíte svůj router?

Administrace routerů různých značek a kategorií se bohužel liší. Nejlepší bude, když si k ruce vezmete manuál dodaný k routeru. My si pro ilustraci ukážeme, jak by nastavení probíhalo u routeru Asus WL600g, který je pro domácí sítě ideální volbou.

- Ve webovém prohlížeči si otevřete administrační rozhraní routeru – tzn. zadejte adresu např. **http://192.168.1.1** a přihlaste se. Klikněte na nabídku *Wireless* v levém sloupci. Pod odkazem Basic se skrývá nastavení SSID či volitelné skrytí access pointu. Pro uzavření doposud otevřené sítě nás však zajímá položka níže – Security.
- V okně Wireless – Security už můžete nastavit požadované zabezpečení. Z nabídky Network Authentication vyberte dostatečně kvalitní WPA-PSK/WPA2-PSK, které je pro domácí sítě dnes nejrozumnější volbou.
- O řádek níže zadejte klíč fungující jako heslo pro vstup do sítě (WPA Pre-Shared Key). Při zadávání vidíte jen hvězdičky – zadaný řetězec si můžete ověřit přes odkaz Click here to display. Ve vyskakovacím okně se klíč vypíše v nemaskované podobě.
- Nakonec zvolte ještě WPA Encryption. V případě tohoto routeru si můžete vybrat mezi TKIP, AES, nebo kombinací obojího.
- Uložte svá nastavení. Pokud se s libovolným počítačem nyní pokusíte připojit do sítě přes Wi-Fi, Windows vás požádají o zadání.

Má softwarový firewall ještě smysl?

Řada uživatelů si po zabezpečení samotné bezdrátové sítě a aktivování firewallu na routeru, který může fungovat i jako modem, klade otázku, zda je opravdu nutné mít zapnuté softwarové firewally na jednotlivých počítačích. Takže – má softwarový firewall ještě smysl?

Určitě. Už třeba jen proto, že lepší firewally dnes dávají uživateli mnohem lepší kontrolu nad aktivitami systému a nainstalovaných programů. Firewall v routeru s ADSL modemem běží více méně tiše a chrání jen před útoky z internetu. Nesleduje aktivity nainstalovaných programů.

Nebezpečí nemusí přijít jen z internetu, ale i z vnitřku sítě. Stačí si donést nějaký malware na USB flash disku. Už se objevil červ, který tento způsob šíření využíval, přičemž pro infikování počítače stačilo jen zasunout klíčenku do USB portu...

Hardwarový firewall nemusí být vždy nutně lepší než ten softwarový, ale to už záleží na konkrétním typu zařízení, a tak lze jen těžko dávat nějaké obecné rady do života.