Bezpečnost Wi-Fi v kostce

Nezabezpečená bezdrátová síť představuje velké riziko, protože se do ní může připojit prakticky kdokoliv, kdo má po ruce zařízení s podporou pro Wi-Fi. Signál bezdrátové sítě totiž obvykle přesahuje prostor, který je fyzicky pod vaší kontrolou (váš byt či dům).

V ČLÁNKU SE DOZVÍTE:
- o rizicích bezdrátových sítí
- o příkladech známých hrozeb
- jak se nejlépe chránit
- o jednotlivých technologiích
- tipy a triky pro zabezpečení bezdrátových sítí

V dosahu vaší Wi-Fi sítě může být hamižný soused šetřící za připojení k internetu, ale třeba i náhodný kolemjdoucí, který netuší, že jde o soukromou síť. Pokud je síť nezabezpečená, nic jim nebrání se připojit. A to může být problém. Cizí lidé v bezdrátové síti jsou totiž velkým rizikem. Například pokud je v rámci sítě nevhodně nastaveno sdílení dat, může nezvaný host snadno získat přístup například k dokumentům, fotografiím či videím. Dalším problémem jsou škody, které může tento nezvaný host napáchat na internetu de facto vaším jménem.

> „Jsou známy případy, kdy zločinci aktivně vyhledávali a zneužívali nezabezpečené bezdrátové sítě k šíření dětské pornografie.“

POLICEJNÍ VYŠETŘOVÁNÍ U VÁS DOMA

Stačí, aby nezvaný návštěvník sítě přes vaši internetovou přípojku zveřejnil na internetu nelegálně pořízenou kopii hudby nebo filmu, eventuálně se v příliš vzrušené diskusi dopustil pomluvy. Pokud se toto provinění dostane k rukám orgánů činných v trestním řízení, není pro ně problém dopátrat se konkrétní internetové přípojky, přes niž mělo dojít k porušení zákona. Logicky pak zabouchají na vaše dveře.

Už samo vysvětlování může být dost nepříjemné, natož kdyby se případ dostal před soud. Problém by byl o to větší, kdyby šlo o společensky závažnější trestnou činnost, jako je šíření dětské pornografie nebo třeba rozesílání výhružných e-mailů.

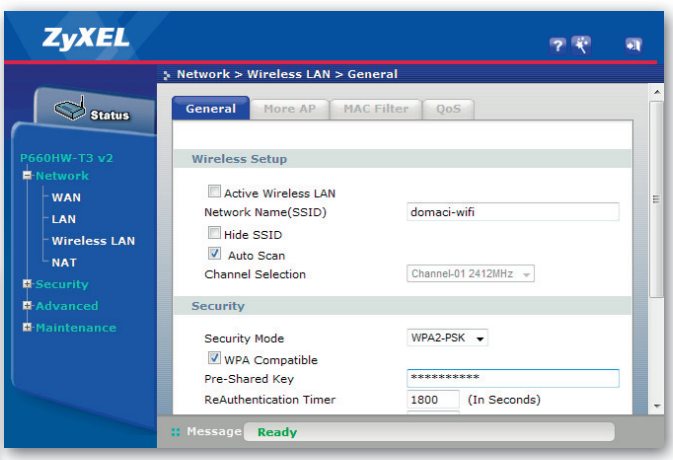
Ze zahraničí jsou známy případy, kdy opravdoví zločinci aktivně vyhledávali a zneužívali nezabezpečené bezdrátové sítě třeba právě pro šíření dětské pornografie. Spoléhali se na to, že stopa vyšetřovatelů končí u člověka s nezabezpečenou bezdrátovou sítí. Zkazit pár týdnů života ale dokáže i poněkud zvrácený vtipálek, který přes vaši bezdrátovou síť rozešle výhružné e-maily o uložených bombách.

GOOGLE A JEHO NAFOUKLÁ KAUZA

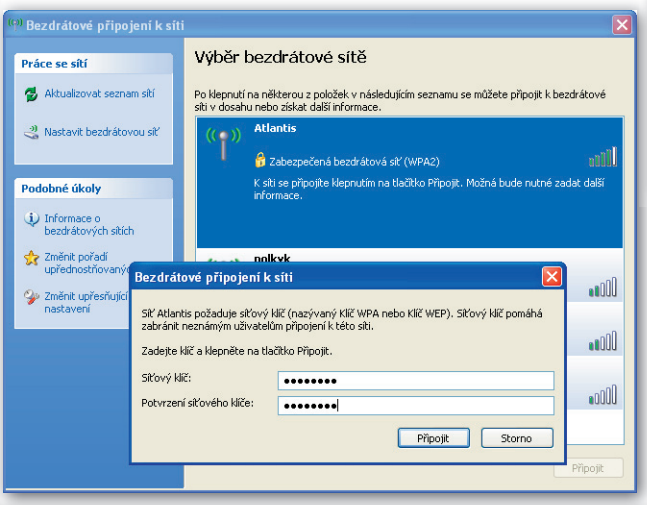
Dalším rizikem je možný únik dat, která v nechráněné formě „polétávají vzduchem“. Bohužel to není jen teorie. Bezpečnostní nahotu řady bezdrátových sítí ukázala kauza, kdy společnost Google během pořizování fotografií pro své internetové mapy nechala katalogizovat bezdrátové sítě. Bezdrátové sítě totiž mohou sloužit pro určení polohy.

Na tom není nic špatného, ale Google ukládal i data, která zrovna byla bezdrátově přenášena. Společnost to přiznala letos po nátlaku německých úřadů a má s tím problémy i v dalších zemích. Google se přitom hájí, že nešlo o úmysl, ale o omyl.

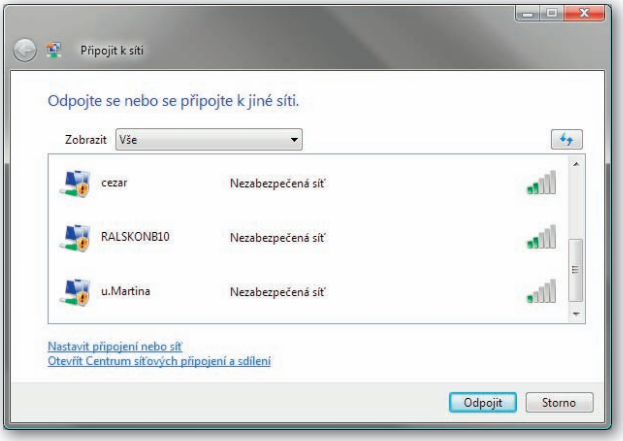
Většina nashromážděných dat by měla být v praxi nepoužitelná, protože za plynulé jízdy automobilem (jímž Google pořizuje snímky) nelze toto odposlouchávání bezdrátových sítí provozovat efektivně. Navíc kritická část internetové komunikace, například



Ideální je zabezpečení bezdrátové sítě na bázi technologie WPA2.



O zabezpečení bezdrátové sítě není třeba se příliš starat – pouze v rozhraní přístupového bodu nastavíte heslo, které pak zadáte na počítači při prvním připojení do bezdrátové sítě.



Nezabezpečených sítí najdete všude dost. Jejich majitelé tím dost riskují.

práce s internetovým bankovnictvím, je už automaticky šifrována, aniž by o tom méně technicky zdatní uživatelé vůbec věděli. Nicméně celý případ je učebnicovou ukázkou rizik bezdrátových sítí.

ŠIFROVAT, ŠIFROVAT, ŠIFROVAT

Nejefektivnější ochranou bezdrátové sítě je šifrování veškeré komunikace, která sítí prochází. Není to tak těžké, jak by se mohlo zdát. Vlastně stačí jednou vhodně nastavit svůj bezdrátový router (přístupový bod), a máte vystaráno. Nikdo nezvaný se do sítě nedostane (přístup je chráněn heslem) a data proudící vzduchem nelze odposlouchávat tak, aby dávala smysl.

Routery s podporou pro Wi-Fi obvykle podporují všechny běžně používané šifrovací technologie: od těch nejprimitivnějších až po ty sofistikovanější. Bohužel, koncová zařízení, která se do sítě budou bezdrátově připojovat, nemusí vždy podporovat to nejlepší šifrování, takže do příliš zabezpečené sítě se pak zdárně nepřipojí. Je tedy třeba zvolit co nejlepší šifrování z těch, která jsou podporována všemi zařízeními v síti.

Za nejlepší dostupné šifrování pro konvenční použití se dnes považuje WPA2 v kombinaci s AES nebo s TKIP. Pokud se všechna vaše zařízení při volbě tohoto šifrování v nastavení routeru dokážou zdárně připojit do sítě, máte vyhráno. Některá zařízení si však s WPA2 nemusí rozumět, takže zde přichází na řadu starší způsob WPA.

V kombinaci s AES je i technologie WPA považována za velmi bezpečnou. O stupínek níže je WPA v kombinaci s TKIP, ale k zabezpečení domácích bezdrátových sítí stačí, pokud nelze nasadit silnější ochranu. Naprosto nevhodné je naopak zastaralé šifrování WEP. S volně dostupnými nástroji si dokáže s tímto šifrováním poradit i kdejaký kutil v oblasti bezdrátových sítí, takže člověka se zlým úmyslem technologie WEP neodradí.

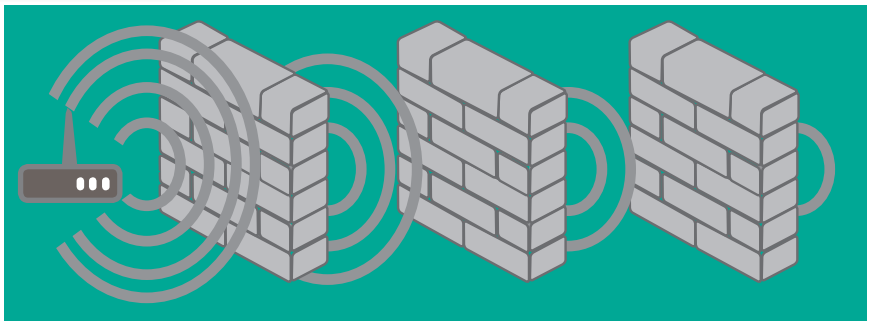
Sebelepší šifrování ale není k ničemu, když heslo (klíč) pro přístup k síti není těžké uhodnout. Heslo by mělo mít alespoň osm znaků a mezi nimi by měla být zastoupena přinejmenším velká a malá písmena a číslice. Ideálně by mělo jít o náhodně vybrané znaky. Neškodí jednou za čas heslo změnit. Zejména pokud jej prozrazujete například návštěvám.

DALŠÍ ZPŮSOBY OCHRANY SÍTĚ WI-FI

K ještě vyšší bezpečnosti lze učinit několik dalších kroků. V domácnosti by měla být jen jedna osoba, která zná heslo pro přístup do administrace routeru (rozhodně nedoporučujeme používat heslo přednastavené výrobcem) a stará se o jeho správu. Tím se eliminuje faktor zvídavého, ale méně technicky zdatného člena rodiny, který neodbornou manipulací může snížit zabezpečení sítě nebo napáchat i další škody na její funkčnosti.

Dále byste měli omezit riziko násilného připojení k bezdrátové síti, uskutečněného ať už překonáním šifrování (WEP), nebo uhodnutím hesla. Ideální je, když bezdrátový router umožňuje provozovat skrytou síť. Ta se pak nebude sousedům či kolemjdoucím zobrazovat jako dostupná síť v okolí. Nebude tedy běžně viditelná (i šifrované sítě jsou viditelné, byť do nich bez hesla nelze vstoupit).

Přestože signál bezdrátové sítě průchodem každou zdí rapidně slábne, v prostorách svého domu/bytu jej neudržíte.



Pokud síť už nemůže být skrytá, měla by se volbou vhodného SSID alespoň schovat pod pomyslným pláštěm anonymity. U bezdrátové sítě, resp. u jejího přístupového bodu si totiž nastavujete jméno, podle kterého je síť identifikovatelná. U soukromých sítí je ale chyba, pokud SSID prozrazuje či naznačuje, kdo je provozovatelem (majitelem). Do soukromých sítí SSID tedy nepatří například číslo domu, či dokonce jméno provozovatele. Lze se tak vyhnout adresným útokům směřujícím vůči vaší osobě.

Vedle schovávání a maskování sítě je také vhodné zamyslet se nad jejím přesahem mimo prostor, který je pod vaší kontrolou. Opravdu musí síť kromě vašeho bytu pokrývat i okolní byty nebo jejich části? Bezdrátové routery mají obvykle anténu všesměrovou, takže signál se šíří všemi směry rovnoměrně. Pokud takový router umístíte ke zdi oddělující dva byty, logicky se signál může ve velmi vysoké kvalitě zatoulat i k sousedovi (pokud tomu nebrání stavební materiál). Router se všesměrovou anténou by tak měl být optimálně umístěn uprostřed prostoru, který má být účelně pokryt.

Jiří Macich ml., jiri@macich.net

O tom, jak je zabezpečení bezdrátových sítí důležité, vědí své i výrobci odpovídajících zařízení. Nejedno má speciální kontrolku, signalizující, zda je síť řádně zabezpečena.