E-Bezpečí 2019, 4(2): Page 46-50. Univerzita Palackého v Olomouci. ISSN 2571-1679.
Online: https://www.e-bezpeci.cz/index.php?view=article&id=1651

JAK ZABEZPEČIT DOMÁCÍ POČÍTAČOVOU SÍŤ

Kamil KOPECKÝ

Internet je velmi užitečným nástrojem, který svým uživatelům nabízí nepřeberné množství možností, je to prostor pro komunikaci, vzdělávání a také zábavu, je také v současnosti primárním zdrojem informací všeho druhu. Bohužel je také prostředím, ve kterém může být náš počítač, tablet či mobilní telefon vystaven velkému množství hrozeb, proto je třeba zajistit bezpečnost jak jednotlivých zařízení, která internet využívají, tak i samotné počítačové sítě, která je k internetu připojena.

Domácí síť je složena z několika vzájemně propojených zařízení (počítačů, tiskáren apod.), která jsou připojena různými způsoby k tzv. **routeru**. Router je zařízení, které má celou řadu funkcí. Na prvním místě poskytuje domácnosti/škole přístup k internetové síti, je základním vstupním a výstupním bodem do/ze světa internetu. Router v zásadě propojuje dvě sítě – tzv. WAN síť (wide area network, rozlehlá síť, která pokrývá rozlehlé geografické území, např. síť poskytovatele internetového připojení připojená k internetu) a LAN síť (lokální, místní síť, tj. naše domácí síť). Mezi těmito dvěma sítěmi pak router usměrňuje (routuje) tok informací (tzv. datový tok).

Nejjednodušším způsobem, jak lze router připojit k internetu, je připojení pomocí běžné digitální telefonní linky. K tomu potřebujeme router, který je zároveň zkombinován s DSL/ADSL/VDSL modemem. Ten umí využít pro připojení k internetu digitální telefonní linku (jejíž kapacita trvale roste) a je tedy využíván především v domácnostech či menších školách.

Router je velmi důležité síťové zařízení a z hlediska bezpečnosti domácnosti, školy či jiné instituce je velmi důležité jeho zabezpečení. Přes nezabezpečený router může útočník proniknout do naší domácí sítě, napadat naše počítače, získat přístup k IP kameře či dalším zařízením, které jsou do domácí sítě připojeny, získávat potenciálně zneužitelná data atd.

Router však není pouze přístupový bod do světa internetu, umožňuje toho podstatně více - např. vytvořit lokální síť (LAN), ale také lokální bezdrátovou sít (lokální „wifinu“, tzv. WLAN), poskytuje nám přístup k online televizi (IPTV), router nám umožňuje připojit do sítě různé druhy datových úložišť (NAS), která nám umožňují např. streamovat video a hudbu, ale také zálohovat, synchronizovat a sdílet naše privátní soubory apod.

Obrázek 1: Mapa jednoduché sítě připojené k internetu

Jak zabezpečit router?

Každému routeru je po spuštění a připojení do počítačové sítě přidělena unikátní adresa – tzv. IP adresa, která je složena ze 4 čísel oddělených tečkou (tzv. IP4). Router má nejčastěji IP adresu 10.0.0.138 nebo 192.168.0.1 (výrobce vždy výchozí adresu routeru uvádí v manuálu k obsluze). Pokud se k routeru připojí další zařízení (počítač, mobilní telefon, domácí asistent, externí datové úložiště apod.), automaticky od routeru obdrží vlastní IP adresu (pomocí tzv. DHCP, dynamic host configuration protocol), pod kterou je v rámci lokální sítě identifikovatelné. Router tak neustále sleduje veškerá zařízení, která jsou k němu připojena.

Pokud chceme mít router dostatečně zabezpečen, je nutné zajistit následující:

1. Změnit výchozí heslo k administraci routeru

Každý router má nastaveno výchozí heslo pro vstup do jeho administrativní části. Zpravidla jde o spojení přihlašovacího jména

a hesla admin/admin nebo root/root apod. Při prvním přihlášení k routeru doporučujeme výchozí heslo změnit. K routeru se přihlásíme zadáním IP adresy routeru do běžného webového prohlížeče (10.0.0.138 nebo 192.168.0.1) – podobně, jako když otevíráme běžnou internetovou stránku.

2. Pravidelně aktualizovat operační systém routeru, tzv. firmware

Stejně jako u operačního systému běžného desktopového počítače je velmi důležité udržovat software routeru stále aktuální. Proto je důležité pravidelně software routeru – tzv. firmware – aktualizovat. Většina routerů má tuto funkci dostupnou v rámci administrativního prostředí.

3. Veškeré bezdrátové sítě vytvořené routerem opatřit heslem

Jak již bylo řečeno, většina routerů umožňuje vytvářet vlastní lokální bezdrátové sítě, tzv. WLAN. Bezdrátovou síť nastavíme přímo v administrativním prostředí routeru – na jedné straně vybereme vhodný název sítě (tzv. SSID) a poté volíme, jak bude přístup k síti zabezpečen (např. heslem). Beztrátovou síť vždy opatřeme vstupním heslem pod zabezpečením WPA2-PSK. Starší typy zabezpečení (WEP apod.) jsou považovány za zastaralé a prolomené.

Moderní routery zpravidla umožňují uživatelům vytvářet bezdrátové domácí sítě operující ve dvou frekvenčních pásmech - 2,4 GHz a 5 GHz, u obou je nutné nastavit zabezpečení na WPA2-PSK.

4. Filtrovat připojení nežádoucích zařízení do naší sítě

Jak jsme si již vysvětlili v předchozí části, router sleduje, která zařízení jsou k němu připojena. Zařízení router identifikuje podle IP adresy, kterou mu router přidělil, ale také podle tzv. MAC adresy

(ta je na IP adrese nezávislá). MAC adresa je tzv. fyzická adresa, která je přiřazována síťové kartě daného zařízení, třeba notebooku, tabletu či běžného PC. Skládá se z šesti dvojciferných hexadecimálních čísel oddělených pomlčkami či dvojtečkami. Přestože byla MAC adresa původně navržena jako neměnná, u moderních síťových karet je možné ji změnit (virtuálně).

5. Filtrovat nežádoucí obsah prostřednictvím systémů rodičovské kontroly

Moderní routery umožňují nastavit, jaký obsah bude možné (či nemožné) z konkrétního počítače (či celé LAN) zobrazovat. Router totiž umožňuje filtrovat přístup k obsahu právě z konkrétní MAC adresy – nezávisle na IP adrese, kterou dostal daný počítač přidělenu. To platí pro veškerá zařízení – mobilní telefony či tablety, které využívají router pro přístup k internetové síti. Některé routery také umožňují regulovat čas, ve kterém mohou daná zařízení přistupovat na internet.

6. Mít aktivní firewall routeru

Firewall si můžeme jednoduše představit jako „stráž vstupu do hradu“, která rozhoduje o tom, koho/co pustí dovnitř a co ven. Úkolem firewallu je bránit místní síť před různými druhy útoků, firewall totiž filtruje příchozí a odchozí data.

Firewall umožňuje filtrovat obsah, ke kterému se na internetu dostaneme, a to pomocí zákazu konkrétních internetových adres či jejich částí (URL). Pomocí firewallu tak lze např. blokovat všechny stránky, které obsahují slovo *porn*, *facebook* apod. Firewall také umí filtrovat konkrétní síťové služby (třeba stahování a odesílání pošty, otevírání www stránek apod.) – a to pomocí blokování konkrétních portů, na kterých služby běží (port je vlastně číslo od 0 do 65535, které označuje konkrétní službu, kterou počítač používá, např. port 80 je port pro http služby, tj. otevírání webových stránek). Pomocí zákazu portů lze také např. blokovat používání konkrétních komunikačních nástrojů, třeba messengerů (Skype).

Obrázek 2: Router v domácí síti

Pro E-Bezpečí,
Kamil Kopecký