# I používání wi-fi chce obezřetnost

V říjnu loňského roku proběhla technologickým světem nepříjemná zpráva. Stávající ochrana bezdrátového připojení wi-fi pomocí šifrování WPA2 je zranitelná a problémem trpí prakticky všechny bezdrátové sítě současnosti. Přitom na otevřené nebo heslem chráněné wi-fi připojení třeba v kavárnách spoléhá řada lidí.

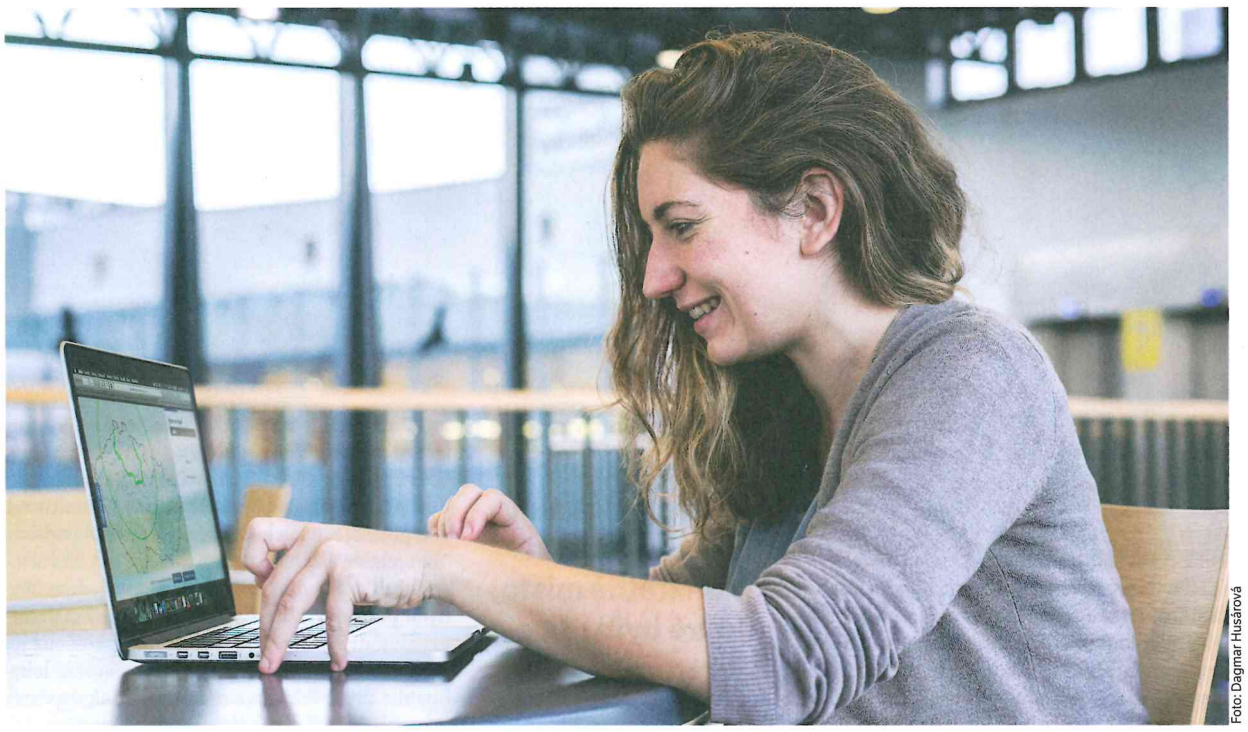

Foto: Dagmar Husárová

„Zranitelnost znamenala, že za určitých okolností bylo možné odhadnout šifrovací klíče, s nimiž útočník mohl číst nebo zasáhnout do komunikace," přiblížil Petr Velan z univerzitního bezpečnostního týmu CSIRT-MU. Jako náhradu za nevyhovující šifrování WPA2 už odborníci oznámili vznik pokročilejšího WPA3. Neznamená to ale, že problémy zmizely.

Běžný uživatel by měl vědět, že pro zařízení, která používala staré šifrování, jejich výrobci většinou vydali aktualizace. „V IT komunitě to funguje tak, že producenti o problému věděli už ve chvíli, kdy se informace o něm dostala do světa, a byli nachystaní jej řešit. Otázka ale samozřejmě je, jestli si koncoví majitelé zařízení aktualizace nainstalovali. A problematická jsou také zařízení s mobilním operačním systémem Android, protože na jeho starší verze se aktualizace často ani nedělají," doplnil Marek Saitl, systémový analytik Ústavu výpočetní techniky MU. Důvodem je podle něj to, že verzí Androidu je dnes už tolik, že je pro výrobce ekonomicky nevýhodné a skoro i nemožné, aby je udržovali v patřičné formě všechny.

Pro uživatele wi-fi připojení, které je v cizích rukou, to znamená to, že by k nim měl přistupovat s rozumnou mírou podezřívavosti a nevstupovat přes internet například v kavárnách do systémů, u nichž by ho mrzelo, kdyby se do nich dostal ještě někdo cizí. Útok je potenciálně možný, i když málo pravděpodobný. „Vyžadovalo by to, aby byl uživatel i útočník napojený na té samé síti a ve fyzické blízkosti a pak samozřejmě docela rozsáhlé technické znalosti," podotknul Velan.

Když už člověk veřejné wi-fi sítě využívá, liší se přístup do nich zpravidla tím, jestli je, nebo není nutné zadávat heslo. Z hlediska bezpečnosti jde o docela důležitý rozdíl. „V otevřené síti se heslo nezadává a komunikace je tím pádem nešifrovaná, kdokoliv v dosahu sítě ji může odposlouchávat," přiblížil Saitl.

Šifrovaná dnes stále ještě většinou znamená zabezpečená systémem WPA2. Pokud je zařízení aktualizované, lze připojení považovat za bezpečné. Pokud tedy člověk věří jeho majiteli a nemá důvod ho podezřívat z nekalých úmyslů.

**Pokud se chcete na wi-fi třeba v kavárně cítit bezpečněji, připojte se přes univerzitní VPN, která je šifrovaná.**

Pro studenty nebo zaměstnance Masarykovy univerzity je po všech stránkách výhodnější používat síť s označením Eduroam. Pokud člověk obětuje pár minut a nainstaluje si ji podle návodu na it.muni.cz/sluzby/wifi bude mít k dispozici připojení k internetu na všech fakultách a díky tomu, že tutéž síť používají i jiné univerzity, tak i ve velké části Brna a dalších městech, a to také v zahraničí.

„Odborníci z té konkrétní univerzity síť opravdu hlídají, to je její velká výhoda," zdůraznil Saitl. A Velan doplnil ještě další drobnost, která se může hodit při používání méně důvěryhodné sítě: „Univerzita poskytuje uživatelům také virtuální privátní síť, zkráceně VPN, ke které se dá na dálku připojit třeba i z oné kavárny. Je šifrovaná, takže i kdyby se komunikaci snažil někdo číst, dovede ho to jen na univerzitu, ale už ne ke konkrétním informacím."

Oba odborníci se shodují na potřebě být obezřetný, ale také na tom, že kdyby chtěl mít člověk pocit absolutního bezpečí při práci s počítačem, dovedlo by ho to možná až k paranoie. Také oni ale upozorňují na neustále se opakující a zbytečné problémy.

Řada uživatelů pořád podléhá phishingu a svěřuje svoje citlivé údaje na základě nedůvěryhodných zpráv nebo e-mailů, chodí na nedůvěryhodné weby a také stahuje hlavně do mobilních telefonů aplikace, které nadělají víc škody než užitku.

„Hlavně systém Google Play je známý svojí otevřeností, je jednoduché do něj aplikaci jako vývojář dostat. Útočníci toho ale zneužívají a vkládají tam také aplikace, které nejsou důvěryhodné. Proto by lidé neměli skočit na kdejakou hru s pěknou grafikou," zdůraznil Saitl, který radí orientovat se podle kvality a množství hodnocení dané aplikace.

Martina Fojtů

## Užitečné pojmy

### Bot (Robot)
Programy, které ovládnou počítače v síti a používají je k provádění zločinných aktivit – například distribuovaným útokům (DDoS) a hromadné distribuci nevyžádané komerční pošty. Individuální boty jsou základem velkých skupin robotů známých jako botnety. Počítač zcela nebo částečně ovládaný botem je známý jako „zombie".

### Crack
Neoprávněné narušení zabezpečení ochrany programu nebo systému či jeho integrity. Někdy se používá také slovo hack, což je ale i označení podařeného, neobvyklého, nápaditého či rychlého vyřešení programátorského či administrátorského problému.

### Červ (Worm)
Autonomní program schopný vytvářet své kopie, které rozesílá do dalších počítačových systémů, kde vyvíjí další činnost, pro kterou byl naprogramován. Často slouží ke hledání bezpečnostních skulin.

### Firewall
Ucelený soubor bezpečnostních opatření, která mají zabránit neoprávněnému elektronickému přístupu k počítači či konkrétním službám v síti. Také systém zařízení nebo soubor zařízení, který lze nakonfigurovat tak, aby povoloval, zakazoval, šifroval, dešifroval nebo vystupoval v roli prostředníka pro všechny počítačové komunikace mezi různými bezpečnostními doménami, založený na souboru pravidel a dalších kritérií.

### Pharming
Podvodná metoda používaná na internetu k získávání citlivých údajů od obětí útoku. Principem je přesměrování klienta na falešné stránky internetbankingu, e-mailu nebo sociální sítě po zadání webové adresy do prohlížeče. Tyto stránky jsou obvykle k nerozeznání od skutečných stránek např. banky a ani zkušení uživatelé nemusejí poznat tuto záměnu (na rozdíl od příbuzné techniky phishingu).

### Phishing
Podvodná metoda usilující o zcizování digitální identity uživatele, jeho přihlašovacích jmen, hesel, čísel bankovních karet nebo účtu za účelem jejich následného zneužití. Jde o vytvoření podvodné zprávy, šířené většinou elektronickou poštou, jež se snaží zmíněné údaje z uživatele vylákat. Zprávy mohou být maskovány tak, aby co nejvíce imitovaly důvěryhodného odesílatele. Může jít například o padělaný dotaz banky, jejíchž služeb uživatel využívá, se žádostí o zaslání čísla účtu a PIN pro kontrolu.

### Ransomware
Program, který zašifruje data a nabízí jejich rozšifrování po zaplacení výkupného.

### Spyware
Program skrytě monitorující chování oprávněného uživatele počítače nebo systému. Svá zjištění tyto programy průběžně (např. při každém spuštění) zasílají subjektu, který program vytvořil, respektive distribuoval. Takové programy jsou často na cílový počítač nainstalovány spolu s jiným programem (např. počítačová hra), s jehož funkcí však nesouvisí.

*Zdroj: Výkladový slovník Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB)*