Router jako šedé místo v zabezpečení

Směrovač v domácnosti je, co se osvěty a prevence v oblasti bezpečnosti týče, stále podceňovaným prvkem. Co všechno vám správné nastavení může přinést a co naopak špatného způsobit?

ZUZANA DURAČINSKÁ

Co se týče routerů, uživatelé se příliš neupozorňují na to, že správné nastavení tohoto zařízení, které je v řadě případů branou do internetu, může mít zásadní vliv na jejich on-line bezpečnost.

Poté, co si router koupí a zapojí ho, často se nedopracují k tomu, aby defaultní nastavení změnili, a tím eliminovali rizika, která tato základní konfigurace může způsobit.

Na domácí routery se kladou stále větší nároky jak z pohledu výkonnosti v důsledku narůstajícího počtu zařízení připojených do internetu v domácnosti, tak z hlediska bezpečnosti. Počet útoků vedených přes routery přitom neustále roste.

Ze světa i z České republiky jsou známé řady případů, kdy zotročené domácí routery posloužily například k DDoS útokům. V tomto textu se zaměříme na nejčastější nedostatky a důvody napadení domácích routerů.

1 Firmware

Specializovaný firmware pro routery obsahuje chyby stejně jako programy, které každodenně používáme, a proto taktéž vyžaduje pravidelné záplatování. Tento zdánlivě jednoduchý krok však může představovat hned několik problémů.

Jedním z nich je někdy poměrně náročné hledání poslední verze firmwaru pro konkrétní typ routeru, jenž uživatel používá. Když se uživateli podaří najít přesně ten, který hledal, musí ho ještě do routeru nainstalovat, což zase nemusí být u všech modelů úplně jednoduché a intuitivní.

Pokud to jde, je dobré, když si uživatel může nastavit automatické nebo alespoň poloautomatické upozorňování na updaty sám, aby mu žádný bezpečnostní update neunikl. Na update by se nemělo zapomínat ani v případě koupě nového routeru, protože mezi nahráním firmwaru do routeru při výrobě a spuštěním routeru v domácnosti může uplynout poměrně dlouhá doba.

Zde je důležité připomenout, že i když vám router poskytl váš provider (ať už ve formě pronájmu nebo koupě), zodpovědnost za aktualizace firmwaru nesete sami. Když se bavíme o firmwaru, může nastat i jedna nezáviděníhodná situace – tedy ta, že výrobce routeru podporu pro daný firmware ukončil.

I s tím mají nejen uživatelé v České republice své neblahé zkušenosti. Proto by se měli mít uživatelé na pozoru a již při koupi nového routeru by si měli ověřit, zda výrobce vydává pro firmware pravidelné updaty.

2 Universal plug and play

UPnP je protokol, který programům umožňuje mimo jiné jednoduše měnit nastavení routeru, konkrétně otevřených portů, které programy potřebují pro svou komunikaci. Protokol byl primárně vytvořen pro použití v lokálních sítích, a tak neobsahuje jeden z důležitých bezpečnostních prvků, jímž je autentizace.

Mnoho routerů má však dostupnost UPnP nastavenou nejen z lokální sítě, ale také z celého internetu. Bezpečnostní riziko je samozřejmě větší, když je protokol UPnP dostupný z internetu, což umožňuje útočníkům přistoupit ke konfiguraci portů, a zneužít je tak například pro získání přístupu do lokální sítě nebo jako proxy pro surfování.

Implementace protokolu UPnP v routerech je také často děravá, a proto se doporučuje protokol raději vypnout a přesměrování služeb na porty udělat ručně.

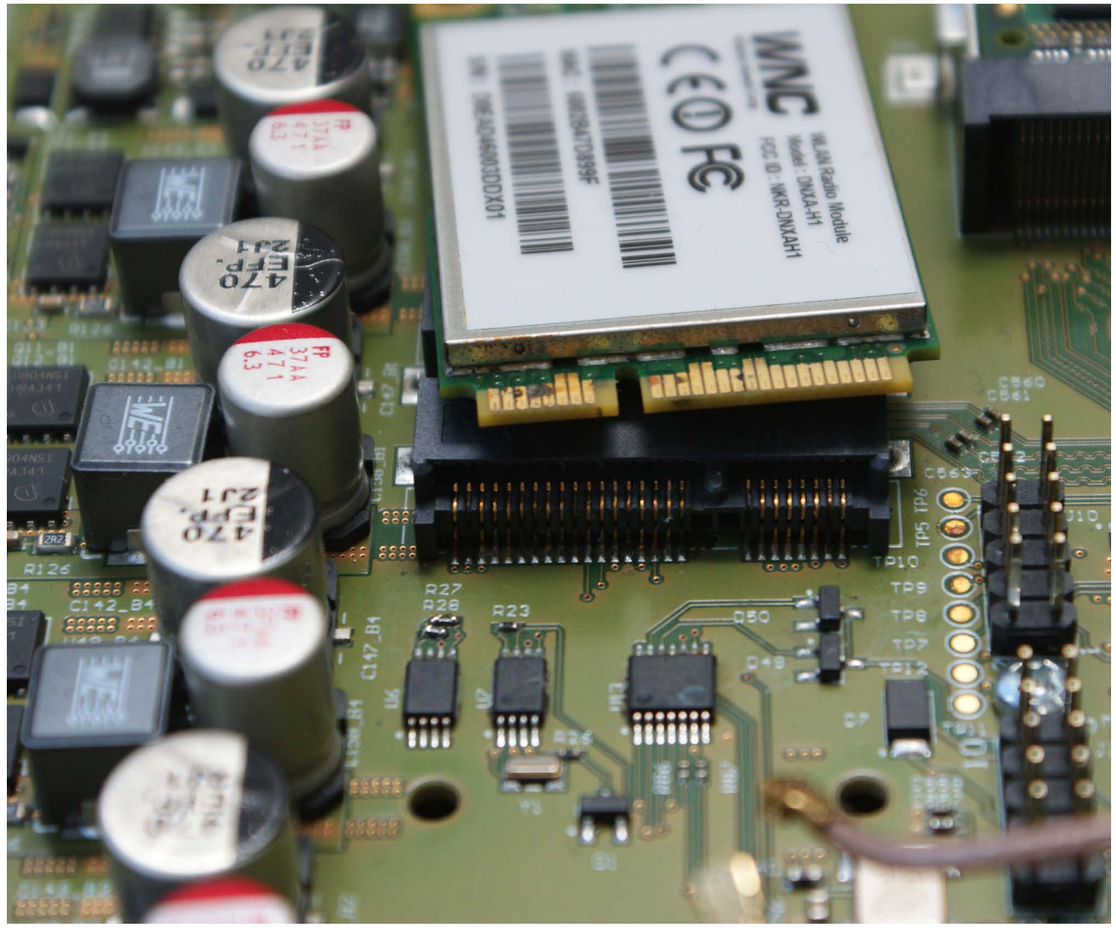
Další bezpečnostní riziko spočívá v defaultně zapnutém protokolu již z výroby. Běžný uživatel si totiž zapnutého nebo vypnutého UpnP protokolu nemusí vůbec všimnout, a proto jeho defaultní zapnutí v domácích routerech představuje určité riziko, které by výrobci routeru mohli velmi jednoduše eliminovat, a předejít tak zbytečným problémům.

3 Přístupnost administrace routeru z internetu

Dostupnost rozhraní umožňujícího nastavení routeru z prostředí internetu představuje zásadní riziko. Tzv. vzdálený přístup (remote access) slouží k administraci nastavení routeru, pokud se uživatel nachází mimo lokální síť.

Podíl domácností, které by tento doplněk využilo, bude však velmi malé. Problém pak opět nastává v routerech, jež nabízejí vzdálenou administraci routeru již v defaultním nastavení.

V tom případě musí uživatel v nastavení routeru tuto funkcionalitu vypnout. Podobně jako defaultně zapnutý UPnP protokol nebo děravý firmware také tento nežádoucí doplněk uživatele v práci s internetem nijak neomezuje, a proto jej obvykle nic nenutí tuto vzdálenou administraci znemožnit, což může být v kombinaci s defaultním nastavením přihlašování do administrace routeru kritickým problémem pro bezpečnost sítě.



Pro minimalizaci rizika je možné omezit také přístup do administrace z lokální sítě jenom pro jedno zařízení, protože útočník může bezpečnost routeru ohrozit i pomocí skriptu nahraného v rámci stránek, které si uživatel připojený přes daný router prohlíží.

4 Podcenění prvotního nastavení

Router má po zakoupení do domácnosti první šanci na správné nastavení při prvním spuštění. Pokud však vše funguje tak, jak má (bez ohledu na bezpečnostní díry), často se stane, že jeho první šance je zároveň tou poslední.

Problém velké většiny modelů spočívá již v úvodním průvodci nastavením, který uživatele nenavede nebo nepřinutí ke změně nebo zvolení vlastních přístupových údajů k administraci routeru.

Pokud se v průvodci nastavení routeru toto nevyžaduje, z uživatelského hlediska není třeba nic měnit. Defaultní kombinace jména a hesla k administraci routerů jsou ale na internetu velmi lehce dohledatelné pro každý model routeru od jakéhokoliv výrobce. A pokud se tam náhodou nějaký model od výrobce nenachází, stačí zkusit použít přístupové údaje jiných modelů, protože ty se u stejného výrobce často opakují. Obejít by to bylo možné například tak, že by si uživatel při prvotní instalaci musel zvolit své heslo pro administraci sám.

U výrobců routerů by také bylo žádoucí, kdyby již při prvním spuštění routeru průvodce vyžadoval zvolení IP adresy jejího administrátorského rozhraní. Nahrazení nejčastěji používané adresy 192.168. 1. 1 nebo 192.168. 0. 1 může uživatele před částí útoků ochránit. Jde hlavně o CSRF (Cross Site Request Forgery), který se jako zranitelnost nachází v řadě routerů. Cílem útoku je pak nejčastěji změna nastavení DNS záznamu.

Snaha o osvětu

Trh v oblasti routerů je poměrně velký a zásadním způsobem do něj vstupují také poskytovatelé připojení, kteří jsou jejich velkými odběrateli a dodavateli zároveň. Běžného uživatele pak při výběru domácího routeru zajímají většinou jenom dvě věci: cena a funkčnost připojení. Nic z výše uvedených funkcí není pak natolik uživatelsky zajímavé, aby přimělo běžného uživatele ke studiu funkcí UPnP protokolu nebo vzdálené administrace.

Bez pochopení základního fungování internetu a jeho protokolů si tak ale nemůže uvědomit ani reálné riziko chybného nastavení svého routeru. Proto by měli výrobci routerů a poskytovatelé připojení pochopit důležitost defaultních nastavení a funkcionalit, které routery využívají.

Právě úvodní průvodce nastavení routeru může být zásadní pro jeho další správné a bezpečné fungování v domácnosti. Při správném a hlavně dostatečně srozumitelném nastavení tak může uživatel sám zhodnotit, které funkcionality bude skutečně využívat, a nevystavovat tak svou domácí síť zcela zbytečným rizikům.

Autorka pracuje jako bezpečnostní analytik sdružení CZ.NIC, které provozuje Národní bezpečnostní tým CSIRT.CZ.