
BEZPEČNÁ DOMÁCA SIĽ ZÁKLADY



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



KOMPETENČNÉ
CENTRUM
KYBERNETICKEJ
BEZPEČNOSTI

STU

SLOVENSKÁ TECHNICKÁ
UNIVERZITA V BRATISLAVE

OBSAH

- **Bezpečná domáca sieť**
- **Brána do vášho digitálneho domova**
- **Opevnenie vášho bezdrôtového kráľovstva (Wi-Fi)**
- **Záver: Kontrolný zoznam pre trvalú bezpečnosť**

ÚVOD – VÁŠ DIGITÁLNY HRAD

Váš digitálny hrad a vy ako jeho strážca

- Predstavte si svoju domácu sieť ako digitálny hrad.
- Vo vnútri sa nachádzajú vaše najcennejšie poklady: osobné fotografie, finančné dokumenty a súkromné konverzácie.
- Vaše zariadenia (počítače, smartfóny, smart TV) sú obyvateľmi tohto hradu.
- Váš internetový router je hlavnou bránou.
- **Vy ste veliteľom hradnej stráže**, zodpovedným za bezpečnosť.

PREČO JE BEZPEČNOSŤ DÔLEŽITEJŠIA AKO KEDYKOL'VEK PREDTÝM?

- Domáca sieť je dnes centrom našich životov.
- Pracujeme z domu, deti sa vzdelávajú online, spravujeme bankovníctvo.
- Pripájame stále viac zariadení, od kamier po inteligentné chladničky.
- Nechránená sieť nie je len riziko pomalého internetu. Je to otvorená brána pre hrozby ako krádeže identity, finančné straty a vážne narušenie súkromia.
- Zlodeji už nemusia vniknúť fyzicky; môžu preniknúť cez vašu digitálnu bránu.

STAVEBNÉ KAMENE VAŠEJ SIETE

Skôr než začneme budovať opevnenie, musíme poznať základné súčasti našej siete.

1. **Modem:** Prekladač signálov
2. **Router:** Dopravný policajt vašej siete
3. **Switch:** Inteligentná rozdvojka

STAVEBNÉ KAMENE: MODEM

Modem: Prekladač signálov

- **Funkcia:** Komunikuje s vaším poskytovateľom internetu (ISP) a "prekladá" vonkajší signál do digitálneho formátu, ktorému rozumejú vaše zariadenia.
- **Analógia:** Diplomata na hraniciach vášho pozemku. Hovorí jazykom vonkajšieho sveta aj jazykom vašej domácnosti. Je nevyhnutným sprostredkovateľom.

STAVEBNÉ KAMENE: ROUTER

Router: Dopravný policajt vašej siete

- **Funkcia:** Mozog vašej domácej siete a kľúčový bezpečnostný prvok. Prijíma internet z modemu a distribuuje ho medzi všetky domáce zariadenia (káblom alebo Wi-Fi).
- Vytvára vašu súkromnú, lokálnu sieť (LAN).

Analógia: Riaditeľ stanice alebo dopravný policajt. Zabezpečuje, aby sa dáta dostali na správne miesto a bráni neoprávnenému vstupu z internetu.

STAVEBNÉ KAMENE: SWITCH

Switch (Prepínač): Inteligentná rozdvojka

- **Funkcia:** Slúži na rozšírenie počtu káblových pripojení vo vašej sieti.
- Je inteligentný – na rozdiel od starších "hubov" posiela dáta len konkrétnemu zariadeniu, pre ktoré sú určené.
- **Analógia:** Inteligentný kruhový objazd, ktorý efektívne rozdeľuje dopravu bez toho, aby spôsobil zápchy.

Poznámka: Poskytovatelia internetu často dodávajú jedno **kombinované zariadenie**, ktoré spája funkciu modemu aj routra.

WAN VS. LAN – POCHOPENIE HRANÍC

Pochopenie rozdielu medzi týmito dvoma sieťami je základom bezpečnosti.

- **WAN (Wide Area Network):** Vonkajší svet. V kontexte domácnosti je to synonymum pre internet – obrovská, verejná a nedôveryhodná sieť.
- **LAN (Local Area Network):** Váš súkromný priestor. Vaša súkromná sieť, ktorú vytvára a spravuje váš router.

Analógia: Ak je WAN rušné a nebezpečné mesto, vaša LAN je váš oplotený pozemok s domom. Router je brána s vrátnikom.

FUNKCIA NAT – PRVÁ LÍNIA OBRANY

- Samotný princíp oddelenia WAN a LAN je prvou a najdôležitejšou vrstvou ochrany.
- Router využíva technológiu

NAT (Network Address Translation).

- **Funkcia NAT:** Skrýva všetky súkromné IP adresy zariadení vo vašej sieti (LAN) za jedinou verejnou IP adresou (WAN).
- Vďaka NAT nie sú vaše zariadenia priamo viditeľné a dostupné z internetu, čo zvyšuje ich bezpečnosť.

ZÁKLADNÝ SLOVNÍK POJMOV

- Samotný princíp oddelenia WAN a LAN je prvou a najdôležitejšou vrstvou ochrany.
- Router využíva technológiu **NAT (Network Address Translation)**.
- **Funkcia NAT:** Skrýva všetky súkromné IP adresy zariadení vo vašej sieti (LAN) za jedinou verejnou IP adresou (WAN).
- Vďaka NAT nie sú vaše zariadenia priamo viditeľné a dostupné z internetu, čo zvyšuje ich bezpečnosť.

OVLÁDNITE SVOJ ROUTER

Brána do vášho digitálneho domova

- Je čas prevziať kontrolu nad najdôležitejším zariadením vo vašej sieti – routrom.
- **Problém:** Výrobcovia často dodávajú routre s univerzálnymi a verejne známymi heslami, pričom uprednostňujú jednoduchosť pred bezpečnosťou.
- Zodpovednosť za nápravu je na vás.

PRÍSTUP DO ADMINISTRÁCIE ROUTRA

Krok 1: Nájdenie IP adresy routra ("Default Gateway")

- **Windows:** V príkazovom riadku (cmd) použiť príkaz ipconfig.
- **macOS:** V Systémových nastaveniach -> Sieť -> Podrobnosti.
- **Android/iOS:** V nastaveniach pripojenej Wi-Fi siete.

Krok 2: Prihlásenie sa

- Zadať IP adresu do prehliadača.
- Zadať používateľské meno a heslo.
- **Tip:** Predvolené údaje sú takmer vždy uvedené na nálepke na spodnej strane routra.

POVINNÉ PRE KAŽDÉHO: 3 KLÚČOVÉ KROKY

Po prihlásení do administrácie je **nevyhnutné okamžite** vykonať nasledujúce tri kroky.

- 1. Zmena administrátorského mena a hesla**
- 2. Aktualizácia firmvéru**
- 3. Zakázanie vzdialenej správy (WAN Management)**

KROK 1: ZMENA ADMINISTRÁTORSKÉHO HESLA

- **Prečo?** Ponechanie predvolených údajov je ako nechať kľúče od hradu pod rohožkou. Sú verejne známe a je to prvá vec, ktorú útočník skúsi zneužiť.
- **Ako?** V administrácii hľadajte sekciu "System Tools", "Administration" alebo "System".
- Nájdite možnosť "Password" alebo "Change Administrator Password".
- Zadajte staré (predvolené) a dvakrát nové, silné heslo. Uložte zmeny.

KROK 2: AKTUALIZÁCIA FIRMVÉRU

- **Prečo?** Firmvér je operačný systém vášho routra. Môže obsahovať bezpečnostné chyby, ktoré výrobcovia opravujú v aktualizáciách. Hackeri aktívne vyhľadávajú a zneužívajú routre so starým firmvérom.
- **Ako?**
 - **Online aktualizácia (odporúčaná):** V administrácii nájdite tlačidlo "Check for Updates". Router urobí všetko sám.
 - **Manuálna aktualizácia:** Stiahnite súbor s firmvérom z webovej stránky výrobcu a nahrajte ho cez administráciu.
- **DÔLEŽITÉ:** Počas aktualizácie nevypínajte router z elektriny a pripojte počítač káblom. Prerušenie môže router trvalo poškodiť.

KROK 3: ZAKÁZANIE VZDIALENEJ SPRÁVY

- **Prečo?** Táto funkcia umožňuje prístup do administrácie vášho routra z internetu (WAN). Pre 99% domácich používateľov je zbytočná, no predstavuje obrovské bezpečnostné riziko. Umožňuje komukoľvek na svete pokúšať sa uhádnuť vaše heslo.
- **Analógia:** Rebrík na vonkajšej strane hradieb vedúci priamo do veliteľskej veže.
- **Ako?** V sekcii "Security", "Administration" alebo "Advanced" nájdite "Remote Management" alebo "WAN Access" a uistite sa, že je **vypnutá (Disabled)**.

OPEVNENIE WI-FI KRÁĽOVSTVA

Správne nastavenie Wi-Fi je kľúčové pre ochranu vašich dát, ktoré lietajú vzduchom.

Stratégia: **Nie neviditeľnosť, ale nerozbitnosť** pomocou silného šifrovania a robustného hesla.

- **Názov siete (SSID):** Zmeňte predvolený názov.
- **Šifrovanie:** Použite najsilnejší štandard.
- **Heslo:** Vytvorte nerozbitné heslo.

WI-FI: NÁZOV SIETE (SSID)

- **SSID (Service Set Identifier):** Verejný názov vašej Wi-Fi siete.
- **Prečo zmeniť predvolený názov?** Názvy ako "TP-LINK_A4F2" prezrádzajú výrobcu a model, čo útočníkovi uľahčuje hľadanie známych zraniteľností.
- **Ako zvoliť dobrý názov?** Zvoľte jedinečný a neutrálny názov. Vyhnite sa osobným informáciám (meno, priezvisko, číslo bytu).
- **Mýtus o skrytí SSID:** Skrytie názvu siete **neposkytuje žiadnu reálnu bezpečnosť**. Útočník ju odhalí za pár sekúnd a môže to spôsobovať problémy s pripájaním. Neodporúča sa.

WI-FI: ŠIFROVANIE – NEVIDITEĽNÝ PLÁŠŤ

Šifrovanie zamieša dáta do nečitateľnej podoby. Prečítať ich dokáže len zariadenie, ktoré pozná správne Wi-Fi heslo.

- **Štandardy šifrovania:**

Vždy zvolte najvyššiu dostupnú možnosť:

WPA3 > WPA2-PSK (AES).

Protokol	Úroveň bezpečnosti	Odporúčanie
WEP	Extrémne vysoké riziko	NIKDY NEPOUŽÍVAŤ
WPA	Vysoké riziko	NEPOUŽÍVAŤ
WPA2	Nízke riziko, bezpečné	DOBRÁ VOĽBA (minimum)
WPA3	Veľmi nízke riziko	NAJLEPŠIA VOĽBA

WI-FI: TVORBA NEROZBITNÉHO HESLA

Aj najsilnejšie šifrovanie je zbytočné, ak je chránené slabým heslom.

Zásady tvorby silného hesla:

- **Dĺžka je dôležitejšia ako zložitosť:** Minimálne 12-15 znakov.
- **Používajte kombináciu:** Veľké a malé písmená, číslice, špeciálne znaky.
- **Vyhňte sa osobným údajom:** Žiadne mená, dátumy narodenia, atď.
- **Použite techniku heslovej frázy (Passphrase):**
 - Veta: "Môj prvý pes bol Max a mal rád párky!"
 - Heslová fráza: MojPrvyPesBolMax&MalRadParky!
 - Je dlhá, ľahko zapamätateľná a extrémne ťažko uhádnuteľná.

POKROČILÉ OBRANNÉ MECHANIZMY

Základ máme hotový. Poďme posunúť bezpečnosť na vyššiu úroveň pomocou **segmentácie siete** – inteligentného rozdelenia priestoru vo vnútri hradiieb.

- **Firewall:** Digitálny strážca
- **Host'ovská sieť:** Bezpečná pohostinnosť
- **Rodičovská kontrola:** Ochrana najzraniteľnejších
- **Zabezpečenie IoT:** Skrotenie inteligentnej domácnosti

POKROČILÁ OBRANA: FIREWALL

Firewall: Váš osobný digitálny strážca

- **Funkcia:** Digitálna bariéra, ktorá monitoruje a filtruje dátovú prevádzku medzi vašou LAN a internetom (WAN).
- **Analógia:** Hradná stráž pri hlavnej bráne, ktorá kontroluje každého, kto chce vojsť alebo odísť.
- **Nastavenie:** Prakticky všetky domáce routre majú vstavaný firewall, ktorý je z výroby zapnutý. Jeho hlavnou úlohou je blokovať nevyžiadané pripojenia z internetu.
- **Vaša úloha:** V administrácii len **overte, že je firewall zapnutý (Enabled)**.

POKROČILÁ OBRANA: HOSTOVSKÁ SIETĚ

Host'ovská Wi-Fi sieť je jednou z najužitočnejších a najviac podceňovaných bezpečnostných funkcií.

- **Prečo ju používať?** Vytvára samostatnú, izolovanú sieť pre zariadenia, ktorým plne nedôverujete.
 - **Zariadenia vašich návštevníkov:** Ich prípadný malvér sa nedostane k vašim dátam.
 - **Vaše vlastné IoT zariadenia (smart TV, kamery):** Mnohé z nich sú slabo zabezpečené.
 - **Ako ju nastaviť?**
 - Povoľte funkciu "Guest Network".
 - Zadajte samostatný názov (SSID) a silné heslo.
 - **NAJDÔLEŽITEJŠIE:** Uistite sa, že možnosť "Povoliť hosťom pristupovať k mojej lokálnej sieti" je **VYPNUTÁ**.
-

POKROČILÁ OBRANA: RODIČOVSKÁ KONTROLA

- **Funkcia:** Umožňuje centrálné spravovať a obmedzovať prístup detí k internetu priamo na routery.
- **Čo to umožňuje?**
 - **Filtrovanie obsahu:** Blokovanie nevhodných webových stránok.
 - **Časové limity:** Nastavenie časového plánu, kedy môžu konkrétne zariadenia pristupovať na internet (napr. vypnutie Wi-Fi o 21:00).
- **Ako to nastaviť?** V sekcii "Parental Controls" vytvorte profily pre deti, priradte ich zariadenia a nastavte pravidlá.

POKROČILÁ OBRANA: INTERNET VECÍ (IOT)

IoT zahŕňa všetky "inteligentné" zariadenia: smart TV, kamery, žiarovky, vysávače atď.

- **Riziko:** Lacnejšie IoT zariadenia sú často navrhnuté na úkor bezpečnosti. Môžu mať nezmeniteľné heslá alebo neopravené bezpečnostné diery.
- Ak útočník ovládne vašu kameru, môže vás špehovať. Ak ovládne iné IoT zariadenie, môže ho použiť ako vstupný bod do celej siete.

ZABEZPEČENIE IOT – ZLATÉ PRAVIDLÁ

- 1. Kupujte od renomovaných značiek**, ktoré s väčšou pravdepodobnosťou poskytujú aktualizácie.
- 2. Zmeňte predvolené heslá** na každom smart zariadení, ak to umožňuje.
- 3. Pravidelne aktualizujte firmvér** zariadení cez ich ovládacie aplikácie.
- 4. NAJDÔLEŽITEJŠIE: Pripojte všetky svoje IoT zariadenia do izolovanej host'ovskej siete.** Tým zabránite, aby v prípade napadnutia ohrozili vaše hlavné zariadenia (notebooky, telefóny).

OCHRANA KAŽDÉHO ZARIADENIA V SIETI

Sieť je len taká silná, ako jej najslabší článok.

- Aj dokonale zabezpečený router je bezmocný, ak si používateľ na svojom počítači sám spustí vírus.
- Útok potom neprichádza zvonku, ale šíri sa zvnútra siete.
- Ochrana musí byť na každom jednom zariadení.

KÚZLO MENOM "AKTUALIZOVAŤ"

Pravidelné aktualizácie sú najdôležitejšou a najúčinnejšou súčasťou bezpečnosti.

- **Prečo?** Softvér obsahuje chyby (zraniteľnosti), ktoré vývojári opravujú v aktualizáciách (záplatách). Hackeri cielene útočia na neaktualizované zariadenia.
- **Čo všetko treba aktualizovať?**
 - **Operačné systémy:** Windows, macOS, Android, iOS. Zapnite automatické aktualizácie.
 - **Aplikácie:** Najmä webové prehliadače, e-mailoví klienti, MS Office, Adobe Reader.
 - **Firmvér:** Router a všetky IoT zariadenia.

ANTIVÍRUSOVÝ SOFTVÉR

Antivírus je ďalšou kľúčovou vrstvou obrany priamo na vašom zariadení.

- **Prečo je potrebný?** Moderný bezpečnostný softvér chráni pred širokou škálou hrozieb (malvér):
 - **Ransomware:** Vydieračský softvér, ktorý šifruje súbory.
 - **Spyware:** Špehovací softvér, ktorý kradne heslá a osobné údaje.
 - **Adware:** Zobrazuje nevyžiadajú reklamu.
- **Chráňte počítače aj mobilné telefóny!** Smartfóny dnes obsahujú obrovské množstvo citlivých dát.

BEZPEČNÉ SŤAHOVANIE

Jeden z najbežnejších spôsobov infekcie je stiahnutie škodlivého súboru.

- **Zlaté pravidlo:** Sťahujte softvér a súbory **iba z oficiálnych a dôveryhodných zdrojov**.
 - Oficiálne weby vývojárov.
 - Oficiálne obchody s aplikáciami (Google Play, Apple App Store).
- **Riziko:** Neoficiálne úložiská a P2P siete sú rajom pre malvér. Útočníci často ponúkajú platený softvér "zadarmo", ku ktorému pribalili škodlivý kód.
- **Pozor na falošné tlačidlá "Download"**. Dôverujte varovaniam vášho prehliadača.

BEZPEČNOSŤ NA VEREJNÝCH WI-FI SIEŤACH

Keď opustíte svoj digitálny hrad, musíte prijať **princíp "nulovej dôvery"** voči akejkoľvek sieti, ktorú sami nespravujete (kaviarne, letiská, hotely).

Skryté nebezpečenstvá:

- **Odpočúvanie (Packet Sniffing):** Na nešifrovaných sieťach môže ktokoľvek čítať vašu komunikáciu.
- **Útok "Man-in-the-Middle" (MitM):** Útočník sa postaví medzi vás a web, zachytáva a môže meniť komunikáciu.
- **Útok "Evil Twin" (Zlé dvojča):** Útočník vytvorí falošný Wi-Fi hotspot s dôveryhodným názvom (napr. "Letisko_Free_WiFi"), ku ktorému sa automaticky pripojíte.

VPN – VÁŠ OSOBNÝ ŠIFROVANÝ TUNEL

Našťastie existuje veľmi účinný nástroj na obranu na verejných sieťach:

VPN (Virtuálna privátna sieť).

- **Ako VPN funguje?** Vytvára bezpečný, šifrovaný "tunel" medzi vaším zariadením a vzdialeným VPN serverom. Všetky dáta prechádzajú týmto tunelom.
- Vďaka silnému šifrovaniu sú vaše dáta pre kohokoľvek v lokálnej sieti len nezmyselnou zmesou znakov.
- **Odporúčanie:** Zapnite si VPN **vždy**, keď sa pripájate k akejkolvek sieti, ktorej na 100 % nedôverujete.

ZÁVEREČNÝ KONTROLNÝ ZOZNAM (1/2)

Bezpečnosť je nepretržitý proces. Použite tento zoznam na kontrolu.

Zabezpečenie routra (Hlavná brána):

- Zmenené predvolené administrátorské heslo.
- Nainštalovaný najnovší firmvér.
- Zakázaná vzdialená správa (Remote Management).
- Overený a zapnutý firewall.

Zabezpečenie Wi-Fi siete (Hradby):

- Zmenený predvolený názov siete (SSID).
 - Použitie najsilnejšie šifrovanie (WPA3 alebo WPA2-AES).
 - Vytvorené silné a dlhé heslo (heslová fráza).
-

ZÁVEREČNÝ KONTROLNÝ ZOZNAM (2/2)

Pokročilá ochrana (Vnútorne opevnenie):

- Vytvorená a používaná samostatná hosťovská sieť pre návštevy.
- Všetky IoT zariadenia pripojené do hosťovskej siete.
- Využívaná rodičovská kontrola (ak je relevantné).

Ochrana zariadení (Obyvatelia hradu):

- Zapnuté automatické aktualizácie OS na všetkých zariadeniach.
- Pravidelne aktualizované dôležité aplikácie.
- Používaný kvalitný a aktualizovaný antivírus.
- Sťahovanie len z oficiálnych zdrojov.

Ľudský faktor (Výcvik stráže):

- Ostražitosť voči phishingu.
- Používanie VPN na verejných Wi-Fi sieťach.

ZÁVER

- **Zostaňte ostražití a váš digitálny hrad zostane bezpečný.**

ĎAKUJEM ZA POZORNOST

- Otázky a odpověde