

Zabezpečení webových serverů

Zabezpečení webového serveru (jako [Apache](#) nebo Nginx) na systému [Linux](#) vyžaduje kombinaci správné konfigurace, šifrování a neustálého monitoringu. Cílem je minimalizovat „plochu útoku“ (attack surface).

1. Šifrování komunikace (HTTPS/TLS)

Základem bezpečného webu je protokol HTTPS. Ten zajišťuje, že data mezi prohlížečem a serverem nemůže nikdo cestou přechít ani pozměnit.

- **SSL/TLS certifikáty:** Dnes je standardem využívat bezplatnou autoritu **Let's Encrypt**.
- **HSTS (HTTP Strict Transport Security):** Hlavička, která prohlížeči přikáže komunikovat výhradně přes HTTPS, čímž brání útokům typu SSL Stripping.

2. Zabezpečení na úrovni sítě (Firewall)

Server by měl mít otevřené pouze ty porty, které nezbytně potřebuje k provozu. Vše ostatní musí blokovat firewall (např. `ufw`, `firewalld` nebo `iptables`).

Port	Služba	Doporučení
80	HTTP	Přesměrovat na 443
443	HTTPS	Povolit pro všechny
22	SSH	Omezit na konkrétní IP adresy nebo změnit port
3306	MySQL	Zakázat přístup zvenčí (povolit pouze localhost)

3. Obrana proti útokům hrubou silou (Brute Force)

Útočníci se neustále pokoušejí uhodnout hesla ke službám jako SSH nebo administrace webu.

- **Fail2Ban:** Nástroj, který sleduje logy a po několika neúspěšných pokusech o přihlášení automaticky zablokuje IP adresu útočníka na úrovni firewallu.
- **SSH klíče:** Úplný zákaz přihlašování heslem a vyžadování privátního klíče.

4. Bezpečnostní hlavičky HTTP

Správně nastavený webový server by měl v každé odpovědi posílat hlavičky, které chrání uživatele v prohlížeči:

- **Content Security Policy (CSP):** Určuje, ze kterých domén může web stahovat skripty a obrázky. Brání útokům typu **XSS** (Cross-Site Scripting).
- **X-Content-Type-Options:** Brání prohlížeči v „hádání“ typu souboru (MIME-sniffing).
- **X-Frame-Options:** Zabraňuje zobrazení webu v `i f` rame na cizí stránce, což brání útoku **Clickjacking**.

—

5. Oprávnění a izolace systému

Pád aplikace nebo napadení webu by nemělo vést k ovládnutí celého serveru.

- **Principle of Least Privilege:** Webový server nesmí běžet pod uživatelem `root`. Musí mít vlastní omezený účet (např. `www-data`).
- **Zakázání Directory Listing:** Útočník by neměl vidět seznam souborů v adresářích, kde chybí soubor `index.html`.
- **Kontejnizace:** Provozování webu v [Dockeru](#) poskytuje další vrstvu izolace od hostitelského systému.

—

6. Detekce a prevence (WAF a IDS)

Pro pokročilé zabezpečení se používají specializované nástroje:

- **WAF (Web Application Firewall):** Např. modul **ModSecurity** pro Apache. Analyzuje HTTP provoz a blokuje podezřelé dotazy (SQL Injection, XSS).
- **IDS/IPS:** Systémy pro detekci a prevenci průniku, které sledují neobvyklé chování v celém systému.

Související články:

- [Apache: Konfigurace modulů](#)
- [Linux: Správa uživatelů a práv](#)
- [Docker: Izolace aplikací](#)

Tagy: security webserver cybersecurity https firewall sysadmin it-basics

From:

<https://www.serviceit.cz/> - **IT ENCYKLOPEDIE**

Permanent link:

https://www.serviceit.cz/doku.php?id=it:sw:security_web

Last update: **2026/01/02 20:03**

