

[009] Tri nevyhnutné kroky na zabezpečenie webu

Vedel si, že každý deň je **hacknutých** až **100 000 webov** na celom svete? Online priestor v súčasnosti ponúka množstvo príležitostí pre **novodobých zločincov**. Preto si je potrebné kvalitne a dostatočne zabezpečovať webové sídla pred ich napadnutím. Tu sú 3 možnosti ako na to:

Krok 1: Zabezpeč si doménu

Najúčinnejším spôsobom ochrany domény je pridať k nej doplnkovú úroveň zabezpečenia, známu pod skratkou **DNSSEC**. Ide o systém, ktorý **zabraňuje hackerom presmerovať používateľa** na nesprávnu www adresu a získať tak citlivé údaje, ktoré môže následne zneužiť. Získaš ho jednoducho – oslov registrátora tvojej domény.

Krok 2: Chráň si webovú komunikáciu

Klient pri vpisovaní platobných údajov do jednotlivých políčok tvojho e-shopu vkladá to teba všetku dôveru, čo sa týka jeho osobných či iných citlivých údajov. Nesklam ho a nedovoľ, aby došlo ku krádeži a zneužitiu jeho údajov. Zabezpeč si tzv. **SSL certifikát**, ktorý **zašifruje komunikáciu** medzi tvojou webstránkou a zariadením klienta. Nainštaluj si ho sám, alebo sa opýtaj svojho registrátora.

Označenie **HTTPS** v adrese webu prezrádza, že ide o web zabezpečený SSL certifikátom. Písmeno „S“ na konci je z anglického slova „secure“.

Krok 3: Zabezpeč si vstup do účtov na webe

Dnes je bežným štandardom, že máš účty zabezpečené heslom. Pri manipulácii s citlivými údajmi je však nevyhnutné akési „heslovanie na druhú“, teda že po zadaní hesla si tvoje zariadenie vyžiada ešte overovací kód, ktorý ti príde napr. na mobil. Tento postup voláme **dvojfaktorová autentifikácia** (skrátene 2FA). Zabezpečenie týmto spôsobom môžeme len odporúčať a nie je to nič ťažké.

Rada na záver:

Šikovný klient vie veľmi ľahko zistiť, či máš DNSSEC alebo SSL certifikát. Na základe toho sa môže rozhodnúť, či u teba nakúpi, alebo pôjde inde, kde je bezpečnosť na prvom mieste.

