



B



E



Z



P



E



Č



N



O



S



T

Bezpečné používání webu

Webové stránky se používají k mnoha činnostem. Je důležité vědět, kde jsou uloženy a že se s nimi přistupuje pomocí tzv. webového prohlížeče. Do adresní řádky webového prohlížeče je třeba správně zadat adresu stránky, abychom komunikovali s tou stránkou, s kterou opravdu komunikovat chceme.

Co je to web

Web je tvořen množstvím webových serverů, rozmístěných po celém světě. Webový **server** je výkonný počítač, který poskytuje nějaký obsah - data. Ten, kdo data požaduje, musí znát adresu serveru, který data poskytuje. Musí být také schopen o data požádat a přijmout je.

Program, který umožňuje připojit se k serveru a komunikovat s ním, se obecně nazývá **klient**. Klient odesílá serveru **požadavek** a čeká na jeho **odpověď**. V případě webu je klientem webový prohlížeč a odpovědí serveru je webová stránka.



Mezi klientem a serverem putuje požadavek i odpověď komplikovanou sítí, jako je například Internet. Klient ani server neřeší cestu požadavku či odpovědi. To řeší síť samotná. Ta se často zobrazuje pro zjednodušení jako obláček.

Co je webová adresa (URL)

Webová adresa je přesný identifikátor toho, co má webový prohlížeč zobrazit. Můžete se setkat také s pojmem URL (Uniform Resource Locator, jednotná adresa zdroje).

Webová adresa se skládá se z několika částí:

HTTP nešifrovaný či HTTPS šifrovaný protokol pro přenos dat.

Doménové jméno označuje cílový **server** požadavku.

protokol://**doménové_jméno**/**umístění_na_serveru**?**parametry**#**kotva**

Na **serveru** se může nacházet více dokumentů nebo aplikací,

Parametry a kotva **požadavek** mohou ještě více upřesnit.

Doménové jméno je velmi důležité! Záměna jediného písmena v doménovém jméně způsobí, že se webový prohlížeč dostane na úplně jiný webový server, který v lepším případě nebude existovat. V horším případě bude nabízet podvodnou stránku.

Jedním z úkolů při putování sítí je převedení cílové adresy požadavku na tzv. IP adresu požadovaného serveru. Tento úkol řeší automaticky specializované servery DNS (Domain Name System). Více o IP adresách viz kapitola 7.

Zkracovače URL

Webová adresa může být někdy příliš dlouhá a špatně by se tiskla nebo diktovala. Lze ji ale zkrátit pomocí speciální webové služby - zkracovače (např. **bitly.com**).

Zkrácená webová adresa je lépe čitelná, ale vypadá jinak než originál. Neobsahuje již původní doménu ani další části. Nelze v ní odhalit případný podvod pouhým pohledem. Proto zkrácené webové adresy často zneužívají kyberpodvodníci.

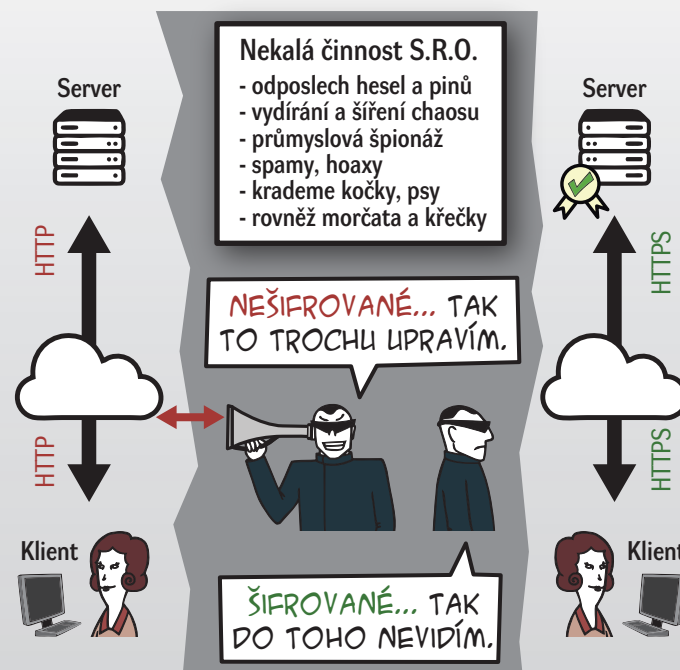
Zkrácenou webovou adresu lze obnovit do plné délky opět stejnou webovou službou a před jejím navštívením bychom si měli ověřit, zda webová adresa odpovídá opravdu webovému serveru, na který se chceme dostat.

Protokoly

Protokol je způsob, jakým spolu webový prohlížeč a webový server komunikují. Základním protokolem je **HTTP** (hypertext transfer protokol). Potokol HTTP nechraní přenášená data

a na jejich cestě sítí je tak může kdokoliv zachytit a přečíst nebo změnit. Proto vznikl protokol **HTTPS** (hypertext transfer protocol secure), který celou komunikaci šifruje.

Šifrovaná komunikace je čitelná (dešifrovatelná) pouze pro daný webový server a daný webový prohlížeč, a kdo ji zachytí, nebude ji moci přečíst ani účinně změnit.



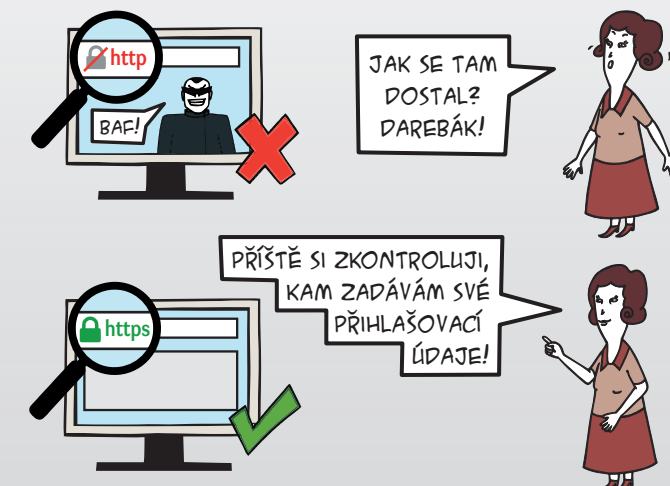
Webové certifikáty

Webový certifikát nám říká, komu patří webový server, se kterým komunikujeme. Vlastníka domény směřující na webový server ověřuje certifikační autorita (CA), kterou považujeme za důvěryhodnou. Podle důkladnosti ověření pak CA vystaví odpovídající certifikát.

Pro komunikaci pomocí HTTPS je potřeba, aby správce webového serveru získal webový certifikát a web správně nastavil.

Certifikáty za nás ověřuje prohlížeč a jakoukoli nesrovnalost s certifikátem na webové stránce hlásí. V takovém případě bychom neměli na stránku pokračovat.

Z důvodu jejich možného odposlechnutí bychom přihlašovací údaje neměli vyplňovat do stránky provozované na nešifrovaném protokolu HTTP, ale výhradně na šifrovaném HTTPS. Zároveň bychom si měli ověřit vlastníka webu, a tedy webového certifikátu stránky, na kterou přistupujeme.



Rozdíl mezi protokolem HTTP a HTTPS je tak důležitý, že se liší i jeho označení na začátku adresního řádku prohlížeče.

Protokol HTTPS je zpravidla označen ikonou zámku. Pokud na tuto ikonu kliknete, prohlížeč zobrazí podrobnosti certifikátu potvrzujícího vlastníka dané domény.

Jsem leták ke školení IT bezpečnosti uživatelů sítě ZČU. Školení má 10 témat. Mě, ostatní letáky, brožury a prezentace najdete na <https://bezpecnost.zcu.cz>.

Naši almu mater je Západočeská univerzita v Plzni a na svět jsme přišli také díky podpoře Fondu rozvoje CESNET, z.s.p.o.

