



Bezpečné používání webu

Materiály vznikly v rámci projektu Fondu rozvoje CESNET na Západočeské univerzitě v Plzni. Školení má celkem 10 kapitol a veškeré texty, prezentace a další podrobnosti naleznete na stránce <https://bezpecnost.zcu.cz>.

Licence: Creative Commons Attribution 4.0 International Public License

- 1 Když nevíš, zeptáš se.**

V případě podezření na kybernetický útok, když obdržím pochybný e-mail nebo se počítač chová divně, kontaktuji uživatelskou podporu a domluvím se na dalším postupu. Řídím se pokyny odborníků.
- 2 Budeš se autentizovat a autorizovat.**

Počítač mě sám nepozná, proto mu musím svou identitu prokázat například znalostí hesla k uživatelskému účtu (autentizace). V aplikacích, programech a informačních systémech často nemám oprávnění ke všem činnostem. Proto po autentizaci následuje autorizace, která stanoví, co smím a co ne.
- 3 Dáš si pozor, kam heslo zadáváš.**

Přihlašovací údaje vyplňuji pouze do webové stránky, která je šifrovaná, tedy její adresa začíná **https://** nebo je na jejím začátku ikona zámku. Je důležité, aby adresa stránky byla uvedena přesně; i podvodné stránky mohou používat šifrování.
- 4 K přichozí poště budeš zdravě podezřívý(á).**

Elektronická pošta je často zneužívána k rozesílání spamů, hoaxů, phishingových nebo hromadných zpráv. Dávám si pozor na podezřelé e-maily, zvláště na ty, které obsahují přílohu nebo odkazy na stránky. Příloha může obsahovat škodlivý kód a odkazovaná stránka může být podvodná.
- 5 Nebudeš věřit všemu, co se na Internetu píše.**

Na Internetu může zveřejňovat informace každý, i autor neznalý nebo záměrně manipulující. Proto si věrohodnost získávaných informací vždy ověřuji. V pracovním prostředí musím zacházet s informacemi uvážene; ne všechny údaje jsou určeny všem.
- 6 Důvěrné informace budeš šifrovat.**

Šifrování dat zajišťuje, že si informaci nemůže přečíst každý, kdo ji získá, ale jen ten, kdo zná navíc dešifrovací klíč. Elektronický podpis potvrzuje, že podepsaná osoba je autorem nebo že s obsahem souhlasí. Zároveň potvrzuje, že obsah elektronicky podepsaného dokumentu se po podepsání už nezměnil.
- 7 Na Internetu nejsi anonymní.**

Prohlížením stránek i používáním služeb na Internetu po sobě zanechávám množství stop. Další stopy vznikají dobrovolným zveřejňováním informací o sobě, zejména na sociálních sítích. Všechny tyto činnosti moji anonymitu snižují a je dobrým zvykem chovat se tak, jako by mě mohl kdokoli identifikovat.
- 8 Budeš chránit své počítače a data zálohovat.**

Nikdo nepovoláný by neměl používat cizí osobní věc, jakou je například počítač. Takové zařízení musím chránit zamykáním kanceláře a používáním zámku obrazovky. Dbám na aktuálnost jeho programového vybavení, případně svěřím správu zařízení odborníkům. Důležitá data pravidelně zálohuji.
- 9 Mobilní zařízení jsou také počítače.**

Mobilní zařízení, dnes nejčastěji chytrý mobilní telefon, je malý počítač a chovám se k němu a datům v něm stejně jako v případě počítače. Navíc si musím uvědomovat rizika, která přináší možnost zařízení přenášet nebo ho mít stále u sebe.
- 10 Budeš dodržovat pravidla a ctít právo.**

Na Internetu platí stejná legislativa jako v reálném světě, ale je rozšířená o některé další specifické právní normy. Mimo tuto státem vyžadovanou legislativu dodržuji také interní pravidla organizací nebo pravidla používání konkrétních služeb.

Bezpečné používání webu

3.1 Úvod

Webové stránky lidé používají k mnoha činnostem, jako třeba ke čtení zpravodajství, blogů, ke komunikaci s přáteli, k prohlížení obrázků a videí a samozřejmě také k pracovním záležitostem. Zobrazovaný obsah je uložen na mnoha místech po celém světě, na tzv. webových serverech. Přístup k obsahu je zprostředkován specializovanou aplikací – webovým prohlížečem, který zobrazí obsah umístěný na adrese zadané do adresní řádky.

Správnost zadané adresy je důležitá, ale sama o sobě nestačí, abychom mohli bezpečně komunikovat. Také bychom nebyli rádi, kdyby do komunikace mohl někdo vstoupit a číst ji nebo ji dokonce pozměňovat, proto je potřeba přenášena data šifrovat. Dále je třeba ověřit, že šifrovaně komunikujeme skutečně s tím, s kým komunikovat chceme. K tomuto účelu slouží certifikáty, kterými nám certifikační autorita potvrzuje, že daný certifikát patří k danému webu, případně dokonce i jaké organizaci.

3.2 Používání webu

V dnešní době, když chcete používat e-mailovou schránku, přehrávat videa, hudbu, posílat velké soubory nebo používat internetové bankovníctví, *nemusíte* mít pro každou činnost *zvláštní aplikaci*, ale je možné používat prakticky vše ve *webovém prohlížeči*, který je často již předinstalován v operačním systému (Internet Explorer, Edge, Google Chrome, Opera, Mozilla Firefox, Safari a další).

Pro využívání webových aplikací je potřeba pouze znalost internetové adresy a samozřejmě síťové připojení (intranet, Internet). Po vyplnění adresy do adresního řádku a načtením stránky (webu) se webová aplikace spustí.

Často je třeba se na úvod přihlásit (autentizovat), tj. zadat jméno a heslo nebo jiným způsobem prokázat svou identitu (viz kapitola [Kdo jsem a co smím](#)).

3.3 Co je to web

Web je tvořen množstvím webových serverů rozmístěných po celém světě. Webový server je výkonný počítač a každý takový počítač vždy poskytuje nějaký obsah - data. Některý obsahuje jízdní řády, jiný zase internetové bankovníctví konkrétní banky, zpravodajství, archivy televizního vysílání apod. 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.



3. BEZPEČNÉ POUŽÍVÁNÍ WEBU

Web je tak rozsáhlý, že o obsah a chování webů se musí starat mnoho lidí. Různí lidé mají také různé odpovědný přístup, a proto je i kvalita webů a jejich obsahů různá. O tom, jak se k věrohodnosti informací z webu stavět, si můžete přečíst v kapitole [Informace a Internet](#).

Nyní se ale soustředíme na to, jak poznat, na kterém webu se zrovna nacházíme nebo kam vede odkaz, který jsme dostali. Každý webový server má přiděleno unikátní doménové jméno, pomocí něž je možné jej jednoznačně odlišit od ostatních. Zpravidla lze ještě serveru upřesnit, co od něj chceme, tím, že za adresu v adresní řádce webového prohlížeče zapíšeme patřičné parametry. Tyto parametry jsou zpravidla generovány automaticky webovou aplikací a není potřeba je jakkoli editovat, jen je potřeba chápat jejich přítomnost a důležitost.

3.4 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 je složena z několika částí:

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

Webový prohlížeč ovládá několik různých způsobů komunikace (tzv. protokoly), kterými se umí domluvit s webovými servery. *Protokol* je v URL krátký text uvedený před dvojtečkou a dvěma lomítky. Pokud žádný neuvedete, prohlížeč si vybere podle nastavení serveru. Protokolům se budeme blíže věnovat později.

Následuje *doménové jméno* webového serveru, což je nejdůležitější informace, protože podle ní lze poznat, ze kterého serveru jsou zobrazovaná data. Pro zajištění jednoznačnosti jsou doménová jména přidělována hierarchicky (obdobně jako IP adresy – viz kapitola [Anonymita na Internetu](#)). Každé doménové jméno se skládá z několika textových řetězců oddělených tečkou, například [www.zcu.cz](#). Stejně jako u běžné poštovní adresy jsou nejobecnější informace na konci (Jan Novák, Falešná 123, Plzeň). Poslední řetězec v doménovém jméně je tzv. doména nejvyššího řádu (TLD, Top Level Domain) a odpovídá často zemi, kde je webový server fyzicky umístěn (.cz, .sk apod.) nebo má určovat způsob použití (.info, .name, .com apod.). Další řetězce se nazývají podle svého pořadí od konce, tj. [zcu.cz](#) je doména druhého řádu, [portal.zcu.cz](#) je doména třetího řádu atd. Jejich interpretace záleží na politice správce příslušné TLD. Například český správce CZ.NIC umožňuje, aby si kdokoli mohl pořídit doménu druhého řádu, zatímco ve Velké Británii až doménu třetího řádu podle charakteru žadatele (doména druhého řádu je přidělena, např. [co.uk](#)). Ve chvíli, kdy fyzická osoba nebo organizace získá svou doménu, může si sama vytvářet další subdomény (např. vlastník [zcu.cz](#) si může vytvořit [www.zcu.cz](#), [webmail.zcu.cz](#) apod.).

Na webové adrese se také může nacházet více dokumentů nebo webových aplikací, které lze odlišit pomocí „umístění_na_serveru“. Ve webové adrese je toto *umístění* uvozeno lomítkem a nemusí být vždy přítomno.

Pomocí webové adresy můžeme také předávat určité *parametry* (například pozici na mapě, předvyplněná políčka ve webovém formuláři apod.), které jsou uvozeny znakem otazníku a také nemusí být vždy přítomny.

Poslední částí je tzv. *kotva* uvozená znakem mřížky. Kotva typicky označuje místo na dlouhých stránkách, které se nevejdou na jednu obrazovku, a webovému prohlížeči říká, kterou část stránky má zobrazit (jak moc ji má posunout/odrolovat).

Důležitost doménového jména

Přesnost doménového jména je důležitá, protože při záměně byť jen jednoho písmena způsobí, že se webový prohlížeč dostane na úplně jiný webový server. V lepším případě dané jméno nebude existovat, v horším je to podvodná stránka, která se snaží vydávat za správnou.

V následujícím příkladu doménové jméno přirovnáme k adrese restaurace „U tří koťátek“ a ukážeme si, co způsobí změna byť jen v jednom jediném znaku.

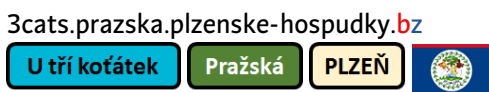
3cats.prazska.plzenske-hospudky.cz



Doménové jméno [3cats.prazska.plzenske-hospudky.cz](#) v podstatě říká, že stránka je v ČR, ve městě Plzeň, v ulici Pražská a v restauraci U tří koťátek (všimněte si, že jdeme zprava doleva).



Pokud ale zaměníme plzenske-hospudky za kotehulske-hospudky, vidíme, že jsme stále v ČR v restauraci U tří koťátek v ulici Pražská, ale nikoli v Plzni, ale v Kotěhůlkách.



Pokud zaměníme .cz na .bz, jsme v restauraci U tří koťátek, v ulici Pražská, ve městě Plzeň, ale nikoli v ČR ale v Belize, tedy dokonce na jiném kontinentě.

Jak je vidět, *jeden znak* může znamenat ve světě Internetu *velký rozdíl*. Pozor je třeba dát hlavně na záměnu znaků, které jsou vizuálně velmi podobné.

Příklad

- ➡ <https://google.com>
Správná adresa Google.
- ➡ <https://goog1e.com>
Jednička místo malého písmene „l“.
- ➡ <https://g00gle.com>
Nula místo písmene „o“.

Všimněte si, že jednotlivé domény, ať už doména nejvyššího řádu, doména druhého řádu, případně subdomény jsou od sebe odděleny tečkou. Tečka je tedy jediný správný oddělovač a jiný znak na místě oddělovače způsobí, že se dostaneme na webový server, kam jsme nechtěli.

Příklad

- ➡ <http://apple.com/iphone>
Dostaneme se na server `apple.com` do adresáře `iphone`.
- ➡ <http://apple.com-iphone.com>
Dostaneme se na server `com-iphone.com`, na subdoménu `apple`.

Na výše uvedených příkladech vidíme, že stačí malá záměna znaku a adresa dostane úplně jiný význam.

Zkracovače URL

Často je webová adresa dlouhá a špatně by se pamatovala, tiskla nebo diktovala, proto vznikly tzv. zkracovače adres, které jsou dostupné jako webová služba. Jako příklad uvedeme bitly.com.

Příklad

- ➡ Hlavní stránka uživatelské podpory ZČU
https://support.zcu.cz/index.php/Hlavn%C3%AD_strana
- ➡ Zkrácený odkaz pomocí bitly.com
<http://bit.ly/supportZCU>

Zkracovačů mohou využít také útočníci, kteří chtějí před potenciální obětí skrýt skutečnou adresu. Před kliknutím na zkrácený odkaz je potřeba zobrazit skutečnou adresu, na kterou zkrácený odkaz vede například zde: <http://www.checkshorturl.com/>



3. BEZPEČNÉ POUŽÍVÁNÍ WEBU

<http://bit.ly/supportZCU>

Expand



Long URL https://support.zcu.cz/index.php/Hlavn%C3%AD_strana

Protokoly

Způsob, jakým spolu webový prohlížeč a webový server komunikuje, se označuje jako protokol a ve webové adrese je uveden jako první položka. Základním protokolem je HTTP (hypertext transfer protocol), který slouží k přenosu hypertextových dokumentů HTML, XML a obecně i dalších souborů. Jeho nevýhodou je, že data jsou přenášena v nešifrované podobě, tj. jsou čitelná po celou dobu přenosu.

Vzhledem k tomu, že web je distribuován po celém světě a data tečou přes různé počítačové sítě, může je cestou někdo vidět nebo dokonce měnit. Proto je potřeba přenášena data šifrovat.

Do nešifrované komunikace je velmi snadné zasahovat

Například pokud se přihlásíte k otevřené veřejné bezdrátové síti (tzv. free wi-fi hotspot), může vám její poskytovatel vkládat reklamu do zobrazovaných stránek. Letištní wi-fi hot-spoty jsou tím pověstné.

Šifrovanou komunikaci zajišťuje protokol HTTPS (hypertext transfer protocol secure), díky kterému je komunikace čitelná (dešifrovatelná) pouze pro server a daný webový prohlížeč. Pokud jsou na webové stránce zadávány důvěrné informace, jakými mohou být třeba přihlašovací údaje, vždy je nutné komunikovat šifrovaně, tedy protokolem HTTPS. Webový prohlížeč nás ujišťuje o použití protokolu HTTPS další signalizací – typicky ikonou visacího zámku před URL.

3.5 Webové certifikáty

Samotné šifrování ještě nestačí, ještě je potřeba mít jistotu, že bezpečně komunikujeme s tím správným protějškem, protože i falešný web může být provozovaný šifrovaně, tedy na protokolu HTTPS. Jinými slovy, je potřeba mít nějakým způsobem ověřeno, že používané šifrovací klíče (viz kapitola [Šifrování a elektronický podpis](#)) patří našemu cílovému serveru. K tomuto ověření slouží tzv. *webové certifikáty*, které vydávají certifikační autority (dále jen CA), což jsou důvěryhodné instituce, kterým věříme.

Podle toho, jak důkladně CA ověřila vlastníka domény, vystaví *typ webového certifikátu*. Základním ověřením je, že žadatel může ovlivňovat obsah domény, ale CA již neověřuje identitu žadatele. V takovém případě certifikační autorita vystaví tzv. *DV (Domain control Validation) certifikát*. S tímto typem certifikátu se lze setkat nejčastěji. Certifikační autorita ale může také ověřovat vlastníka daného serveru, například telefonuje na vybraná telefonní čísla, vyžaduje písemné vyjádření, apod. V takových případech pak vystaví *OV (Organization Validation) certifikát* v případě zběžného ověření, nebo *EV (Extended Validation) certifikát* v případě důkladného ověření.

Může se vám zdát, že musíte být odborníkem s mnohaletou praxí, abyste vše dokázali ověřit, ale není tomu tak. Ve skutečnosti stačí pouze naslouchat svým webovým prohlížečům a vědět, co si ohlídat. Takový webový prohlížeč totiž za nás udělá mnoho práce sám. Stačí mu zadat správnou adresu webu, který chcete prohlížet, a sám si domluví šifrovací klíče, ověří platnost certifikátu, šifruje komunikaci, a pokud je něco v nepořádku, navíc vás ještě varuje. Po kliknutí na ikonu

zámečku, indikující, že komunikujeme šifrovaně, je možné si prohlédnout certifikát, kde je uveden termín konce platnosti, jaká certifikační autorita jej vydala a v případě OV a EV certifikátů také identifikace vlastníka.

Při prohlížení webových stránek je možné se setkat s hlášením webového prohlížeče, že je certifikát neplatný, obvykle vypršela jeho platnost a administrátor webu včas nezajistil jeho obnovu. Aby bylo možné říci, co v konkrétním případě způsobuje varovné hlášení, je potřeba detailnější porozumění problematice. Obecně platí, že pokud webový prohlížeč hlásí jakýkoliv problém s certifikátem webové stránky, neměli bychom na takovou stránku pokračovat. Prohlížeč vás také může upozornit, že se chystáte zadat heslo do stránky komunikující nešifrovaně, tedy po HTTP. Pokud se tak stane, předmětná stránka bude pravděpodobně podvodná, protože dnes již žádný rozumný administrátor přihlašovací stránky na protokolu HTTP neprovozuje.

3.6 Shrnutí

V této kapitole jsme se dozvěděli, že web je tvořen mnoha samostatnými servery a že k jeho prohlížení slouží webový prohlížeč. Dále víme, že webová adresa (URL) určuje, jaký obsah prohlížeč zobrazuje, a že její první část prozrazuje, na jakém webovém serveru se vlastně nacházíme, což umožňuje rozpoznat podvodnou webovou adresu.

Nyní již také víme, že důležité informace (například přihlašovací údaje) je potřeba přenášet šifrovaně. Skutečnost, že daná webová stránka používá šifrovanou komunikaci, nám sděluje náš webový prohlížeč – obvykle ikonou zámečku a/nebo zobrazením použitého protokolu HTTPS před adresou webové stránky. K ověření, že komunikujeme se správným protějškem, slouží webové certifikáty, které mohou mít různou úroveň ověření vlastníka domény.

Každopádně webový prohlížeč je schopen zařídit téměř všechny činnosti potřebné pro bezpečné prohlížení webových stránek, a když mu něco přijde podezřelé nebo si neví rady, upozorní vás. Naslouchajte tedy svému prohlížeči, pomáhá vám.