

ÚVOD DO WEBOVÝCH STRÁNEK

Úvod do teorie webových stránek a příbuzných pojmů, které jsou nutné pro práci se stránkami.

KOMUNIKACE NA INTERNETU

Počítačová síť je lokální propojení alespoň dvou zařízení, které spolu umí komunikovat. Počítačová síť může vlastně obsahovat další počítačové sítě a může vznikat jakýsi hierarchický systém. Tyto počítačové sítě komunikují nějakými protokoly a rozumí si. Probíhá tedy výměna informací a používají stejné technické prostředky.

V komunikaci rozdělujeme dva typy komunikací, a to **peer to peer** a **client-server**. Peer to peer je způsob komunikace, kdy jsou si obě dvě strany rovny a zároveň si nepřikazují. Client-server je způsob, kdy je jedna strana autoritativní a je cílena různými klienty. Server zpracovává jejich příkazy a může je i odmítnout.

Internet je celosvětový systém navzájem propojených počítačových sítí. Propojení sítí je realizováno různými způsoby (např. drátově a bezdrátově), které tu nebudeme hloubkově probírat.

Internet používá nespočet služeb, jedná se například o:

- webové stránky
- přenos videa a zvuku (streams, např. YouTube, Twitch, Netflix)
- komunikace, e-mail, sociální sítě
- a další

Počítačové sítě často rozdělujeme do dalších skupin, pro lepší představu, co jsou vlastně dané počítačové sítě, se jedná například o:

- vědecké, vojenské a bankovní instituce
- školy
- osobní, domácí sítě (router-switch, hodinky-telefon, ...)

Poznámky:

Žádné poznámky k této lekci jste ještě nezapsali.

HISTORIE INTERNETU

Začátek internetu lze trasovat do různých bodů v historii. Každý odborník definuje tento začátek jinak, obecně je však i začátkem point-to-point internetu při a po druhé světové válce, kdy potřebovali dvě místa komunikovat mezi sebou. Více je však uznávána **síť ARPANET**, která vznikla v roce 1969. **Při vzniku byly propojené čtyři vysoké školy.** Postupem se k nim připojovali další místa a tím internet vzniknul.

Již po třech letech (1972) po vzniku sítě bylo připojeno 70 zařízení. Tato síť je nyní součástí internetu, který je po celém světě. V roce 1992 se připojila jako první instituce v Česku k internetu Česká vysoká univerzita technická (ČVUT), přesněji se připojila na uzel v Linci v Rakousku.

Počet zařízení na internetu se stále zvětšuje. Aktuální odhad je mezi 50 miliardami zařízení.

Poznámky:

Žádné poznámky k této lekci jste ještě nezapsali.

WORLD WIDE WEB A DOMÉNY

Hypertextový dokument je dokument, který může být vázán na jiné dokumenty. Propojují se tzv. **hyperlinky**. Tento dokument často není lineární, ve slova smyslu, jako jsou obyčejné dokumenty, které můžete číst ze shora dolů. Tento dokument může být definován tak, že se něco může zobrazit jinde, než bylo definováno.

World wide web je soustava propojených hypertextových dokumentů. Zjednodušeně se jedná o mapu propojených dokumentů, které lze navštěvovat pomocí **webového prohlížeče**. Používá se protokol HTTP (a HTTPS) ve formátu HTML. Pro adresaci ve WWW používá URL.

Doména je částí URL adresy a určuje jednoznačný identifikátor nějakého místa (přesněji počítačové sítě či server) na internetu. Vznikla z důvodu, že komunikace pomocí IP adres je složitá:

- pro lidi je složité si zapamatovat (v případě IPv4) 4 čísla pro každý web, který navštěvují
- v případě HTTP se otevírá pouze jeden port - tím pádem by na jedné IP adrese mohl být jeden web. To by šlo obejít různými dalšími porty či rekonfigurace webů např. na 23.201.102.3/alza

Doména se rozděluje do několika částí, které jsou oddělené tečkami, všechny části musí být ASCII a ignoruje se velikost písmen. Základní je generická (doména 1. řádu, top level domain = **TLD**), která určuje úplný "zdroj" stránky, která je po poslední tečce. Většinou se jedná o země a nově i další věci. Jedná se například o **.cz, .uk, .fr, .io, .website**. Je možné si svojí vlastní generickou doménu nějak zařídit, musíte ale získat spoustu povolení a spřátelit si různé instituce. Stojí to velmi velké peníze, protože své TLD musíte spravovat, například pomocí WHOIS a zařizovat pro ně domény, administrace, ...

Nejčastější další doména je doména 2. řádu, která je nejčastější koupě. Určuje nějakou společnost, entitu či prostě danou stránku. Nejčastěji je doména kupována na rok, kdy první rok je levnější než ty následující. Jedná se např. o

seznam.cz, ssps.cz, google.com.

Všechny následující domény lze označovat jako x. řádu a často se jim říká **subdoména** (sub - menší část z něčeho). Často je to nějaká pod služba dané stránky. Např. se jedná o **email.seznam.cz, skripta.ssps.cz, calendar.ssps.cz**. S domény větším jak 4. řádu se v podstatě v praxi nelze potkat.

Internationalized Domain Names (IDN) je standard, který dovoluje, aby se v doménách mohli vyskytovat libovolné znaky abecedy z celého světa. Doména je stále však tvořena ASCII, jen jsou znaky překódovány. Například znak **á** se přetvoří na **xn-1ca**. Pro českou doménu je vypnuto z bezpečnostních důvodů (přepis může přesměrovat na phishing stránku) a taky z konfúze, protože pro jednu doménu by bylo nutné koupit další pro zaručení bezpečnosti. Společnost CZ.NIC, která českou doménu spravuje, pravidelně dělá dotazník, kde se na tuto technologii ptá. Více si lze přečíst [ZDE](#).

Poznámky:

Žádné poznámky k této lekci jste ještě nezapsali.

URL ADRESA

URL (uniform resource locator) je řetězec znaků s definovanou strukturou, který se používá pro adresaci na WWW. Když chceme webovou stránku navštívit, tak nechodíme pouze na doménu, ale můžeme určovat další věci, nejčastěji však například cestu, na které najdeme nějaký zdroj. Je rozdělen do částí a platí pro ně různé pravidla.

Části:

- **protokol** (nezáleží na velikosti písmen, povinná část, jen ji prohlížeč automaticky doplňuje) - např. `HTTPS`, `HTTP`, `FTP`, ...
- **doména** (nezáleží na velikosti písmen, povinná část)
- **port** (povinná část, jen ji prohlížeč automaticky doplňuje) - číslo od `0` do `65535`, pro HTTP se používá `80`, pro HTTPS `443`
- **umístění na serveru** - určuje místo souboru / zdroje na serveru, např. `o-skole/pedagogicky-sbor.html`
 - lomeno většinou reprezentuje přestup do jiné složky (najdi soubor `pedagogicky-sbor.html` v složce `o-skole`), ale nemusí to tak být
- **parametry** - určuje parametry se kterými může poté stránky či server pracovat, např. `?p=1` a `?name=Matěj Cajthaml&age=59`.
 - parametry vždy začínají `?`, aby se rozeznaly od umístění na serveru - ten otazník tedy obsahovat nemůže.
- **kotva** určuje jedno místo na stránce, na které se při načtení přeneseme, více si o něm povíme v dalších lekcích, např. `#seznam`

Často se k URL zapisuje i WWW, které k ničemu neslouží a je to normální doména 3. řádu. Ukázky správných URL adres:

- `https://cs.wikipedia.org/wiki/Česko`
- `https://www.jakpsatweb.cz/html/url.html`
- `https://www.luxor.cz/checkout/delivery_and_payment`
- `https://ssps.cz/news/read/452`
- `https://www.preslovinny.cz/kategorie/technologie/`
- `https://www.postovnisporitelna.cz/portal/ucty/postovni-ucet`

URL se postupně vyvíjí, prošli jsme pouhé základy a více informací naleznete na dokumentaci [ZDE](#).

Poznámky:

Žádné poznámky k této lekci jste ještě nezapsali.

VYHLEDÁVÁNÍ NA WEBU

Webový vyhledávač je automatický systém vyhledávající informace na WWW. Automaticky tedy server prochází (crawluje) stránky a zjišťuje si z nich informace, které poté uživateli, který vyhledává, ukazuje. Z různých odkazů se tvoří mapa (pavučina) WWW.

Webový katalog je seznam odkazů, které vedou na různé weby. Je spravován ručně.

Webové vyhledávače lze omezit pomocí souboru robots.txt, ve kterém lze zakázat, aby tento web navštěvovali (nebo omezit nějaké URL). Etické crawleři toto Vaše rozhodnutí budou respektovat.

Na části WWW, kam se vyhledávače nemohou dostat, říkáme, že je to **hluboký web (deep web)**. Jsou to jednoduše veškeré stránky, které potřebují přihlášení. Například se jedná o internetové bankovníctví, Vaše zprávy na Instagramu, či cokoliv obdobného. **Jedná se o největší část WWW.**

Hluboký web se často zaměřuje s **temným webem (dark webem)**. To je web, na který se nedá dostat pomocí klasických technologií a je potřeba speciální software, speciální připojení, připojení v určitý čas a různé další ochrany. Dark web stojí na anonymitě pomocí různých technologií, které lze při určitých podmínkách obejít. Na dark webu se často konají ilegální prodeje a další věci.

Do obvyčejného webu patří:

- stránky školy
- Wikipedia
- Facebook profil (dle nastavení soukromí)

Do hlubokového webu patří:

- virtuální škola / moodle
- Bakaláři
- zprávy v Messengeru / Instragramu
- zprávy v e-mailovém klientovi

Do temného webu patří:

- tzv. onion web

Poznámky:

Žádné poznámky k této lekci jste ještě nezapsali.

PROTOKOLY PRO WEB

Pro webové stránky existuje nespočet protokolů, které jsou pro jeho funkčnost nutné. My si ukážeme ty nejzákladnější z nich. Více o nich byste se měli dozvědět v předmětu PSI v 1. a 2. ročníku. Protokol je vlastně takový definovač toho, jak dvě věci mezi sebou budou komunikovat, aby si rozuměli. Mají vlastní syntaxe, sémantiku a např. synchronizaci.

HTTP

Zkratka pro Hyper Text Transfer Protocol. Je určen pro přenos hypertextových dokumentů (definované v WWW). Běží na portu 80, ale lze jej zřídit na jakémkoliv. Moderně se nepoužívá jenom pro přenos těchto dokumentů, ale i pro další věci a stal se takovým hlavním protokolem - je ve všech odvětvích IT.

HTTPS

Zkratka pro Hyper Text Transfer Protocol Secure. Je to zabezpečená nástavba HTTP, používá asymetrické šifrování pomocí klíčů a certifikátů. Data jsou po cestě šifrována. Používá se port 443. Dříve se používal pouze na důvěrné informace, nyní se používá na vše (je nutný všude).

IP

Zkratka Internet Protocol, určený na směrování paketů na internetu. Funguje na síťové vrstvě (komunikace mezi více sítěmi). Existují dvě verze, jedna je IPv4, který je vyčerpaná. Proto vznikla nová IPv6, která má i mimo počet adres více výhod.

Formát IPv4: `192.168.0.1`

Formát IPv6: `2001:718::fec9:ca5`

DNS

Zkratka Domain Name System. Jedná se o převod doménového jména na nějaké IP. Jedná se o hierarchický systém, který určuje že např. `seznam.cz` se převede na `77.75.76.3`. Může se totiž stát, že nějaké subdomény mohou vést na jiné servery, aby se všechna doména nemusel nacházet na jednom serveru, což je nebezpečné. DNS neslouží jen na převod jmen, ale například i na určování e-mailových serverů a dalších záznamů pro počítače.

DNS se musí cachovat, tedy ukládat, aby se nemuseli počítače při připojení vždy ptát, kudy se mají vydat, aby navštívili tuhle doménu. Nejbližší uložení DNS je například v routeru, u ISP a dál. DNS server si ukládá svoje záznamy o daných doménách a komunikuje s ostatními, se kterými sdílí svoje záznamy.

FTP

Zkratka pro File Transfer Protocol. Slouží k přenášení souborů mezi počítači a servery. Podporuje nespočet operací, která každá dělá něco jiného. Využívá model klient-server a pro připojení je potřeba FTP klient, který je často i v prohlížeči.

Známí FTP klienti jsou např.: WinSCP, FreeCommander, FileZilla, ...

Poznámky:

Žádné poznámky k této lekci jste ještě nezapsali.

NEBEZPEČÍ INTERNETU

Internet je bez pozoru obecně velmi nebezpečné místo. Jeden z důvodů proč tomu tak je většinou přisuzována **anonymita**, kdy v podstatě kdokoli může být kdokoli.

Nejčastější nebezpečí je závislost na internetu, kde je uživatel **závislý na samotném internetu**, kde tráví například většinu dne a není schopen bez něj žít.

Obecně je dále nebezpečné **zneužití osobních informací**, do čeho patří údaje, fotografie, vaše pozice nebo třeba i záznamy webkamery a zvuky. Je důležité své údaje zadávat jen tam, kde je to potřeba a můžete dané společnosti věřit.

Dále se na internetu nachází **podvody**, které mohou vést ke **ztrátě majetku, peněz, dat či zablokování zařízení**. Je důležité si prověřovat, s kým komunikujete a například požadovat zálohy. Obecně je dobré se s daným člověkem sejit.

Nejdůležitější je téma **kyberšikany**, které souvisí i s tématem zneužití osobních informací. Kyberšikana může stát na vydírání a dalších věcech a je dobré se ji bránit. Nejzákladnějším pravidlem by mělo být to, že danou věc řeknete další osobě, které věříte.

Poznámky:

Žádné poznámky k této lekci jste ještě nezapsali.

MALWARE

Zkratka názvu **malicious software**, který označuje nějaký nevyžádaný software nebo obecně program, který je určen k poškození počítače či uživatele. My si ukážeme jednotlivé typy.

Virus

Často je používán jako synonymum pro malware. Samovolně se šíří bez vědomí uživatele. Obvykle obtěžuje, ničí data a šíří se. Nejčastěji pomocí e-mailů a obecně přenosných médií.

Spyware

Určen ke sledování uživatele. Zaznamenává aktivitu uživatele a buď si vytváří log, který je jednou za čas poslán nebo aktivně posílá informace na server. Může se jednat o keylogger, tj. jen sledování kliku na klávesnice, ale i například pořizování snímků obrazovky či kamery.

Trojský kůň

Schovává se v zdánlivě nezávadném programu či souboru. Často při pirátění sw, her a obdob. Uživatel nemůže jednoduše zjistit zda se jedná o trojského koně - velikost souboru se značně nemění (uživatel reálnou velikost neví). Často může pomáhat zkontrolovat hash daného souboru. Obsahuje jiné typy malwerů. Název pochází z řecké mytologie [ZDE](#) najdete článek na Wikipedii.

Často se objevují i v často používaných souborech jako jsou zazipované balíčky (.rar, .zip), který například pro vybalení souborů něco udělá. Počítá se do toho i například Word se svými makry.

Počítačový červ

Šíří se po síti sám a bez vědomí uživatele. Často maže či odesílá soubory. Taktéž se často aktivuje až po čase, po tom, co se rozšíří více - tím zraní více míst / počítačů, což může vést ke větším škodám. Šíří např. i na routerech.

Adware

Po získání tohoto malwaru se uživateli začnou ukazovat různé nevyžádané reklamy, pop-up okna a další falešné ikony, které většinou žádají uživatele něco koupit a kliknout na stránku, kde bude více reklam, za které útočník dostává zaplacení. Často je to "bezpečné", je to spíše otravné a může zpomalovat počítač.

Ransomware

Vychází z anglického slova ransom, které znamená výkupné. Po aktivaci toho malwaru se veškeré data na počítači (resp. discích) zašifrují klíčem. Na PC se uživateli ukáže informace o tom, že musí zaplatit v kryptoměně nějakou částku na určitou adresu. Za zaplacení nabízí útočník heslo k rozšifrování. Data nelze bez klíče v rozumném čase rozšifrovat - o data jste buď přišli, nebo věříte, že Vám klíč po zaplacení útočník předá. Když máte štěstí, o data

nepřijdete, ale může se stát, že ransomware bude později znovu aktivován - v souborech může nadále existovat nebo v nich bude další malware.

Toto výkupné často má i časový limit, aby to uživatele nutilo vykonat nepromyšlenou akci. Po tomto časovém limitu budou všechny data smazána. Někdy obsahují i časový limit, který často zvedne.

Poznámky:

Žádné poznámky k této lekci jste ještě nezapsali.

PHISHING

Zkratka pro **password harversting fishing**. Jedná se o podvodnou techniku, která se používá k získávání citlivých údajů z různých míst. Často využívá **podvodné e-maily, bannery, stránky, SMS, hovory, administrátoři žádající údaje** a další. Pro důvěryhodnost používají stejný **design, kopírují stránky** a **snaží se působit důvěryhodně**. Po získání údajů je použijí pro získání dalších informací či majetku a peněz.

Cílem tohoto úkolu jsou často nezkušení uživatelé internetu jakéhokoliv věku. Často se však útočí i na starší obyvatele, kteří jsou obecně více důvěřiví. Česká stránka hoax.cz velké (nejen) phishingové útoky monitoruje a zveřejňuje, najdete je [ZDE](#).

Poznámky:

Žádné poznámky k této lekci jste ještě nezapsali.

OCHRANA NA INTERNETU A DIGITÁLNÍ STOPA

Ochrana na internetu

Proti nebezpečí na internetu se lze chránit různými způsoby. Nejzákladnější poznámka by měla být ta, že většina nebezpečí vzniká pokud to uživatel dovolí. Tedy je obecně dobré prověřovat to co dělat a kontrolovat svůj bezpečnostní stav. Zjednodušeně neklikejte a nestahujte věci, které neznáte. Není dobré věřit e-mailům, které neznáte.

Je dobré mít na počítači **antivirus** či **antimalware**. **Antivirus** je program, který skenuje počítač pro nebezpečí, které jsou již dlouho známé a má svojí databázi, kterou aktualizuje. Na druhé straně, **antimalware** je program velmi podobný, ale má aktivní kontrolu nebezpečí. Kontroluje tedy často to, co daný program dělá a má velmi obsáhlou a aktualizovanou databázi (stahuje i několikrát denně).

Další důležitá věc je mít vždy **pravidelné aktualizace veškerého softwaru**. Nové aktualizace mimo nové funkčnosti skoro vždy opravují nějaké chyby, které v předchozích verzích vznikly.

Při zadávání údajů je dobré **kontrolovat certifikáty a domény**. Nemělo by se zadávat důvěrná data na vyzvání.

Digitální stopa

Digitální stopa jsou záznamy na internetu, které vytváříme při procházení WWW a internet. Tyto záznamy se nacházejí jak v **prohlížeči** (klientovi) tak i na **serverech**. Patří do toho očekávané věci - příspěvky, komentáře, objednávky a další věci, které logicky musí server uchovávat.

Digitální stopa patří do **cenných informací**, což jsou informace, které mohou společnosti využívat k lepšímu marketingu a obecně k cílení. Dělíme je na **vědomé** (výše popsané, např. příspěvky, ...) a **nevědomé** (historie procházení, samotná návštěva stránky, kde na webu klikáte, ...). Tyto informace nemusí být určité použité k špatné věci (tj. zanechané nepříteli), ale **mohou být využity k zlepšení služby**.

Pro minimalizaci zanechávání stopy je dobré si nastavit prohlížeč tak, aby **posílal webům co nejméně informací**. Poté je dobré při první návštěvě webu nastavit cookies tak (podle cookies law od EU), že **nechcete využívat soubory ke sledování**. Proti některé stopě se nelze bránit - jak se říká, to co nahrajete na internet tak bude velmi pravděpodobně navždy.

K tématu patří taky **metadata**. Jsou to data, které popisují data (tj. **data o datech**). Jako ukázka můžou být například fotografie, kde se často ukládá, kdo je vyfotil, kdy byly vyfoceny, kdy byl soubor naposledy upraven a podobně. Tyto informace existují skoro ke každým datům - souborech, příspěvech, e-mailech, ...

K realizaci toho, jak moc jen samotný prohlížeč posílá na internet informací (metadat), doporučuji navštívit stránku [AmIUnique](#), na které si můžete ověřit jak unikátní jste. Webové stránky mohou například skenovat nainstalovaná písma a podle toho je velmi jednoduché kohokoliv poznat.

Žádné poznámky k této lekci jste ještě nezapsali.

PROHLÍŽEČE

Webový prohlížeč je software, který je určený k **procházení WWW**, zjednodušeně webů. Jeho cílem je komunikovat se servery v různých protokolech, nejčastěji pomocí HTTP/S. Prohlížeč však má různé věci, které s procházením nemusí přímo souviset. Často řeší i jiné úlohy (záložky, kalendáře, e-maily, historii) a jsou nastavitelné. Hlavní částí prohlížeče je **vykreslovací (renderovací) jádro**, které slouží pro vykreslování stránek v jazyce HTML, se kterým se tento rok budeme učit.

Nejčastější jádra jsou **Gecko** (Mozilla Firefox), **Webkit** (Safari), **Blink** (Google Chrome) a např. Trident (Internet Explorer). Jádra se hlavně liší v tom, jak se webové stránky vykreslují.

Chromium je vlastně takový "prohlížeč" bez ničeho na víc. V podstatě obsahuje jen vykreslovací jádro **Blink**, které obsahuje Google Chrome. Je to velmi oblíbený nástroj, který se používá pro vykreslování webových stránek bez zbytečných věcí na více. **Velmi mnoho prohlížečů na něm staví svůj základ** a nepoužívají tím své jádra - jedná se např. o Vivaldi, Operu, MS Edge, Brave a spoustu dalších. Chromium je **opensource** a tedy každý do něj může nahlížet a upravovat jej. Chromium lze používat samostatně jako náhrada Google Chrome, ale neobsahuje například ani synchronizaci mezi zařízeními. **Hlavní nevýhodou Chromia** je to, že jej využívat již tolik prohlížečů, že se stal Google gigantem, který může velmi jednoduše ovlivňovat vývoj webu - **velmi se snížila kompetivnost na tomto trhu**. Jediné použitelné možnosti je Gecko a Blink, kdy Webkit od Safari s weby velmi stagnuje.

Moderní prohlížeče by se měli co nejvíce přizpůsobit potřebám uživatele, jedná se např. o:

- úpravy barev
- úpravy velikosti písmen a fontů
- umí ochránit uživatele před reklamou či sledovači
- má anonymní režim
- být rychlý a nebrat zbytečné zdroje počítače
- podporuje rozšíření
- má synchronizaci

Poznámky:

Žádné poznámky k této lekci jste ještě nezapsali.

HOSTOVÁNÍ

Hosting je služba, která Vám dovoluje nějak **pronajmout hardware**, který je schopen komunikovat s internetem a nebo např. něco vypočítávat. Existuje nespočet typů hostingů, my si ukážeme jen základní.

Serverhosting je pronájem celého serveru (počítače), na kterém si lze spustit jakýkoliv software. Zákazník má přístup k celému serveru a může složit úplně na cokoli - např. hostování stránek, her či různé vnitřní systémy.

Webhosting je pronájem místa na cizím serveru, který je určen na hostování stránek. Je to omezené místo a jsou omezeny i další parametry. Server a web spravuje daná organizace, většinou nejsou práva pro nějakou konfiguraci.

Freehosting je nějaký typ hostingů, který je zdarma. Často chybí technologie, databáze a další služby. Vkládá se například reklama nebo je jinak omezena. Používá se taky jako ukázka služeb daného hostingů. Často je k dispozici i doména 3. řádu zdarma.

Mezi další služby, které hostingy nabízí, patří:

- doména
- certifikáty
- databáze
- e-mail
- výpočetní služby

Pro výběr hostingů existuje nespočet kritérií. Je nutné odhadnout, kolik webová stránka zabere místa a jaké technologie budou potřeba. Mezi známe české hostingy patří:

- Wedos
- Endora
- Forpsi
- Stable
- Active24

Poznámky:

Žádné poznámky k této lekci jste ještě nezapsali.

CERTIFIKÁTY

Certifikát je určen pro jednoznačnou identifikaci entity (stránky, služby, uživatele) na internetu. Stojí na **asymetrickém šifrování** a podpisech. **Podepsání** je vlastně akt, kdy je certifikát podepsán (jiným) certifikátem a tím je schválena jeho existence - pravost.

Certifikát obsahuje **veřejný (encrypt) klíč**, který slouží k šifrování dat. Poté obsahuje **soukromý (decrypt) klíč**, který slouží k rozšifrování dat. K tomu obsahuje ještě **expiraci** daného certifikátu - jedná se o datum, po kterém by se certifikátu nemělo důvěřovat. Obsahuje další informace o tom, kdo jej **podepsal (vydal)**, **pro koho je určen**, pro jaké je domény a podobně.

Certifikační autorita je společnost, která podepisuje cizí certifikáty za určitý obnos. Poté je certifikát platný a kdokoliv si jeho pravost díky klíče certifikační autority ověřit. Tyto služby jsou často zpoplatněné (poskytují více věcí a služeb) a nebo i zdarma, jako např. [Let's Encrypt](#). **Certifikát může autorita zneplatnit.**

Důvěryhodnost certifikátu je založen právě na tom, že si kdokoliv může **zkontrolovat kdo jej podepsal**. Klíče pro asymetrické šifrování jsou natolik bezpečné na normální počítačích (na kvantových tomu tak nemusí být), **že je nemožné je v rozumném čase dešifrovat i se všemi PC na světě**. Přesto se používá životnost certifikátů, aby se certifikáty často měnili. Když si sám vytvoříte certifikát, tak si jej sám můžete podepsat svým certifikátem. Jedná se tzv. o **self-signed** certifikáty, které se hodí na osobní použití a prohlížeče a další služby jej berou jako nebezpečný.

Certifikáty se používají všude - např. v HTTPS, VPN, SFTP, SSH a spoustě dalších službách.

Pro lepší představení certifikátů doporučuji tento materiál k dispozici [ZDE](#).

Poznámky:

Žádné poznámky k této lekci jste ještě nezapsali.

AUTORSKÝ ZÁKON

Webové stránky jsou chráněny autorským zákonem. Často se na stránkách uvádí formulace `2022 © Cajthaml, All right reserved`, která je vlastně jen pro upozornění.

Bez uvedení licence je stránka stále pod autorským zákonem. Vašeho práva jako autora díla není možné se vzdát. Tento termín je však takovým standardem, že je velmi dobré jej tam psát.

Bez používáním jakékoliv věci je dobré zkontrolovat **zdroj, licenci a podmínky**, pod kterými můžete danou věc používat. V žádném případě licenci neignorujte - můžete z toho mít velké problémy.

Pro ulehčení licencování věci existují předpřipravené licence, které definují jak se věci mohou používat již předem. Jedná se například o [Creative Commons](#), které definují různé kombinace licencí, které povolují a zakazují různé věci. Jedná se například o **zákaz používat věc pro komerční využití**, nebo že musí po úpravě díla být použita stejná licence. Druhá věc je **fair use**, kde použijete věc v zájmu sebe, ale však uvedete správně zdroj - jedná se např. pro školní účely.

Poznámky:

Žádné poznámky k této lekci jste ještě nezapsali.

SPRÁVA OBSAHU

Content Management System (CMS) je systém pro správu obsahu. Jedná se o nějaký **redakční** nebo **publikační** systém, ve které pomocí uživatelského prostředí lze editovat obsah. Existuje pro různé jazyky a platformy.

Jedná se např. o: WordPress, Strapi, Joomla!, Drupal a další.

Poznámky:

Žádné poznámky k této lekci jste ještě nezapsali.

