**Úvod do problematiky**

Internet, celosvětová síť propojující zařízení různého typu a nabízející nespočetně služeb po celém světě, je bezesporu fenomén několika posledních dekád. Internet poskytuje pohodlí, umožňuje sdílet informace v reálném čase a prostoru, ale skrývá nebezpečná a zákeřná místa, pokud uživatel není dostatečně pozorný. Je tedy, podobně jako oheň: "dobrý sluha, ale zlý pán". Většina světových autorů se ve svých výzkumných pracech, které jsou zaměřeny na výzkum v oblasti kybernetické šikany (tzv. kyberšikany) a obraně proti ní, shoduje na nutnosti prevence a šíření osvěty. V naprosto drtivé většině případů jsou však tyto aktivity velmi povrchně zaměřeny na definice jednotlivých kroků, které nezkušený uživatel na Internetu má či nemá provádět bez uvedení do souvislostí a vysvětlení podstaty, proč je třeba se jistým aktivitám vyhnout a naopak, které komunikační kanály a nástroje si zvolit, aby bylo riziko nechtěného výsledku minimalizováno. Tento materiál apeluje na nutnost mezioborového propojení humanitních a technických oborů již na základních a středních školách. Je třeba vysvětlovat problematiku bezpečnosti na Internetu v souvislostech tak, aby nezkušení uživatelé věděli, jaká bude pravděpodobná reakce následovat po provedené akci a především, zda bude pro uživatele takový následek akceptovatelný, to vše bez ohledu na metodu připojení, tj. pomocí pevně instalovaného osobního počítače (z angl. „personal computer", ve zkratce PC) nebo přenosného zařízení (jako mobilní telefon, tablet, notebook apod.)

**Existuje absolutní bezpečnost?**

Nejprve je nutné si uvědomit, že v případě bezpečnosti na Internetu je třeba mluvit o minimalizaci bezpečnostních rizik. Stoprocentní neboli absolutní zabezpečení neexistuje, neboť se jedná o ideální stav, který lze obvykle dosáhnout pouze za předpokladu nepřiměřeně vynaložených zdrojů (ať už v podobě finančních nebo časových). Podobně, jako na ulici člověk musí pořád dávat pozor, aby do někoho nevrazil, nepřejelo ho auto při přecházení, je třeba na Internetu dávat pozor, ať už děláme cokoliv. Zjednodušeně lze tedy říci, že většina kryptografických nástrojů, jež se v současnosti používá pro zabezpečení komunikace na Internetu, je založená na nemožnosti vyzkoušet všechny možnosti v rozumném časovém horizontu (tzv. hrubou silou). S rozvíjejícími se technologickými možnostmi zařízení a systémů, které zpracovávají informace, roste pravděpodobnost, že některé nástroje již nebude možné používat, protože budou snadné utajenou informaci získat nebo kompromitovat (a znemožnit použití daného mechanismu) bez nutnosti vynaložení nepřiměřených zdrojů. Mimoto roste i počet kvalitně vzdělaných expertů (z angl. „hackers"), kteří rozumí podstatě jednotlivých mechanismů natolik, že jsou v nich schopni nalézt chyby (tzv. díry, z angl. „errors" nebo „holes"). Pokud jsou tito odborníci hodní (etičtí, z angl. „white hat hacker"), chybu oznámí výrobci, který, pokud je též etický, chybu opraví obratem a vydá příslušnou aktualizaci (tzv. záplatu, z angl. „patch"). Pokud je odborník zlý (z angl. „black hat hacker"), snaží se chyby využít ve svůj prospěch, aniž by ji výrobci ohlásil (obvykle s cílem se finančně obohatit). Případů, kdy byla objevena nedostatečná úroveň bezpečnosti nebo chyba v původně dobře fungujících systémech, je známo z historie mnoho. Mezi nejvýznamnější z hlediska dopadu na uživatele lze uvést např. šifrovací algoritmus Data Encryption Standard (DES), hashovací algoritmus Message Digest verze 5 (MD5) nebo zabezpečovací mechanismus Wired Equivalent Privacy (WEP) v bezdrátových (WiFi) sítích.

**Co si tedy zapamatovat?**

1. Pro správné chování na Internetu je třeba chápat bezpečnost v souvislostech.
2. Neexistuje stoprocentní bezpečnost (ani na Internetu, ani jinde).
3. Snažíme se tedy o minimalizace rizik spojených s určitou aktivitou (ať už na Internetu nebo jinde).
4. Protože se technologické nástroje stále vyvíjejí, je nutné jednotlivé metody a algoritmy neustále prověřovat (práce příslušných expertů v oboru).
5. Bezpečnost je tedy nikdy nekončící proces, nikoliv ustálený stav.

## Jak ten INTERNET vlastně funguje?

V této sekci se pokusíme vysvětlit technické principy, na nichž stojí dnešní systémy a nástroje používané pro účely komunikace a výměny informací na Internetu. Nebudeme však zabíhat do přílišných detailů, neboť to není účelem a ani zde na to není prostor. Bezhlavé memorování jakýchkoliv pravidel je přežitkem a nevede ke kýženému zapamatování poznatků. Domníváme se proto, že pro zodpovědné chování na Internetu je třeba rozumět elementárním způsobům, jakými jsou informace po Internetu přenášeny, zpracovávány a ukládány. Uživatel pak lépe porozumí pravděpodobným dopadům jednotlivých akcí, které na Internetu uskutečňuje.

##### Model komunikace

V mezinárodní síti Internet komunikují zařízení různého druhu a účelu. Z pohledu uživatele se většinou jedná o osobní počítač (PC), přenosný počítač (notebook/laptop, ultrabook apod.), tablet, mobilní telefon, server apod. Tato zařízení se obvykle nepřipojují přímo k síti Internet, ale přes nebo pomocí dalších (mezilehlých, přístupových či páteřních) zařízení jako např. síťový přepínač (z angl. „switch"), směrovač (z angl. „router"), brána (z angl. „gateway"), přístupový bod technologie WiFi z angl. „access point", ve zkratce AP), firewall apod. Říkejme všem těmto zařízením obecně síťové uzly. Aby si tyto uzly mohly navzájem vyměňovat informace, je pro komunikaci potřeba znát jejich adresu, podobně jako je tomu v případě domů v ulici.

Síťový experti se ve dvacátém století dohodli a navrhli model, který dodržují výrobci síťových uzlů s drobnými úpravami v podstatě dodnes. Tento model byl Mezinárodní standardizační institucí (z angl. „International Standardisation Organisation", ve zkratce ISO) přijat jako reference, na kterou se lze vždy odkázat v případě návrhu síťového uzlu komunikujícího s propojenými otevřenými systémy (z angl. „Open System Interconnection", ve zkratce OSI). Dlužno dodat, že referenční model (ve zkratce RM ISO/OSI) byl původně navržen pro potřeby telekomunikačních sítí, tedy v dobách telefonních ústředen, kdy Internet, jak ho známe dnes, byl ještě v plenkách. Na druhou stranu lze tento sedmivrstvý model vhodně využít pro snazší pochopení, jak zařízení v síti Internet komunikují, kde je možné očekávat úskalí v souvislosti s bezpečností, soukromím apod.

|  |  |  |
| --- | --- | --- |
| **Číslo vrstvy** | **Název vrstvy** | **Datová jednotka** |
| **7** | Aplikační | Data |
| **6** | Prezentační | Data |
| **5** | Relační | Data |
| **4** | Transportní | Segment/Datagram |
| **3** | Síťová | Paket |
| **2** | Spojová (Linková) | Rámec |
| **1** | Fyzická | Bit |

Referenční model ISO/OSI včetně datových jednotek

Veškerá datová komunikace probíhá vždy od horní vrstev směrem k dolním na vysílací straně a v opačném směru na přijímací straně. Poznámka: v rámci síťové komunikace se může síťový uzel chovat jako vysílací a přijímací zařízení zároveň a ve většině případů tomu tak i je. Na vysílací straně se data vyšší vrstvy ve většině případů opatří servisní (služební) informací nižší vrstvy (tzv. záhlavím, někdy hovorově „hlavičkou" z angl. „header") a na přijímací straně je před odebráním tato informace síťovým uzlem příslušně vyhodnocena a zpracována. Až na výjimky, kdy je několik vrstev sloučeno do jedné, komunikuje každá vrstva pouze s vrstvami sousedními (resp. vrstvou sousední). Způsob, jakým bude vyjádřena datová jednotka na úrovni dané vrstvy, určuje tzv. protokol. Obecně může na jedné vrstvě pracovat více protokolů, a to proto, že ne každý protokol lze použít pro libovolný způsob komunikace. Jinými slovy, ne každý protokol lze použít pro ten samý účel.

Jednotlivé vrstvy jsou jednoznačně definovány v příslušném normativním dokumentu. Pro naše potřeby však postačí, pokud porozumíme jejich účelu a základnímu principu. Prostředí Internetu je výhradně digitální, jednotlivé signály tak reprezentují datové jednotky popř. skupiny datových jednotek. Nejjednodušší (základní) datovou jednotkou je jeden bit (označován malým „b"). Bity lze sloučit do osmice zvané oktet (z angl. „octet") neboli bajt (z angl. "byte" označován velkým „B"). Bajty lze dále sdružovat v tisíce bajtů (kilobajty, ve zkratce kB), v milióny bajtů (megabajty, MB), v miliardy bajtů (gigabajty, GB) podobně, jako např. metry v kilometry apod.

Fyzická vrstva představuje reálné (fyzické) prostředí, skrze které jsou jednotlivé bity přenášeny. Takové prostředí může být metalické (drátové), bezdrátové (WiFi nebo mobilní) či optické (vlákno). Podobně, jako je v ulici města adresován dům číslem orientačním a popisným, lze si představit i účel spojové a síťové vrstvy a jejich adres. Na úrovni spojové vrstvy se jedná o adresu řízení přístupu k médiu (z angl. „Media Access Control", ve zkratce MAC), která má, podobně jako číslo orientační, pouze lokální význam, a je dostupná (a zjistitelná) obvykle pouze mezi sousedními zařízeními. Nejčastěji používaným protokolem je Ethernet, jehož adresa je 48bitová. Síťová vrstva má naopak funkci zajištění plné adresovatelnosti v rámci celého Internetu podobně, jako číslo popisné v ulici. Nejčastěji používaným protokolem je Internetový protokol (z angl. „Internet Protocol", ve zkratce IP) a to ve verzi 4 (IPv4), jehož adresa je 32bitová. S rozvojem Internetu narostl počet požadavků na veřejnou adresu IPv4 natolik, že budou brzy vyčerpány do poslední možné. Proto byl nejprve navržen mechanizmus překladu adres (z angl.„Network Address Translation", ve zkratce NAT), kdy se za jednou veřejnou adresou brány či jiného zařízení vybaveného touto funkcí (např. směrovač) "schová" více dalších síťových uzlů. Zařízení ukrytá přímému kontaktu s vnějším světem jsou vybavena adresou neveřejnou, taková adresa může být použita za více branami v Internetu a ostatní zařízení se o ní nedozvědí (pro vnější Internet budou její požadavky vypadat, jakoby pocházely od příslušné brány nebo směrovače). V další fázi byl pak původní IPv4 přepracován na verzi 6 (IPv6), který podporuje 128bitové adresy. Verze 4 a 6 jsou však navzájem nekompatibilní, což znamená, že je nelze použít pro vzájemnou komunikaci. Na druhou stranu je lze používat vedle sebe, takže zařízení má obvykle jednu IPv4 a jednu IPv6 adresu, přičemž přednost má obvykle IPv6.

Čtvrtou vrstvou v pořadí je vrstva transportní, která zajišťuje přenos dat vyšších vrstev (iniciovaných obvykle z aplikační vrstvy) z vysílací na přijímací stranu. Pro rozlišení, která aplikace (program) požaduje z aplikační vrstvy spojení s cílovou stanicí, není tentokrát použita adresa nýbrž číslo tzv. portu (z angl. „port"). Běžně používané aplikace mají čísla portů známá a obvykle i na těchto portech fungují. Poznámka: je na vůli administrátora serveru, na kterém portu bude daná služba identifikovatelná. Je však třeba si uvědomit, že záměna čísla portu může způsobit nedostupnost této služby, pokud o takové změně není uživatel informován, který se bude dotazovat na známém čísle portu. Mezi nejčastěji používané protokoly transportní vrstvy patří Transmission Control Protocol (TCP) a User Datagram Protocol (UDP). První zmíněný slouží pro takové programy aplikační vrstvy, které vyžadují jistotu, že přenášená data byla spolehlivě doručena. Typickými příklady jsou služba World Wide Web (WWW), která umožňuje pomocí protokolu HyperText Transfer Protocol (HTTP) přistupovat na webové stránky nebo služba elektronické pošty (tzv. e-mail). UDP se naopak hodí v případě, kdy se např. posílá přes Internet televizní nebo rádiové vysílání. Nedoručená nebo zpřeházená informace je cílovým uzlem ignorována a uživateli se projeví jako výpadek, který snadno přehlédne, případně toleruje. Výpadek části webové stránky nebo e-mailu by naopak akceptován nebyl.

Vrstva relační umožňuje řízení vytvoření, ukončení a výměnu dat mezi oběma komunikujícími uzly. Nejdůležitějším protokolem této vrstvy je z hlediska bezpečnosti zabezpečení transportní vrstvy (z angl. „Transport Layer Security", ve zkratce TLS, který je následovníkem „Secure Sockets Layer", ve zkratce SSL). Tato vrstva, resp. tyto protokoly této vrstvy, mj. poskytují zabezpečení pro komunikační protokoly aplikační vrstvy (viz dále např. Tab. 2), které byly původně navrženy bez takové vlastnosti. Prezentační vrstva je podpůrná a slouží pro transformaci a přípravu dat mezi aplikační a relační vrstvou a z hlediska bezpečnosti není tak důležitá. Proto si ji dovolíme v tomto výkladu přeskočit a rovnou se zaměřit na vrstvu aplikační, která je uživateli nejblíže.

##### Programy, aplikace, servery

V předcházející části jsme si již uvedli typické příklady a nejznámější protokoly aplikační vrstvy, tedy: HTTP a e-mail, který používá poštovní protokol (z angl. "Post Office Protocol" verze 3, ve zkratce POP3) pro stahování pošty ze serveru do poštovního klienta, tj. programu komunikujícího z poštovním serverem, a jednoduchý poštovní protokol (z angl. "Simple Mail Transfer Protocol", ve zkratce SMTP) pro odesílání pošty. Ani jeden z uvedených protokolů ve své původní podobě nezajišťuje utajení přenášených informací. Jinými slovy, přenášená aplikační data nejsou šifrována, takže je může zachytit a přečíst kdokoliv, kdo má přístup na mezilehlé uzly (např. mezi uživatelským PC a serverem). Z tohoto důvodu byly navrženy jejich zabezpečené varianty (z angl. "secure"), tedy: HTTPS, POP3S a SMTPS, které využívají bezpečnostních mechanizmů protokolů relační vrstvy (např. TLS). Jak jsme si uvedli, každá z těchto služeb se rozlišuje číslem portu, takže prvním vodítkem, zda je komunikace zabezpečená, je změna čísla portu z nešifrované na šifrovanou variantu.

|  |  |
| --- | --- |
| **Protokol** | **Typické (známé)číslo portu** |
| **HTTP** | 80 |
| **HTTPS** | 443 |
| **POP3** | 110 |
| **POP3S** | 995 |
| **SMTP** | 25 |
| **SMTPS** | 465 |
| **IMAP** | 143 |
| **IMAPS** | 993 |

Příklady aplikačních protokolů a jejich přiřazených čísel portů TCP

Na závěr této sekce připomeňme, že data vyšší vrstvy jsou na odesílací straně před předáním nižší vrstvě vždy opatřena příslušným záhlavím, aby bylo přijímací straně jasné, jakým způsobem se s ní pokouší odesílací strana komunikovat. Tento princip se označuje jako zapouzdření (z angl. „encapsulation") nebo zabalení. Na přijímací straně pak probíhá opačný proces rozbalení dat.

Pro názornou představu uvádíme následující příklad: uživatel požaduje zobrazit webovou stránku nejznámějšího celosvětového vyhledávače [www.google.cz](http://www.google.cz/). Aby se toto přání stalo skutečností, spustí si nejprve internetový prohlížeč, což je program nainstalovaný v počítači uživatele, který umožňuje mj. komunikaci pomocí protokolů HTTP a HTTPS s cílovým serverem, přičemž nevyžaduje po uživateli detailní znalost těchto protokolů a usnadňuje tak uživateli práci. Takový program je např. Internet Explorer, Mozilla Firefox, Google Chrome, Opera apod.



Zdroj: Jiří Macich ml., [Webové prohlížeče: současní lídři a jejich historie (1/2)](http://www.root.cz/clanky/webove-prohlizece-soucasni-lidri-a-jejich-historie-1-2/), www.root.cz

Přehled několika různých prohlížečů

Internetový prohlížeč doplňuje do komunikace velmi automaticky čísla portů (80, 443 apod.), použitý protokol (HTTP, HTTPS apod.) a dost často tyto informace v adresním řádků prohlížeče ani nezobrazuje. A jak už to tak bývá, to má své výhody i nevýhody zároveň. Mezi výhody patří zjednodušení dlouhého zápisu adresy stránky serveru. Nevýhodou je však nejasná signalizace směrem k uživateli, zda komunikuje se serverem zabezpečeně či nezabezpečeně. Prohlížeče se snaží odstranit tuto nedokonalost barevným odlišením barvy textu v adresním řádku, ale to je mnohdy spíše matoucí. Některé prohlížeče tyto informace umožňují upravit nastavení tak, aby tyto informace řádně zobrazovaly, některé však nikoliv.



*Rozdíl v přístupu k internetovému obsahu pomocí protokolu HTTP a HTTPS*

Princip zapouzdření tzv. webové komunikace je na odesílací straně následující:

1. uživatelská data pro zobrazení webové stránky jsou opatřena HTTP záhlavím,
2. v případě požadavku na zabezpečení komunikace (HTTPS) jsou opatřena TLS záhlavím,
3. protože protokoly HTTP/HTTPS vyžadují spolehlivé doručení, jsou data opatřena TCP záhlavím,
4. na síťové vrstvě jsou opatřena IP záhlavím (není důležité jakou verzí, ale obě strany musí komunikovat stejnou verzí, neboť jsou vzájemně nekompatibilní)
5. na spojové vrstvě příslušným záhlavím protokolu Ethernet
6. a odeslána na fyzické médium, ať už je metalické, bezdrátové nebo optické.

Přijímací strana data rozbaluje v opačném směru (od 1 směrem k 7), kdy předá požadavek běžícímu serverovému programu (tzv. webovému serveru), který uživateli vrátí požadovanou stránku (pokud taková existuje). Všimněte si, že data jsou mezilehlými zařízeními analyzována pouze do vrstvy, která je pro jejich činnost důležitá. Tím je zajištěna maximální efektivita zpracování všech požadavků, které nejsou zdrženy déle, než je nutné. To však neznamená, že by data nemohla být rozbalena až po aplikační vrstvu, jenom to není nutné. O tomto typu problému ale až později.



*Znázornění klasického zapouzdření od L7 až po L1 a naopak na přijímací straně (včetně mezilehlého PŘEPÍNAČE a SMĚROVAČE)*

**Co si tedy zapamatovat?**

1. Komunikace na Internetu probíhá pomocí protokolů.
2. Protokoly se od sebe liší kromě účelu především vrstvou, na které komunikují.
3. Protokoly se do sebe zapouzdřují (zabalují) na vysílací straně a rozbalují na straně přijímací.
4. Mezi zdrojovým a cílovým komunikujícím uzlem je možné datovou komunikaci v mezilehlých uzlech rozbalit až po aplikační vrstvu, jen to tyto uzly zpravidla nedělají.

**INTERNET pro lidi**

V předcházející sekci jsme si uvedli příklad komunikace s webovým serverem společnosti Google, ve které uživatel požadoval zobrazení stránky [www.google.com](http://www.google.com/). Popsali jsme si způsob, jakým je požadavek sestaven a odeslán cílovému serveru. Jak ale zjistit adresu cílového serveru, která je číselná, když je požadována výše uvedená webová stránka (tj. jméno)? Tomu se budeme věnovat v této části.

**Adresa, jméno, doména**

Připomeňme, že počítače pracují se základní jednotkou jeden bit, který může nabývat pouze dvou hodnot, a to hodnoty nula nebo jedna, odtud binární, a dále, že adresa IP je číslo buďto 32bitové (IPv4) nebo 128bitové (IPv6). Zápis adresy IPv4 má pak formu 32 po sobě jdoucích kombinací nul a jedniček. V případě IPv6 je jich 128. Takový zápis není úplně dobře zapamatovatelný a ani se s ním lidem dobře nepracuje (na rozdíl od počítačů a dalších síťových uzlů). Proto si lidé nejprve vymysleli zjednodušený zápis těchto čísel převedených z původně binární formy do formy v desítkové soustavě, která je jim bližší a srozumitelnější. V případě Internetového protokolu verze 6 je však adresa i tak dlouhá, takže přešli k vyjádření v šestnáctkové soustavě, ale to jsme opět na začátku v řeči nesrozumitelné běžným uživatelům.

Z tohoto důvodu byl lidmi navržen systém doménových jmen (z angl. Domain Name System, ve zkratce DNS), který umožňuje automaticky mapovat, tzn. převádět, IP adresy na jména a zpět. Doménové jméno (doména = oblast, pozn. autora) je hierarchické, takže má přesně danou strukturu. Za poslední tečkou je doména nejvyšší úrovně (z angl. „Top Level Domain", ve zkratce TLD), která zpravidla označuje stát, ve kterém se webový server a stránky na něm provozované nacházejí (např. „cz", „sk", „de" apod.) Existují i další domény nejvyšší úrovně, které se státy nemají nic společného (např. „com", „info", „biz" apod.), princip ale zůstává stejný. Před touto doménou (myšleno zprava doleva) je tečkou oddělená doména první úrovně, která zpravidla vyjadřuje jméno firmy, název služby apod. (např. „google", „seznam" atd.) Všimněte si, že doménová jména jsou psána malými písmeny. Ve skutečnosti však protokol HTTP nerozlišuje velikost písmen. Další úroveň, tj. druhá, obvykle slouží k vyjádření služby, kterou daná společnost poskytuje, takže může existovat doménový záznam např. [www.seznam.cz](http://www.seznam.cz/) pro službu WWW a [email.seznam.cz](http://email.seznam.cz/) pro službu přístupu k elektronické poště.



Hierarchie doménového jména

Doménu první úrovně si za roční poplatek registrují zájemci u příslušné registrační autority (společnosti s právem spravovat vybrané domény nejvyšší úrovně), která má možnost spravovat příslušnou doménu nejvyšší úrovně. Doménu druhé a nižší úrovně (třetí, čtvrté, atd.) si spravují vlastníci příslušné domény první úrovně již sami. Je tedy vždy na vlastníkovi zakoupené domény první úrovně, aby zajistil správně nastavené mapování mezi adresou a jménem u příslušné registrační autority. Služba DNS pak zajistí rozšíření této informace do celého světa, ale to je již nad rámec tohoto kurzu.

**Webová stránka a její kód**

Pokud všechno funguje jak má, uživateli se nakonec skutečně objeví požadovaná webová stránka, se kterou může dále pracovat. Jak ale taková stránka vypadá ve své původní podobě, se dozvíme v této části materiálu.

Aby mohl prohlížeč Internetu zobrazit požadovanou webovou stránku, získá od webového serveru kód webové stránky, který následně interpretuje (přetvoří do grafické podoby). Tentokód je napsán v k tomu navrženém značkovacím jazyce (z angl. HyperText Markup Language, ve zkratce HTML). Jazyk sestává z jednotlivých značek a umožňuje formátovat text to bloků, tabulek, tlustým písmem, kurzívou, upravovat barvy jednotlivých elementů a přidávat odkazy na další stránky (jejich doménová jména). Protože HTML byl původně navržen pro tvorbu neměnných (tzv. statických) webových stránek a neumožňoval začlenit dynamické (animované) elementy (obrázky, videa), byl postupně upravován a spolu s ním vznikly i další jazyky pro snazší práci s těmito objekty jako např. JavaScript, Flash, Java apod. Způsob, jakým interpretují prohlížeče kód těchto jazyků (který se od HTML a mezi nimi navzájem liší), není vždy identický, a vzniká tak prostor pro hledání bezpečnostních chyb, ale o tom až později.

**Co si tedy zapamatovat?**

1. DNS slouží ke snazšímu zapamatování adresních informací cílového serveru.
2. DNS automaticky převádí doménová jména na číselné adresy IP.
3. Doménové jméno je hierarchické s pevně danou strukturou, tj. doména nejvyšší úrovně oddělená tečkou od domény první úrovně, která je oddělená dále tečkou od domény druhé úrovně atd.
4. Kód webové stránky je napsaný jazykem HTML, ale může obsahovat i další kód jazyků (např. JavaScript).

**Služby na INTERNETu**

V předcházejících částech jsme diskutovali asi nejznámější službu vyhledávače společnosti Google, ale obecně je nejen spousty vyhledávačů, ale také dalších služeb umožňujících uživatelům sdílet svoje zážitky pomocí textových služeb, digitálních dokumentů, společenských (tzv. sociálních) síti, diskusních konferencí, fór apod.

**Vyhledávač**

Vyhledávače obecně procházejí kód jednotlivých stránek na Internetu a ukládají si tyto informace do vlastního úložiště (tzv. databáze). Serverů nabízejících svoje služby v oblasti vyhledávání informací je mnoho, v České republice je asi nejznámější Seznam.cz, na Slovensku Zoznam.sk, ve světě pak např. Yahoo.com, Yandex.ru, Bing.com, DuckDuckGo.com atd. Systémy vyhledávače si tyto informace si navíc třídí tak šikovně, že uživatel nemusí hledat přímo stránku, ale stačí zadat dotaz na cokoliv souvisejícího s touto stránkou (tzv. klíčové slovo, z angl. „keyword") a vyhledávač takovou stránku dříve či později ve výsledcích hledání zobrazí. Někdy je třeba zadat klíčových slov více, aby se množina výsledků zmenšila a zjednodušila.

Vyhledávač společnosti Google ale umožňuje mnohem více, a to zobrazit předcházející verze webových stránek, které se v průběhu času (dnů, měsíců i let) vyvíjely a měnily. Tento fakt je třeba si uvědomit, neboť cokoliv jako uživatel na Internetu zveřejním, může být dohledatelné i několik let zpět, a to i v případě, že aktuální podoba dané webové stránky je odlišná. Poznámka: takovouto službu „vyrovnávací paměti" (z angl. „cache") neposkytuje pouze Google, ale i jiné vyhledávače nebo webové stránky k tomu určené. Vymazání informace z minulosti „z Internetu" proto nemusí být snadný úkol, a na to je třeba vždy pamatovat, ať už jako uživatel zveřejňuji cokoliv.

**Elektronická pošta a „kecátka"**

Elektronickou poštu jsme si již popsali z pohledu vrstvového modelu komunikace. Nezměřili jsme se však na způsoby, jakým jsou zprávy (tzv. e-maily, z angl. „e-mails") zpracovávány. Pokud není uživatel dostatečně zkušený, založí si „zdarma" svůj účet u některého z poskytovatelů takové služby. Slovo zdarma je úmyslně v uvozovkách, poněvadž je třeba si uvědomit, jako cenu za tuto službu uživatel platí. Tato cena se závislá na podmínkách, za kterých je daná služba poskytována. Obvykle není vyjádřena v penězích, ale v částečné ztrátě či omezení soukromí. Např. podmínky nejrozšířenější služby Gmail společnosti Google jasně hovoří, že veškeré informace přenášené skrze systémy společnosti Google jsou majetkem této společnosti a budou s nimi také tak nakládáno. V praxi to znamená, že systémy Google prohledávají e-maily a další elektronickou komunikaci (fotky, blogy, hangouts atd.) s cílem získat co nejvíce informací o uživateli, který si dané konto či službu aktivoval, a tyto informace pak může prodávat dalším subjektům (společnostem). Toto neplatí pouze pro Google, ale pro naprostou většinu „zdarma" poskytovaných služeb.

Další službou, která je velmi často poskytována zdarma, je služba „kecátek" (z angl. „chat") pro okamžitou výměnu zpráv (z angl. „instant messaging") s našimi přáteli. Mezi takové služby se řadí např. AIM, ICQ, Skype, již zmíněný Hangouts, Viber, Facebook a mnoho dalších. Obvykle jsou tyto služby mnohem všestrannější, takže nabízejí kromě možnosti diskuse také volání nebo sdílení fotek či videí. Nežli uživatel do těchto sítí zveřejní svoje příspěvky, je třeba si uvědomit, kde budou tyto příspěvky ve své digitální formě uloženy a jak s nimi bude nakládáno, to vše podle příslušných podmínek používání dané služby.

**Mraky sdílených dokumentů, fotek a videí**

Tuto tématiku jsme v podstatě probrali v minulé části. Připomeneme tedy, že vždy je nutné se před vlastní registrací (aktivací) dané služby informovat a prostudovat podmínky používání takové služby. Velmi často totiž taková přistupuje k uloženým informacím jako ke svým a nakládá s nimi podle toho. V poslední době jsou velmi často záznamová zařízení (mobilní telefony, fotoaparáty, videokamery apod.) vybavená možností uložení globální informace o poloze (z angl. „Global Positioning System", ve zkratce GPS), kde byla fotografie pořízena. Tato informace je uložena v rámci tzv. metadat (tj. strukturovaných dat o datech) a obvykle je označována zkratkou Exif (z angl. „Exchangeable Image File Format"). Pokud je taková fotografie umístěna na webové stránce na Internetu a server umí takovou informaci přečíst a zobrazit, může dojít k nechtěnému vyzrazení, kde a kdy byl snímek pořízen.

V poslední době je trend v ukládání digitálních dokumentů (fotek, videí apod.) do tzv. mraků (z angl. „cloud"), které nejsou nic jiného než skupina velkého množství serverů a databázových úložišť vykonávajících jednu a tutéž funkci, ale z jiného kraje světa za účelem efektivního přístupu k těmto informacím z celého světa. Velmi často se pak stává, že tatáž fotografie či video je uloženo v Evropě, USA a Asii, přičemž uživatelům z Evropy je zobrazována informace uložená z evropské části, uživatelům z USA z americké atd. Typickým příkladem takových služeb jsou webové stránky YouTube, Vimeo apod.

**Společenské sítě**

Společenské sítě nebo též sociální sítě (z angl. „social networks") slouží k vytváření profilu registrované osoby, jenž lze sdílet veřejně, částečně nebo pouze s přáteli, ke komunikaci s ostatními členy sítě a vzájemnému sdílení digitálních informací (fotografie, videonahrávky apod.) Někdy může být za sociální síť považováno i diskusní fórum. Mezi typické příklady patří již zmiňovaný Facebook, nebo dále Twitter, Google+, Instagram, Ask.fm, Tumblr, Myspace, LinkedIn a spousty dalších. V České republice můžeme nalézt portály jako lide.cz, spoluzaci.cz, libimseti.cz, atd.

Nebezpečí v těchto sítích je dvojí. První je stejné, jako v ostatních službách, které poskytují služby „zdarma" pouze za cenu částečné (nebo úplné) ztráty soukromí. Druhé je situace, kdy hrozí nebezpečí, že se za mojí osobu bude vydávat někdo jiný. Prvnímu nebezpečí se mohu vyhnout tak, že se do daných sítí vůbec nezaregistruji, nebo do nic sdílím omezené informace, které půjde s mojí osobou těžko spojit. Druhému se vyhýbá těžko, ale vždy je potřeba o problému mluvit s rodiči či učiteli. Problém zcizení identity se netýká pouze dětí či mladistvých. Je to prohřešek proti zákonu především ze světa dospělých a podle toho je třeba s ním nakládat.

**Co si tedy zapamatovat?**

1. Internetových vyhledávačů je spousta a jsou určeny k rychlému vyhledání požadované informace.
2. Internetový vyhledávač a další služby si umějí zapamatovat i několik historických verzí dané webové stránky.
3. Elektronická pošta a další programy pro „pokec" mohou být bezplatné, ale nejsou vždy zdarma. Cena je částečná nebo úplná ztráta soukromí, popř. práv na sdílené materiály.
4. Dokumenty jako fotky a videa lze snadno na internetu sdílet. Nechtíc však může uživatel vyzradit informace, které si původně přál utajit (např. GPS souřadnice fotografie apod.)
5. Podobně jako u vyhledávacích služeb je v rámci společenských (sociálních) sítí potřeba zvážit, co všechno chce v rámci této komunity uživatel sdílet. Obecně lze říci, že čím méně, tím lépe, ale záleží vždy na konkrétní informaci, které je sdílena, neboť i drobná informace může být vodítkem ke spoustě informací jiných a mnohem zajímavějších nejen pro zlomyslné uživatele.

**Jak se chovat na INTERNETu**

Jak jsme na začátku uvedli, nebezpečí se na Internetu vyskytuje v různých podobách, takže je třeba být vždy ostražitý podobně, jako se chováme na ulici. A jaká je odpověď na otázku „Jak se chovat na Internetu?" Překvapivě jednoduchá: „Zodpovědně." V čem taková zodpovědnost spočívá, si uvedeme v následujících odstavcích.

**Podmínky používání**

Drtivá většina stránek definuje svoje podmínky pro používání služeb, které nabízí. Přestože nebývají krátké a jejich čtení není zrovna dvakrát zábava, je nutné si je přečíst, a získat tak jasnou představu o tom, co z nich pro jejich uživatele vyplývá. Pokud něco není jasné, je důležité tuto informaci konzultovat s někým, kdo je zkušenější než my (rodiče, učitelé apod.) V neposlední řadě je také důležité zjistit podmínky pro ukončení registrace (např. zda je vůbec možné zrušit profil, registraci, a co se stane s daty, které registrovaný uživatel sdílel, jestli budou smazány apod.)

**Ochrana osobních údajů**

Mimo podmínek, za který smí registrovaný uživatel danou službu používat, jsou obvykle definovány i způsoby, jakým je nakládáno s uloženými informacemi a především, s osobními údaji uživatelů. I tyto informace je třeba prostudovat, a pokud jsou nejasné, pak je konzultovat se zkušenými osobami (rodiče, učitelé apod.)

**Práce s prohlížečem a aplikacemi**

Většina služeb vyžaduje pro registraci a následné přihlášení tzv. přihlašovací údaje. Obvykle se jedná o uživatelské jméno (nejčastěji je to e-mailová adresa uživatele) a heslo, které musí uživatel vyplnit do příslušných polí v rámci webové stránky nebo aplikace. Pro pohodlí uživatelů mohou být obě tyto informace uloženy v počítači pro další použití. Informace jsou přitom uloženy na definovaném místě v počítači, mobilu či tabletu uživatele. V takovém případě je třeba dbát zvýšené opatrnosti, protože případný škodlivý program (z angl. „malware") může mít o tyto informace zájem. Zpravidla jde o virus nebo červ, který se šíří buďto přílohou e-mailu nebo se stáhne v podobě škodlivého kódu v rámci webové stránky (o jazyce JavaScript, objektu Flash apod. jsme si již říkali dříve).

Jako ochranu proti takovému škodlivému programu lze použít antivirový program, ale ten nemusí vždy fungovat stoprocentně. Proto je třeba v první řadě nevstupovat na podezřelé stránky (většinou nelegální tématika jako např. inzerce stažení placeného programu zdarma apod.) a neotevírat přílohy e-mailů, které přišly od neznámých adresátů, přišly sice od známých adresátů, od kterých jsme takový e-mail vůbec nečekali (lze si ověřit např. telefonicky), anebo znění textu e-mailu není správně česky či nedává česky smysl. Informace o zdrojové e-mailové adrese lze totiž podvrhnout. V případě, že k počítači (nebo mobilu či tabletu) získá přístup někdo jiný, snadno se pak může přihlásit k dané službě (službám) a provádět tam, co se mu zlíbí. Takovou funkci je třeba velmi dobře zvážit, zda ji chceme skutečně mít zapnutou a používat ji.

O relační vrstvě a protokolech šifrujících původně nezabezpečené protokoly aplikační vrstvy jsme si již říkali dříve. Nyní vysvětlíme jejich praktický význam, a to nejlépe na příkladu. Za předpokladu, že se chceme přihlásit k nějaké službě, kde jsme registrováni (nebo ke které se chceme nejprve registrovat), je třeba se ujistit, zda je spojení mezi naším prohlížečem (či jinou aplikací) a cílovým serverem šifrováno pomocí zmíněného protokolu TLS (alternativně jeho předchůdce SSL). Pokud by tomu tak nebylo, budou přihlašovací informace odeslány v tzv. otevřené podobě (pouze pomocí protokolu HTTP, nikoliv HTTPS) a kdokoliv, kdo bude mít přístup k datovému toku mezi naším počítačem a cílovým serverem, si bude moci komunikaci zobrazit, a to včetně našich přihlašovacích údajů. Ochranou je kontrola použití protokolu HTTPS v adresním řádku prohlížeče.

Některé prohlížeče podporují dodatečnou instalaci tzv. zásuvných (nebo rozšiřujících) modulů (z angl. „plugins"). Jedná se o software třetích stran (tedy dalších výrobců) jako např. Adobe Flash, Adobe Reader, Java, ActiveX apod. Tyto moduly rozšiřují funkce prohlížeče a usnadňují uživateli práci. Může se však stát, že je modul špatně napsán, takže umožňuje útočníkovi např. přístup do počítače oběti. To je situace, které se jako uživatelé chceme vyvarovat. Proto je třeba vždy dobře zvážit, zda dané rozšíření skutečně potřebujeme a případně jej nainstalovat na dobu, kdy jej potřebujeme, a pak zase odinstalovat.

Poslední zajímavostí a nebezpečností zároveň v oblasti webových prohlížečů jsou tzv. koláčky (z angl. „cookies"). Jedná se o soubory, do kterých si na dobu určitou ukládají webové stránky pomocné údaje. Pokaždé, když se uživatel vrátí na danou webovou stránku, tento koláček jí odešle. Typicky obsahují obsah nákupního košíku v elektronickém obchodě, ale lze je používat webovými servery (především třetích stran) ke sledování chování uživatelů a zobrazování cílených reklam. To znamená, že se do tohoto souboru uloží např.: co uživatel na stránce otevřel apod. Nejhorší varianta je, že se do těchto souborů mohou uložit i údaje potřebné pro přihlášení uživatele. Pokud je takový soubor odcizen zlomyslným „hackerem", může je využít pro přihlášení a zcizení naší identity. Obranou je vhodné nastavení příslušného webového prohlížeče, aby takové koláčky nedovolil stránkám ukládat, nebo je alespoň smazal, dříve než je program ukončen.

**Podvržené zlomyslné stránky**

Občas se stane, že se někdo snaží napodobit svou webovou stránku tak, aby vypadala jako stránka někoho úplně jiného. Důvod je jednoduchý, nalákat uživatele, aby do této podvržené stránky vložil své přihlašovací údaje. Tím je útočník získá a může se přihlásit na legitimní stránky našimi přihlašovacími údaji. Tomuto chování se říká „rhybaření" (z angl. „phishing"), což je termín vycházející z analogické situace, kdy rybář láká ryby na svou návnadu. Obrana proti tomuto zlomyslnému chování je jednoduchá, neotvírat odkazy z podezřelých e-mailů a vždy kontrolovat, že skutečně přistupujeme pomocí webového prohlížeče na stránku, kterou jsme chtěli (korektní jméno serveru v adresním řádku).

**E-mail vyžadující zaslání přihlašovacích údajů**

Po uživateli nikdo nikdy nebude chtít přihlašovací údaje (jméno a heslo), ať už e-mailem, zprávou SMS nebo po telefonu, aby je zaslal e-mailem, zprávou SMS nebo nadiktoval do telefonu. Pokud ano, jedná se určitě o podvodníka a nejlepší je takovou zprávu smazat. Případně je možné na tuto situaci upozornit rodiče či učitele.

**Co si tedy zapamatovat?**

1. Na Internetu je třeba se vždy chovat zodpovědně. Uvědomit si, že naše akce bude mít nějakou reakci, která může mít malý, ale také sáhodlouhý dopad.
2. Vždy je třeba číst důkladně podmínky, za kterých smí být daná služba používána.
3. Vždy je třeba se důkladně informovat, jakým způsobem je nakládáno s osobními údaji, jak jsou chráněny a kde jsou uloženy.
4. Při práci s prohlížečem a dalšími aplikacemi je třeba zvážit, zda si chceme trochu ulehčit život vyplňováním přihlašovacích údajů, ale budeme riskovat, že je pomocí zlomyslného kódu nebo programu může získat někdo jiný.
5. Dále si vždy ověříme, že stránka odesílá přihlašovací údaje šifrovaně (pomocí HTTPS), jinak riskujeme, že informace zachytí a zneužije někdo jiný.
6. Nakonec se ujistíme, že jsme skutečně otevřeli webovou stránku, kterou jsme chtěli, neboť víme, že existují podvržené zlomyslné stránky, jež se snaží vypadat jako legitimní webové stránky, aby získaly naše přihlašovací údaje.
7. Nikdy nikomu nevyzrazujeme naše přihlašovací údaje přes telefon, e-mailem, SMS zprávou ani žádnou jinou cestou, a to ani počítačovým odborníkům, administrátorům či správcům sítě.

## POZOR! To ještě není všechno...

Jak jsme si dosud ukázali, nebezpečí číhá na Internetu spousta, a to především v případě, že sofistikované a složité programové vybavení a nástroje jako běžní uživatelé používáme bez ohledu na porozumění, jak fungují a co jejich používání obnáší. Zjistili jsme, že je třeba si dávat pozor v mnoha ohledech, abychom zabránili nechtěnému úniku informací a chránili si svoje soukromí v co možná největší míře a minimalizovali rizika spojená se sdílením informací. Nyní víme, že stoprocentní bezpečnost neexistuje, a proto je potřeba vzít do úvahy i faktory, které přímo nemůžeme ovlivnit, ale které se nás mohou velmi citelně zasáhnout.

##### Kyberšikana

Pojem šikana je většinou známý, jedná se o úmyslné jednání proti jedinci či skupině s cílem uškodit či ublížit oběti. Co když jsou ale k páchání takové činnosti zneužity informační a komunikační technologie (ICT), např. mobilní telefony připojené na Internet? Pak se jedná o šikany v kybernetickém prostoru, neboli kyberšikanu.

Kyberšikana může vznikat nevině, jejím cílem nemusí být nutně úmysl ublížení, ale obvykle se z vtipu stane útok. Oproti klasické šikaně není omezená časem ani prostorem a pachatele je mnohem složitější odhalit. V dnešní době však existují nástroje, které umožňují pachatele takového činu vystopovat i zpětně v čase. A přestože to může být nepříjemné, je potřeba takovou činnost včas ohlásit rodičům či učitelům, kteří zjednají nápravu.

Kyberšikana může nabýt různé formy, mohou to být výhrůžné a obtěžující telefonáty nebo textové či obrázkové zprávy (SMS a MMS), rozesílání obtěžujících či dokonce výhrůžných e-mailů, obtěžování nebo vyhrožování ve společenských sítích a diskusích (viz výše), vytváření zesměšňujících webových stránek, zveřejňování fotografií a videonahrávek na Internetu, zneužití přihlašovacích údajů ke změně informací na profilech, které může přejít až ve vydírání.

##### Další formy útoků

V případě zasílání lechtivých, oplzlých až vulgárních zpráv (obrázkových nebo textových) pomocí mobilních telefonů se jedná o tzv. „sexting". Jestliže je oběť pronásledována či jinak špehována v rámci kybernetického prostředí (Internetu), jedná se o tzv. „cyberstalking". Za předpokladu, že se osoba či skupina osob vydává za jinou osobu s cílem navázat přátelský vztah s obětí a vylákat ji k fyzické schůzce, jedná se o tzv. „cybergrooming". Poslední zmíněný je velmi nebezpečný, protože cílem je obvykle sexuální zneužití oběti, v horším případě její únos či jiné „katastrofické scénáře".

##### Jak se bránit

Neustále je nutné nezkušeným uživatelům Internetu zdůrazňovat, že nedůvěra je vždy na místě, a to nejen v informace, které lze na Internetu nalézt, ale především ve virtuální přátele, kteří se v reálném světe vůbec nemusí podobat těm, za které se vydávají. Nesprávné nebo zavádějící informace si lze vždy ověřit u jiných zdrojů. Ověření skutečné totožnosti virtuálního přítele, se kterým se nezkušený uživatel seznámil v rámci kybernetického prostředí, však nemusí být tak jednoduché. Proto je třeba o takových možnostech preventivně mluvit a vysvětlovat dopady, které mohou nastat. Obranou je včasné upozornění na takovou podezřelou aktivitu směrem k rodičům nebo učitelům.

Bohužel si nemalá část nezkušených uživatelů neuvědomuje, že se stává obětí kyberšikany, neboť považují za „normální" nebo „přijatelné" býti filmován, focen a následně zveřejňován na Internetu. Dalším úkolem v prevenci je tedy podat vysvětlení, že toto není normální a každý jedinec má právo na své vlastní soukromí.

Díky obecným technickým poznatkům uvedeným v dřívějších částech tohoto materiálu lze pachatele vystopovat nebo ho dokonce přistihnout při činu. Není to ale jednoduché a mnohem efektivní je být poučený o možnostech, a jak takovýmto kritickým situacím předcházet svým vlastním zodpovědným chováním.