Skripta – teorie, Modul 7
ECDL Core

peoplesource v.o.s.

Co je to internet - **Internet je celosvětový systém navzájem propojených počítačových sítí („síť sítí“)**, ve kterých mezi sebou počítače komunikují pomocí rodiny protokolů TCP/IP. Společným cílem všech lidí využívajících Internet je bezproblémová komunikace (výměna dat).

Nejznámější službou poskytovanou v rámci Internetu je WWW (kombinace textu, grafiky a multimédií propojených hypertextovými odkazy) a e-mail (elektronická pošta), avšak nalezneme v něm i desítky dalších. Laici někdy spojují pojmy WWW a Internet, i když WWW je jen jednou z mnoha služeb, které na Internetu nalezneme. (zdroj: Wikipedia.org, http://cs.wikipedia.org/wiki/Internet)

Internet = „železo“, WWW = obsah

ISP – je poskytovatel připojení k internetu. Bez jeho služeb byste se na síť nedostali (ISp = Internet Service Provider, poskytovatel internetových služeb)

URL – Unique Resource Locator je umístěním zdroje informací na internetu. Také můžeme říci, že URL je internetová adresa. URL stránek společnosti Peoplesource je http://www.peoplesource.cz , pokud bychom hledali soubor sylabus.pdf, který by se nacházel na stránkách Peoplesource, byla by adresa http://www.peoplesource.cz/sylabus.pdf, tj. by přesně odkazovala na ten který soubor.

Hyperlink – je vlastně proklik. Nebo také odkaz. Když kliknete na internetu na odkaz, zavede vás tento na jinou stránku, nebo na jiný dokument. Internetové stránky jsou takových odkazů plné. Odkaz zpravidla poznáme tak, že je podržený a že reaguje na kliknutí levým tlačítkem myši (vit také minulý odstavec – http://www.peoplesource.cz/)

Struktura internetové adresy: Máme před sebou internetovou adresu společnosti Peoplesource
(1) (2) (3) (4)
http://www.peoplesource.cz

Ta je rozdělená na 4 části – začněme od konce – čtyřka, to takzvaná národní doména, nebo také doména prvního stupně. V této adrese ukazuje, že firma Peoplesource působí v české republice (CZ). Naši sousedé mají domény SK, HU, DE, AT a PL. Evropská unie má doménu EU.

Krom těchto národních domén existují také speciální domény vyjadřující účel, pro který byla webová stránka zřízena – například COM pro komerci, BIZ pro byzys, ORG pro neziskové organizace, NET pro internetové služby, INFO pro informační stránky apod. Rozdělení je jen orientační, v současnosti si může každý registrovat doménu, jakou uzná za vhodné.

Trojka je doména druhého řádu, neboli doménové jméno – tato doména vyjadřuje to, co na webu najdeme. V adrese peoplesource.cz ukazuje doména druhého řádu, že se jedná o web společnosti Peoplesource.

Domény nejvyššího stupně se neudělují individuálním subjektům, jsou určeny pouze k rozlišení státu či skupiny subjektů, např. domény „.cz“, „.net“, „.org“. Domény druhého stupně registrují k tomu určení registrátoři. Domény třetího a dalšího stupně si může libovolně zřídit vlastník domény druhého stupně a není třeba je nikde registrovat. (epravo.cz)

Dvojka je výše zmíněná doména třetího řádu. Tato doména slouží zejména k navigaci po rozsáhlých webech. Například, pokud chceme využít službu google mail od vyhledávače google, zadáme adresu http://mail.google.com a google nás přesměruje do mailu. Podobně, pokud chceme využít slovník,

který google nabízí, napíšeme http://translate.google.com a využijeme slovník. S doménami třetího řádu se setkáváme také na serverech, které nám umožňují zdarma vkládat webové prezentace. Kupříkladu stránka http://janmika.sweb.cz bude adresa stránky uživatele janmika na serveru sweb.cz.

A, konečně, jednička (http://) odkazuje na to, že se jedná o přenos hypertextu – hyper text transfer protocol. Pokud by bylo v adrese uvedeno https://, znamenalo by to, že se jedná o zabezpečený přenos dat (ten používáte například u internetového bankovnictví).

Pokud chceme procházet WEB (www), potřebujeme k tomu specializovaný program – internetový prohlížeč. V současnosti lidé využívají k přístupu na síť prohlížeče internet explorer, mozilla firefox, safari opera a google chrome. Prohlížečů existuje celá řada, tyto jsou však nejpoužívanější)

Obrázek 1, loga nejužívanějších browserů

RSS neboli really simple syndication (česky možno přeložit jako „opravdu jednoduché shromažďování“). Technologie RSS umožňuje uživatelům Internetu přihlásit se k odběru novinek z webu, který nabízí RSS zdroj (RSS feed, též RSS kanál, RSS channel). Tento zdroj se většinou vyskytuje na stránkách, kde se obsah mění a přidává velmi často (například zpravodajské servery).

Původně tento formát sloužil pouze k předávání aktuálních novinek mezi jednotlivými servery, které takto velmi jednoduše mohly odkazovat na aktuální články na jiných serverech.

Podcast může být příspěvek, který autor celý namluvil a převedl do MP3. Poslouchání takového zápisku je pro návštěvníka webu zajímavé, protože slyší skutečný hlas autora textu. Namlouvání podcastu moderátorem či autorem textu je náročné na čas. Podcast také může namlouvat profesionální moderátor.

Druhou možností je využití automatické čtečky, která zápisek automaticky předčítá či převádí do zvukové podoby. Touto čtečkou je například Doppler či iPodder. Hlasovou čtečku si uživatel nainstaluje na svůj počítač a používá na webech, které navštěvuje.

Třetím způsobem je převádění textových příspěvků do zvukového formátu pomocí software. Jedním z řešení je otevřený software Epos. Ten nabízí on-line demo, kde si autor může nechat vygenerovat z textu zvukový soubor (WAV). (zdroj: http://cs.wikipedia.org/wiki/Podcast)

Digitální certifikát webové stránky: SSL je protokol, který zajišťuje šifrování přenášených dat a autentizaci serveru pomocí digitálních certifikátů. To, že jsme připojení na webové stránky zabezpečené pomocí SSL, poznáme podle adresy stránky, která obsahuje navíc písmeno „s“, např. https://www.peoplesource.cz/ nebo podle upozornění prohlížeče.

Jakmile je certifikát na stránky nainstalovaný, zobrazí se v prohlížeči WWW stránek symbol zámečku.

Obrázek 2, Zabezpečená adresa

Digitální podpis: umožňuje ověřit, že zprávu podepsal vlastník odpovídajícího soukromého klíče. To samo o sobě ovšem nijak neidentifikuje skutečnou osobu, která daný klíč vlastní. A právě digitální certifikát je tím instrumentem, který umožňuje spolehlivě identifikovat skutečného odesilatele zprávy.

Abychom mohli podpisu opravdu důvěřovat, musí certifikát vydávat nějaký třetí, nezávislý subjekt. Tímto subjektem je takzvaná certifikační autorita (v zákoně 227/2000 Sb. o elektronickém podpisu se nazývá poskytovatel certifikačních služeb). Vydáním certifikátu certifikační autorita stvrzuje, že subjekt, kterému byl certifikát vydán, skutečně vlastní daný pár klíčů. Přirozeně certifikační autorita musí být dostatečně důvěryhodná organizace, protože jí důvěřují obě komunikující strany. Certifikát by se s trochou fantazie dal přirovnat k občanskému průkazu. Občanský průkaz vlastně spojuje identifikační údaje s jedinečným identifikátorem konkrétní osoby, kterým je v tomto případě její podoba (reprezentovaná fotografií). V případě certifikátu je tímto identifikátorem veřejný klíč.

Na internetu číhá celá řada hrozeb – viry, tzv. spyware, adware. Této „havěti“ se souhrnně říká „malware“ – tj. špatný software.

Jako virus se v oblasti počítačové bezpečnosti označuje program, který se dokáže sám šířit bez vědomí uživatele. Pro množení se vkládá do jiných spustitelných souborů či dokumentů. Takový program se tedy chová obdobně jako biologický virus, který se šíří vkládáním svého kódu do živých buněk. V souladu s touto analogií se někdy procesu šíření viru říká nakažení či infekce a napadenému souboru hostitel. Viry jsou jen jedním z druhů tzv. malwaru, zákeřného softwaru. V obecném smyslu se jako viry (nesprávně) označují i např. červi a jiné druhy malwaru.

Zatímco některé viry mohou být cíleně ničivé (např. mazat soubory na disku), mnoho jiných virů je relativně neškodných popřípadě pouze obtěžujících. U některých virů se ničivý kód spouští až se zpožděním (např. v určité datum či po nakažení určitého počtu jiných hostitelů), což se někdy označuje jako (logická) bomba. Nejdůležitějším negativním důsledkem šíření virů je však samotný fakt jejich reprodukce, která zatěžuje počítačové systémy a plýtvá jejich zdroji. Některé viry mohou být takzvaně polymorfní (každý jeho „potomek“ se odlišuje od svého „rodiče“). Viry se na rozdíl od červů samy šířit nemohou. (wikipedie)

Spyware je program, který využívá internetu k odesílání dat z počítače bez vědomí jeho uživatele. Někteří autoři spyware se hájí, že jejich program odesílá pouze data typu přehled navštívených stránek či nainstalovaných programů za účelem zjištění potřeb nebo zájmů uživatele a tyto informace využít pro cílenou reklamu. Existují ale i spyware odesílající hesla a čísla kreditních karet nebo spyware fungující jako zadní vrátka. Protože lze jen těžko poznat, do které skupiny program patří, a vzhledem k postoji k reklamě řada uživatelů nesouhlasí s existencí a legálností jakéhokoliv spyware.

Adware (advertising-supported software) je označení pro produkty znepříjemňující práci nějakou reklamní aplikací. Ty mohou mít různou úroveň agresivity - od běžných bannerů až po neustále vyskakující pop-up okna nebo ikony v oznamovací oblasti. Další nepříjemnou věcí je např. změna domovské stránky v Windows Internet Exploreru, aniž by o to uživatel měl zájem.

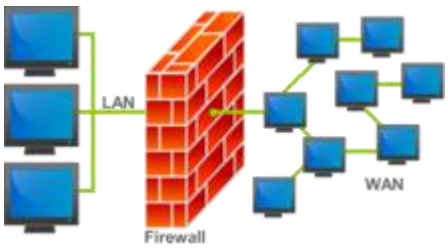
Většinou ale nejsou přímo nebezpečné jako spyware a jsou spojeny s nějakým programem, který je freeware. To se dělá z důvodu toho, že díky těmto reklamám mohou vývojáři financovat dál svůj program. Nebo když se jedné o placený produkt, může se díky těmto reklamám prodávat program se slevou. Nějaký adware je taky shareware, ale není to totéž. Rozdíl mezi adware a shareware je ten, že u adware je reklama podporovaná. Některé produkty nabízejí uživateli možnost odstranění reklam po zaplacení.

Spousta lidí si plete pojmy spyware a adware. Adware velmi často využívá výsledků, které dokázal vyprodukovat spyware, ale není na něm závislý. Adware se instaluje do počítače za souhlasu uživatele. Uživateli je při instalaci hlášeno, že program obsahuje malware a sám má možnost se rozhodnout jestli s tím souhlasí a bude dál pokračovat v instalaci, nebo ne. To je díky licenčnímu ujednání “EULA“ (End User License Agreement). Naproti tomu spyware se instaluje do počítače bez vědomí a souhlasu uživatele. Někdy program, který je použit jako reklamní podpora, je spyware - tedy adware instaluje spyware, často se zastíráním detailů činnosti tohoto spyware.

Programy obsahující adware na rozdíl od spyware neshromažďují tajně informace a neodesílají je přes internet bez souhlasu uživatele.

Této havěti se zbavíte tak, že budete mít v počítači aktivní a denně aktualizovaný program, který proti těmto prográmkům zakročí.

Jmenujme snad jen AVG, Avast, Nod32 pro viry nebo Spybot – search and destroy pro spy- a adware. (www.avg.cz, www.avast.cz, www.nod32.cz, www.safer-networking.org)



Pokud chceme mít seznam „pomocníků“ kompletní, nemůžeme zapomenout na firewall (ang. Protipožární zeď). Je to vlastně síťové zařízení, které slouží k řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení. Zjednodušeně se dá říct, že slouží jako kontrolní bod, který definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje.

Obrázek 3, Firewall