1. Internet jako základní informační médium

Internet je globální sítí spojující miliony počítačů. Více než 100 zemí světa mohou navzájem mezi sebou vyměnovat data, zprávy a názory. Na rozdíl od online služeb, které jsou centrálně kontrolovány, je Internet designován jako decentralizovaná síť. Každý Internetový počítač, tzv. „*host*“, je nezávislý. Ti kdo s ním pracují si mohou vybrat, které Internetové služby užívat a které lokální služby poskytnout globální Internetové komunitě. Přístup k službám Internetu poskytují tzv. Internet Service Providers (ISP). Internet je síť využívající protokoly TPC/IP a přepojování paketů (viz dále).

Služby, které Internet poskytuje:

a) www = world wide web

Je definován jako systém internetových serverů, který podporuje speciálně formátované dokumenty. Tyto dokumenty jsou formátovány v jazyce nazvaném HTML (**Hyper Text Markup Language**), který podporuje hypertextové odkazy na jiné dokumenty stejně jako na grafiku, audio, nebo video soubory. Ne všechny internetové servery jsou však součástí WWW. Aplikace zvané web browsery jsou určeny ke snadnému přístupu na www, nejpopulárnějšími jsou MS Internet Explorer (Exploder☺)
A druhým nejpopulárnějším je dvojice Mozilla/Netscape běžící dnes na podobném jádru. Mezi další známé patří např. Opera.
World Wide Web není synonymem Internetu, www je jen jednou z jeho služeb. WWW využívá protokolu ***HyperText Transfer Protocol*** **(http)**
Tvorba webových stránek – pomocí jazyka HTML – instituce pečující o vývoj standardů – www.w3c.org (World Wide Web Consortium).

b) e-mail = electronic mail

Lze definovat jako transmisi zpráv přes komunikační sítě. Většina počítačových sítí a počítačů má nějaký e-mail systém. Některé jsou omezeny na 1 počítač nebo síť, ale jiné mají brány do jiných počítačových systémů, umožňují uživatelům posílat elektronickou poštu odkudkoli na světě (tzv. web-mail). E-mail je rychlý, flexibilní, spolehlivý ale mnohdy problematický v obchodním styku a z bezpečnostního hlediska. Z počátku byly e-mailové zprávy neformátované, dnes existuje množství programů, které umožňují pokročilé formátování včetně web-mailu (jazyk html). Pro přijímání pošty se užívá FTP a pro odesílání ***SMTP (Simple Mail Transfer Protocol)***, zpráva může být obdržena e-mailovým klientem (programem) za použití POP (Post Office Protocol) nebo IMAP (Internet Message Access Protocol). SMTP je hlavně využíván k posílání zpráv z programu na mailových server. To je ten důvod pro specifikaci obou – POP i IMAP serveru a SMTP serveru když uživatel konfiguruje svoji e-mailovou aplikaci.
POP – slouží ke stažení resp. přenesení mailu z mailového serveru. Existovaly dvě verze – POP2 se stala standardem v pol. 80. let a vyžaduje SMTP, novější verze POP3 může být použita i bez něj.
IMAP je novější. IMAP4 je podobný POP3 ale podporuje další prvky. Lze hledat maily podle klíčových slov zatímco jsou tyto zprávy stále na serveru. Lze si tedy zvolit zprávy, které se stáhnou do počítače. IMAP vytvořila Standfordská univerzita v roce 1986.

c) ftp = File Transfer Protocol,

Je to protokol, využívaný pro výměnu souborů. FTP pracuje na stejném principu jako **HTTP pro transfer *webových stránek*** od serveru k uživatelově browseru a ***SMTP*** **k transferu elektronické pošty**. FTP používá Internetové protokoly TCP/IP, které umožňují přenos dat.

FTP je běžně používán k stahování souborů ze serveru nebo k nahrávání souborů na server (popř. nahrání webové stránky na server).

d) Telnet
Je obecně terminálový emulační program, pro TCP/IP sítě jako Internet. Připojuje PC k serveru na síti. Umožňuje ovládat server a komunikovat s jinými servery na síti. Je potřeba zadat svoje uživatelské jméno a heslo. Umožňuje dálkově ovládat webové servery.

e) Gopher
Systém, který datově přeměňuje WWW pro organizaci a zobrazení souborů na Internetových serverech. Gopher server zobrazuje svůj obsah jako hierarchicky strukturovaný seznam souborů. S nadvládou Webu bylo množství gopherových databází přeměněno na Webové stránky, které jsou snadněji zpřístupněné pomocí webových „hledacích motorů“. Gopher byl vytvořen Minesotskou univerzitou, dva systémy – Veronica a Jughead umožňují hledat zdroje uložené v Gopher systémech. Používá se už velmi málo.

f) USENET
Celosvětový, do kterého lze vstupovat prostřednictvím Internetu a prostřednictvím mnoha online služeb. USENET obsahuje více než 14000 diskusních fór, zvaných newsgroups, které pokrývají každou představitelnou skupinu zájmů. Je používaný denně miliony lidí na celém světě. Soudobá jednička internetových vyhledávačů, server Google, vytvořila pro USENET webové rozhraní umožňující diskusní skupiny číst a přispívat do nich. Navíc ke konci minulého roku server Google oznámil, že začlenil do svého archivu asi 700 milionů příspěvků, směrovaných od května 1981 do 35 tisíc diskusních skupin USENET (lze je najít na stránce www.google.com - skupiny).
V roce 1979 propojili tři studenti univerzit v Severní Karolině počítače "duke", "unc" a"phs" a zahájili na nich prvopočáteční provoz diskusních skupin USENET. Rozvíjející se provoz probíhal pouze v unixovém prostředí a teprve od roku 1986 se začal rozšiřovat po Internetu a nabývat na popularitě.

Encyklopedie Webopedia
http://www.webopedia.com

Internet Society
http://www.isoc.org

Trocha historie fungování internetu

Rozhodující význam pro sítě s přepojováním paketů[1] měl vývoj sady protokolů **TCP/IP**. Hlavními tvůrci této sady byli **Vinton Cerf** a **Robert Kahn**. Na tvorbě, která byla zahájena již v roce 1973, se podílela i řada dalších osobností. Prvé testy se začaly provádět v roce **1975**. V roce **1977** proběhla demonstrace práce sítě **ARPANET** pod řízením internetových protokolů.

Motivem tvorby nových protokolů byla především reálná perspektiva propojovat počítačové sítě mezi sebou. A to i sítě různých architektur. Na počátku sedmdesátých let minulého století

[1] Paket je část zprávy posílané přes síť s přepojováním paketů. Paket obsahuje adresu – místo určení podle dat. V IP sítích jsou pakety nazývány často datagramy. Zprávy jsou rozděleny na pakety před tím, než jsou poslány. Každý paket je odeslán individuálně a může se k cíli dostat dokonce různými způsoby. Jakmile všechny pakety dosáhnou cíle, jsou znovu sestaveny do původní zprávy.

se totiž objevily další LAN (Ethernet, radiové a satelitní paketové sítě) a na významu nabyl pojem internet, chápaný jako síť počítačových sítí. Pro propojení dvou počítačových sítí pracujících dle různých protokolů se stal klíčovým pojmem **gateway**, počítač tvořící rozhraní mezi oběma sítěmi. Toto rozhraní převádělo datový tok z řízení protokolů výchozí sítě na datový tok řízený protokoly cílové sítě.
Klasickým případem byl gateway pro předávání elektronické pošty. Elektronický dopis se adresoval na vhodné síťové rozhraní, které vyhodnotilo část specifikující adresu v druhé síti, provedlo potřebné transformace a dopis odeslalo na určenou adresu. Díky tomuto řešení bylo možné například posílat později elektronické dopisy z Internetu do komerční počítačové sítě **CompuServe**, ve které mělo pronajatu schránku elektronické pošty například i naše velvyslanectví v USA Jeho adresa byla 72360,544, a proto stačilo poslat dopis na příslušný gateway, tedy na internetovou adresu 72360.544@compuserve.com. **Než sada TCP/IP zvítězila** a sítě odlišné architektury přešly na internetovou architekturu, bylo možné s nimi vést analogickým způsobem komunikaci prostřednictvím elektronické pošty.

Základním novým protokolem byl **TCP (Transmission Control Protocol)**, který v roce **1978** autoři rozdělili na dva, na vlastní **TCP** a na **IP (Internet Protocol)**. Do sady mezi hlavní internetové protokoly byl zařazen ještě **UDP (User Datagram Protocol)** a **ICMP (Internet Control Message Protocol)**. O dalších se nebudeme zmiňovat, protože k celkovému pochopení činnosti Internetu, sítě pracující dle TCP/IP, stačí porozumět uvedeným protokolům.

- **Protokol IP** specifikuje formáty paketů - datagramů, zahrnuje internetové adresní schéma (IP adresy) a zabývá se přenosem paketů k určenému hostitelskému systému. Původní verze předpokládala internetový adresní prostor o rozsahu 32 bitů, tedy adresy pro zhruba čtyři miliardy počítačů. Vývoj ukázal, že tento prostor nestačí a že je třeba adresní prostor Internetu rozšířit. Nová experimentální verze IP tento prostor rozšiřuje na 128 bitů a dovoluje adresovat neskutečně velké množství počítačů.

- **Protokol TCP** umožňuje vytvořit mezi dvěma hostitelskými systémy oboustranné propojení garantující bezchybný přenos posloupnosti paketů v tomtéž pořadí, v jakém byly vyslány. **UDP** pracuje nad protokolem IP podobně jako TCP. Je vybaven slabším mechanizmem pro zotavení z chyb, zato jednodušším způsobem vysílá a přijímá pakety přes síť. Obvykle se používá pro posílání stejného paketu většímu množství příjemců (broadcasting). **ICMP** se zabývá pakety obsahujícími chybová, příkazová nebo informační data. Tak například program **PING**, testující průchodnost propojení k danému cíli, využívá tento protokol.

Plné posvěcení dostaly protokoly **TCP/IP** v roce **1983**, kdy **se staly oficiálními protokoly sítě ARPANET**. O rok později byl zaveden **DNS (Domain Name System)**, který ustavil pro internetové počítače hierarchicky organizovaná doménová jména a vzájemnou konverzi mezi IP adresami a doménovými jmény. Bylo definováno šest velkých domén nejvyšší úrovně: *EDU* (education), *GOV* (government), *MIL* (military), *COM* (commercial), *ORG* (organization) a *NET* (network resources). Tato skupina byla rozšířena i o národní domény. Pro USA byla zavedena doména *US*.

Poznámka - co je to URL?
Zkratka pro Uniform Resource Locator, což je globální adresa dokumentů nebo jiných zdrojů na www. První část adresy indikuje, který protokol využívá, a druhá část specifikuje **IP adresu** nebo **název domény**, kde je zdroj umístěn. **Domain Name System (DNS) je**

Internetovou službou, která překládá názvy domén překládá do IP adres[2]. Názvy domén jsou snadněji zapamatovatelné, avšak Internet je založen IP adresách. Pokaždé, když uživatel zadá jméno domény, musí DNS přeložit toto jméno do odpovídající IP adresy (např. 198.105.232.4). DNS systém je fakticky svou vlastní sítí. Pokud jeden DNS server neví, jak přeložit doménu, zeptá se jiného, a tak dále, dokud není navrácena správná IP adresa.

Začátek osmdesátých let byl ve znamení zrodu dalších počítačových sítí pracujících nezávisle na síti ARPANET. V roce **1981** vznikla síť **BITNET** (Because It's Time NETwork), která byla postavena na bázi počítačů firmy IBM. Stala se rychle velmi populární, zejména na amerických vysokých školách. Brzy se rozšířila i mimo hranice USA. Vedle služeb elektronické pošty a přenosu souborů poskytovala také služby pro organizaci a provoz elektronických konferencí (mailing lists). V roce **1984** vznikla v Evropě sestra sítě BITNET, síť **EARN**. V roce **1979** byl zahájen prvopočáteční provoz diskusních skupin **USENET** (viz výše), který se začal rozvíjet na platformě UNIX, v roce **1986** pak na Internetu.

Výhodou, se kterou tento systém vítězil nad elektronickými konferencemi bylo to, že příspěvky byly uživateli přístupné pouze na specializovaných serverech, osvobozovalo jeho e-mailovou schránku od eventuální nepřehledné a nezvládnutelné záplavy informací. Speciální šíření proudu diskusních příspěvků se navíc ukazovalo z hlediska tehdejších málo výkonných spojů jako velmi rozumné. Bohužel uživatel potřeboval pro přístup k USENET specializovaný software, a pokud promeškal příjem některého příspěvku, tak se k němu zpravidla po určité době již nedostal. V USENET se archivovalo velmi zřídka a pokud ano, tak pro uživatele málo přívětivým způsobem.

V roce **1982** byla vytvořena síť **EUnet (European UNIX Network)** zabezpečující elektronickou poštu a distribuci diskusních skupin USENET. Její původní konektivita zahrnovala počítače v Holandsku, Dánsku, Švédsku a ve Velké Británii.

Rozhodující význam pro další vývoj Internetu a jeho vítězství nad ostatními sítěmi mělo **vytvoření páteřní sítě NSFNET severoamerického Internetu v roce 1986**. NSFNET byla převážně sponzorována vládní agenturou **NSF (National Science Foundation** – www.nsf.gov). NSFNET propojovala zpočátku pouze několik amerických superpočítačů, později sloužila k propojení vznikajících amerických národních a lokálních počítačových sítí včetně sítí mezinárodních. Podmínkou využívání služeb NSFNET byl nekomerční provoz připojených sítí. Ke konci roku **1990** propojovala NSFNET již přes 300 tisíc počítačů. Původní páteřní rychlost 56 Kb/sec byla v roce 1988 zvýšena na rychlost 1,544 Mbps (T1), v roce 1991 pak na 44,736 Mbps (T3).

Vítězná cesta TCP/IP - Vladimír Vrabec
http://www.lupa.cz/clanek.php3?show=2467

[2] Existuje i služba WHOIS, která slouží uživateli ke zjištění, jaké doménové jméno se skrývá pod určitou IP adresou (využívá se např. pro vyhledávání původců či zprostředkovatelů hackerského útoku).

Timetable

1948 – matematická teorie komunikace
1958 – první křemíkový čip
1962 – představena počítačová síť
1964 – vynalezeno přepojování paketů
1965 – vynalezen Hypertext
1969 – vznik ARPANETu
1972 – vytvořen protokol TCP/IP
1984 – vznik názvu Internet, Internet začíná pracovat na TCP/IP
1989 – vytvořen world wide web
1993 – vznik prvního prohlížeče – Mosaic (předchůdce Netscape Communicatoru)
1995 – začíná věk eCommerce

Růstové trendy Internetu

- 1977: 111 hosts on Internet
- 1981: 213 hosts
- 1983: 562 hosts
- 1984: 1,000 hosts
- 1986: 5,000 hosts
- 1987: 10,000 hosts
- 1989: 100,000 hosts
- 1992: 1,000,000 hosts
- 2001: 150 – 175 million hosts
- 2002: over 200 million hosts
- By 2010, about 80% of the planet will be on the Internet

V březnu 2001

Přes 115 mil. počítačů
Přes 407 mil. uživatelů
218 z 246 zemí světa přístup k Internetu
31 mil. domén

Přibližně v září 2002 Internet dosáhl dvou důležitých milníků:
200 mil. IP počítačů[3]
840 mil. uživatelů
Zdroj: Netsizer.com

Internet Society
http://www.isoc.org

[3] Je zřejmé, že jen zlomek IP adres má své doménové jméno

Bezpečnost Internetu

Bezpečnost Internetu a bezpečnost práce na Internetu je stále více sledovanou oblastí, s růstem naší závislosti rostou požadavky na **spolehlivost** a **bezpečnost**. Naším přáním je, aby se veškerá data, dostala do rukou pouze těm, kterým jsou určena, a že všechny provedené transakce jsou směrovány vůči těm, kterým to zamýšlíme.

Internet si můžeme představit jako řetěz, jehož síla je determinována silou jeho nejslabšího článku, takto musíme chápat schopnost Internetu bránit se náhodným i záměrným chybám. Napadení počítače či skupiny počítačů je vždy důsledkem nějaké chyby: buď **programové** nebo **lidské** (z abstraktního hlediska to je vždy chyba uživatele, programátora nebo lidské selhání těch, kteří zákeřný kód vypustili na síť).

Na jedné straně *„pevnosti řetězu“* stojí **páteř Internetu**, tvořená spojovacími linkami a směrovači, s vysoce robustními vlastnostmi. Páteř je pod trvalým dohledem kvalifikovaných odborníků, kteří jsou schopni rychle zareagovat na každou nestandardní situaci. Na druhé straně *„pevnosti řetězu“* stojí koncové prvky sítě, tvořené servery a především uživatelskými stanicemi. Kvalifikační úroveň je velmi odlišná, což výrazně ovlivňuje rychlost a adekvátnost případné reakce. Internet sám je vysoce heterogenní – jedná se o Síť sítí, a liší se i kvalita zabezpečení jednotlivých sítí.

Největší ohrožení **spolehlivosti** i **bezpečnosti** Internetu spočívá v jeho dostupnosti a rozšíření a dále v prakticky nulové ceně přenosu informací po již vytvořené infrastruktuře. Rozšíření s sebou nese anonymitu – kriminální činnosti je snáze provozovatelná ve velkoměstě než na vesnici. Určitá **anonymita** je sice pozitivní vlastností Internetu a je v centru pozornosti skupin zasazujících se za ochranu soukromí, na druhé straně je výhodným prostředím pro nežádoucí až nelegální činnost. Anonymita však s sebou nese i pocit beztrestnosti.

Snadnost anonymního pohybu po Internetu a bezvýznamnost geografické vzdálenosti, zapojení obrovského množství zařízení, která jsou v mnoha ohledech identická - vysoká pravděpodobnost, že jeden klíč bude pasovat do více zámků – kvůli těmto faktům je těžké toto prostředí udržet bezpečné a spolehlivé. **Konkrétní počítač, připojený do Internetu, je vystaven možnému útoku z velkého virtuálního neznáma – udává se, že v mnoha sítích v USA se doba od připojení nového počítače na Internet do příchodu prvního „návštěvníka“ pohybuje v desítkách minut. V ČR je tato doba podstatně delší, ale můžete spolehlivě počítat s tím, že do cca 5 hodin je i Váš počítač „objeven“ a „oťukán“.** Růst bezpečnostních incidentů má i svou technologickou podstatu, která spočívá v rostoucím počtu kopií de facto identického programového vybavení počítačů i aktivních prvků sítě. Nejvíce problémů mají uživatelé OS od firmy Microsoft, což není jen důsledek kvality vývoje, kdy se OS vyvíjel původně pro nepřipojené počítače, ale zejména důsledek největšího počtu uživatelů, kteří zároveň patří mezi nejméně poučené. Skuliny existují i v jiných OS, ty ale nejsou tak rozšířené a jejich uživatelé většinou patří mezi ty informovanější (Linux).

Luděk Matyska – Bezpečnost na Internetu (Matyska L., ÚVT, a FI MU – pdf na www.fi.muni.cz)

Bezpečnostní historie Internetu a budoucnost

- Internet původně vzniknul jako vojenský experiment (ve formě zárodečné sítě jménem ARPAnet, ke které se později připojovaly daší sítě, až se postupně zrodil dnešní Internet).
- Cílem tohoto experimentu bylo ověřit možnost vybudování takové sítě, která by dokázala přežít i atomový úder nepřítele, a její nezasažené části dokázaly alespoň nějak rozumně fungovat.
- Velká robustnost a absence centrálního prvku pak zůstala Internetu až do dnešních dnů, a právě díky těmto vlastnostem Internet dokáže fungovat i v situaci, kdy některé jeho dílčí části mají problémy a jsou mimo provoz.
- Z pohledu bezpečnosti je ale důležité, že **při volbě celé koncepce budoucího Internetu nebyl nastolen explicitní požadavek na výraznější zabezpečení** - v době kdy už bouchají bomby by nějaké utajování už stejně nebylo k ničemu. **Proto se budoucí Internet zrodil jako síť bez zabudovaných mechanismů zabezpečení.**
- Konkrétním projevem bylo například to, že **přenosové mechanismy** používané v rámci Internetu (tj. zejména protokol IP na úrovni síťové vrstvy a protokoly transportní vrstvy) **se samy nesnaží jakkoli šifrovat, kódovat či jinak zabezpečovat přenášená data proti neoprávněnému odposlechu.**
- S postupem času pak začal Internet přecházet více a více do rukou akademické sféry, která nakonec (kolem roku 1986) převzala od vojáků i financování páteřní části Internetu. Ani akademická sféra však neměla výraznější požadavky na zvýšení míry bezpečnosti Internetu, resp. na zabudování potřebných zabezpečovacích mechanismů do protokolů TCP/IP.
- Po převzetí Internetu v roce 1990 komerční sférou, se výrazně zvýšily požadavky na míru bezpečnosti. Stejně tak se výrazně zvětšila i schopnost komerční sféry investovat potřebné finanční prostředky do Internetu a do zvýšení jeho bezpečnosti.
- S postupem času se ale začalo stále jasněji ukazovat, že zvýšení bezpečnosti Internetu není až tak technickým problémem. Problém byl spíše v tom, jakou zvolit celkovou koncepci a strategii zvyšování bezpečnosti, jaká dostupná technická řešení zvolit, jak najít konsensus mezi všemi zainteresovanými stranami o zvoleném řešení, jak ho standardizovat a jak ho prosadit do praxe. Tento proces bohužel není ani dnes zdaleka dokončen.
- Přenosové mechanismy Internetu stejně jako např. telefonu nijak nešifrují ani jinak nezabezpečují data. Přesto se lidé naučili telefony používat a sami si zvolit, co svěří relativně málo bezpečnému telefonu a co si sdělí jinou cestou. Tak by tomu mohlo být i u Internetu..
- **Je-li potřeba přenést nějaká citlivější a důvěrnější data, je nutné je zabezpečit již na úrovni aplikace, která je produkuje, a k přenosu je předat v již zabezpečeném tvaru. Vlastní přenosové mechanismy Internetu pak mohou zůstat takové jaké jsou (tj. nezabezpečené).**
- Alternativní možností by bylo zabudovat příslušné zabezpečovací mechanismy přímo do přenosových sítí. To by ale přineslo mnoho negativních aspektů: například ten, že by nebylo možné zvolit takové řešení, které by vyhovělo všem možným požadavkům na bezpečnost. Požadavky jednotlivých aplikací na míru zabezpečení jsou a vždy budou odlišné. Pak by uživatel plně vkládal bezpečnost svých dat do rukou někoho jiného.
- V neposlední řadě by se zabudováním bezpečnostních mechanismů přímo do přenosové infrastruktury Internetu tato infrastruktura výrazně prodražila.
- Další příčinou relativně nízké míry bezpečnosti dnešního Internetu jsou dosti "důvěřivé" služby, používané v této síti sítí. Některé z nich vůbec nevyžadují žádná hesla či jiné

formy ověřování identity a oprávněnosti uživatelů, zatímco jiné ano, ale dělají to dosti naivním způsobem, který je poměrně snadné překonat. Mnoho služeb, které po uživateli požadují zadání hesla, toto heslo přenáší po síti nezakódované, a tedy přesně v takovém tvaru, v jakém jej autor zadal. Není pak příliš těžké takovéto heslo neoprávněně odposlechnout a zneužít – je to např. **elektronická pošta**.

Možnosti zabezpečení WWW

Zde není žádným problémem prohlásit některé WWW stránky za neveřejné a přístup k nim vázat na zadání správného přístupového hesla. **Problém je spíše s přenosem informací** mezi WWW servery a jejich klienty, a zejména pak opačným směrem, od klientů (a jejich uživatelů) směrem k WWW serverům. Za standardních okolností tato data cestují po síti v nezabezpečeném tvaru, lidé však chtějí využívat službu World Wide Web pro nejrůznější účely, včetně elektronického obchodování, nakupování, provádění finančních transakcí apod., a pro tyto účely je opravdu nutné zvýšit stávající úroveň bezpečnosti, kterou služba World Wide Web vykazuje.

- **Prvním možným přístupem** je očekávat, že zvýšit míru své bezpečnosti bude potřebovat více aplikací resp. služeb, používaných v rámci Internetu, a že se tudíž vyplatí zabudovat příslušné mechanismy takovým způsobem, aby byly využitelné všemi aplikacemi které o to budou mít zájem (což znamená implementovat je pouze jednou, a začlenit je na vhodné místo do vrstev síťového programového vybavení). Takovýmto řešením je např. koncepce tzv. **SSL (Secure Socket Layer), vyvinutá firmou Netscape** a podporovaná jejími browsery. Výhodou tohoto přístupu je i skutečnost, že vše se dá zařídit tak, aby se používané aplikace nemusely nějak výrazněji měnit. Zabudované zabezpečovací mechanismy totiž mohou vytvářet jednotlivým aplikacím iluzi toho, že pracují nad takovou přenosovou infrastrukturou, která je již sama zabezpečená a sama se stará o bezpečnost přenášených dat. Nevýhodou je pak skutečnost, že takováto "společná" míra bezpečnosti nemusí všem aplikacím postačovat – viz výše.

- **Alternativním přístupem** je očekávat, že bezpečnost bude vyžadovat spíše méně aplikací, a že se tudíž vyplatí, aby si každá svou bezpečnost zajišťovala sama, vlastními prostředky (neboli aby potřebné zabezpečovací mechanismy byly implementovány pokaždé znovu, v každé z aplikací která něco takového potřebuje). Zřejmou výhodou je možnost tyto zabezpečovací mechanismy doslova "ušít na míru" příslušným aplikacím, nevýhodou nutnost jisté nadbytečnosti (opakované implementace jednoho a toho samého). Příkladem může být protokol **S/HTTP (Secure HTTP**), který je rozšířením stávajícího protokolu HTTP (HyperText Transfer Protocol, slouží pro komunikaci mezi WWW serverem a uživatelským browserem) o potřebné zabezpečovací mechanismy.

- **Jiným příkladem** může být **protokol SET (Secure Electronic Transactions)**, který je specificky zaměřen na potřeby placení po Internetu, včetně placení pomocí kreditních karet. Jde o řešení, společně vyvinuté velkými firmami v oblasti programového vybavení pro Internet (mj. i firmami Microsoft a Netscape) a společnostmi které se zabývají kreditními kartami (mj. Mastercard i Visa). Pomocí protokolu SET by například mělo být možné přenášet po Internetu údaje o kreditních kartách (v rámci jednotlivých transakcí) v zabezpečeném tvaru, aniž by se platící

majitel kreditní karty musel obávat, že se někdo neoprávněný dostane k údajům o jeho kartě a bude moci je zneužít.

Peterka Jiří – Internet a bezpečnost (Ekonomický poradce podnikatele č. 11/97)
http://www.earchiv.cz/a97/a711p200.php3

Bezpečnostní rizika

- Nejsnadnějším způsobem jsou **útoky na hesla uživatelů** (tzv. *slovníkově založené útoky*). Při tomto útoku se postupně generují různá přístupová hesla. Většinou se jedná o automatizované útoky pomocí jednoduchých programů, které se cyklicky opakují.

- **Útoky založené na předstírání IP adresy** umožňují získat vnitřní přístup k systému a to předstíráním IP adresy hostitele interní sítě.

- Již obtížnějším způsobem je **náhodné prohlížení přenášených paketů** (nebo také tzv. *monitorování sítě*). Útočníci se snaží zachytit a zkopírovat pakety předávané mezi jednotlivými komunikačními uzly – místy na Internetu.

- **Přivlastnění IP adresy** řádného klienta a jeho následné odpojení umožňuje jak import, tak export dat do systému.

- V případě, kdy se útočník vydává za administrátora sítě a vyžaduje po uživatelích důvěrné informace (například hesla), se jedná o útok zvaný společenské monitorování (tzn. **Předstírání administrátorů systému**).

- Existuje i způsob, kdy tvůrce softwaru vědomě naprogramuje bezpečnostní trhliny svého produktu, které pak následně zneužívá ke svému prospěchu. V podstatě se jedná o **útok vedený pomocí neautorizovaného softwaru**.

Další příklady možných útoků

Např. běžným uživatelům připojeným „dial-upem“ hrozí tzv. **nebezpečí „žluté linky“** – odpojení modemu od serveru poskytovatele a přepojení na linku s větší minutovou sazbou (exotické země – zejm. v karibském moři apod.). Tento typ útoku je způsoben bezpečnostní mezerou v zabezpečení skriptů ActiveX, vytvořené firmou Microsoft. Možností je prevence – vyhnout se serverům s nebezpečným obsahem, případně existuje i software – např. *Connection Meter*)

Různé typy škodlivých skriptů, dále **spyware** – programy odesílající do Internetu soukromá data. Dále **trojští koně** – dostanou se do počítače ve formě programů a monitorují např. stisknutí kláves a mohou odeslat uživatelovo přihl. jméno a heslo např. ke vstupu do Internetové banky jinému uživateli Internetu. E-mailové viry – tvz. **červi** apod.

Další informace (v angličtině) o různých formách útoků hackerů a nebezpečích plynoucích na stránce Hacking FAQ and Information
(http://www.btinternet.com/~shawweb/george/hacks/info.html)

Zásady ochrany počítače

1. Používat kvalitní a hlavně pravidelně aktualizovaný **antivirový program**. (např. *Avast!, AVG, Norton Antivirus* atd.)
2. Počítač napojený jakýmkoli způsobem na Internet by měl mít nainstalovaný tzv. **Firewall** (alespoň softwarový) – volně dostupné jsou např. *Kerio Personal Firewall* nebo *ZoneAlarm*.
3. Pravidelné **aktualizace operačního systému** – bezpečnostní záplaty – zejm. produkty firmy Microsoft (Windows, Office, Explorer). Linux je mnohem bezpečnější ale ani jeho bezpečnost nepřeceňovat a stahovat aktualizace.

Doporučuji vyzkoušet test zabezpečení počítače na serveru Agerit, s. r. o. – Test bezpečnosti (http://www.test.bezpecnosti.cz)

Firewally

Firewall je systém vytvořený k prevenci před neautorizovaným vstupem do nebo ze soukromé sítě. Firewally mohou být použity ve dvou formách – hardwarové a softwarové nebo kombinace obou. Jsou často užívány k prevenci neautorizovaných Internetových uživatelů před vstupem do soukromých sítí, zejm. intranetu připojených na Internet. Všechny zprávy vstupující nebo opouštějící intranet procházejí firewallem, který zkoumá každou zprávu a blokuje ty, které nevyhovují uživatelem specifikovaným bezpečnostním kritériiím.
Zde je několik typů firewallových technik:

- **Paketový filtr** – kontroluje každý paket, který vstupuje nebo opouští síť a akceptuje nebo nepřijme je dle uživatelem definovaných pravidel. Filtrování paketů je poctivě efektivní a transparentní uživatelům, ale je obtížné je konfigurovat. Je náchylný na IP spoofing[4].
- **Aplikační gateway** – vztahuje se na bezpečnostní mechanismy specifických aplikací, jako FTP a Telnetových serverů. Je velmi efektivní, ale může přivodit snížení výkonu.
- **Circuit-level gateway** – vztahuje se na bezpečnostní mechanismy při navázání spojení pomocí protokolů TCP nebo UDP. Jakmile je spojení navázáno, pakety mohou proudit mezi počítači bez další kontroly.
- **Proxy server** – zachycuje všechny zprávy vstupující a opouštějící síť. Proxy server efektivně skrývá skutečnou síťovou adresu. Proxy server sedí mezi klientovou aplikací, jako je webový browser a skutečným serverem. Zachycuje všechny žádosti zasílané reálnému serveru za účelem zjištění, zda je schopen žádosti sám splnit. Když ne, předává je skutečnému serveru.

www.webopedia.com

[4] Technika k získání přístupu do počítačů, při níž vetřelec posílá zprávy do počítače s IP adresou, která indikuje, že zpráva která byla vetřelcem odeslána, pochází z důvěryhodného počítače. Hacker musí nejprve najít IP adresu důvěryhodného počítače a modifikuje hlavičku paketu tak, že se jeví jako paket, který přichází z tohoto počítače.

Spam

Spam je označení pro nevyžádaný obtěžující dopis. Tato definice je značně subjektivní a je vázána na pocit příjemce – odesílatel tedy nemůže předem s jistotou určit, zda je dopis obtěžující. Ne každý spam vyžaduje zásah proti odesílateli. Zasáhnuto by mělo být tehdy, pokud odesílatel spam zasílá opakovaně nebo hromadně.

Mezi spamem můžeme rozlišit několik typů:

- Reklamní zprávy
- „Hoaxy“
- Řetězové dopisy a další

Reklamní zprávy – spammer zasílá texty, které mu mají přinést finanční nebo jiný prospěch.
„Hoaxy“ – jsou řetězové dopisy obsahující zpravidla nepravdivou informaci, jež příjemce určitým způsobem nutí (apeluje na city, informuje o neexistujících počítačových virech nebo jiných hrozbách, upozorňuje na neexistující služby zdarma apod.), aby zprávu poslal co nejvíce lidem dále. Často obsahují, pro zvýšení věrohodnosti zprávy, také návod na vyřešení situace (zbavení se viru apod.)

Klasické řetězové dopisy – oproti hoaxům jsou neškodné, srovnatelně ale mohou obtěžovat adresáta. Nejčastěji vyžadují po příjemci, aby je odeslal dále, jinak nebude mít štěstí apod. Na principu řetězových dopisů funguje také naprosto běžné přeposílání e-mailových zpráv, obsahující vtipy, veselé obrázky atd.

V březnu 2003 organizace CDT (Center for Democracy and Technology) zveřejnila výsledky půlročního průzkumu chování spammerů. Průzkum probíhal následovně:

- během léta roku 2002 CDT vytvořilo 250 e-mailových adres,
- každou z nich jednou použilo pro některou z rizikových aktivit,
- zkoumalo, které z adres přitáhly spammery a jaký objem spamu na ně byl odesílán,
- adresy měly podobu náhodného řetězce, aby nehrozila možnost, že na ně spammer přijde náhodou.

Během 6 měsíců bylo přijato asi 10 tis. zpráv, z nichž 8842 zpráv mělo charakter spamu. Z průzkumu vyplynuly závěry:

- e-mailové adresy zveřejněné na Internetu jsou spammery často používány,
- množství spamu zaslaného na adresu zveřejněnou na webu je přímo úměrné návštěvnosti těchto stránek,
- e-mailové adresy získané z webu jsou používány relativně krátce (po odstranění adres množství přijatých zpráv klesá),
- maskování em. adres je efektivním způsobem zamezení získávání adres z webových stránek nebo USENETu,
- on-line služby, které publikují podmínky a dávají uživatelům možnost výběru zda dostávat, nebo nedostávat, tyto podmínky většinou respektují,
- registry doménových jmen nejsou pro spamery velkým zdrojem adres,
- i když nebyla adresa nikde zveřejněna, je možné dostávat spam skrz útoky na poštovní server.

Rozdíl mezi spamem v ČR a USA

- Typický americký nevyžádaný dopis rozesílá profesionální agentura, která se podobnými aktivitami živí a která si plně uvědomuje všechny konsekvence svého jednání.
- Typický český spam rozesílá malá firma nebo soukromý uživatel, aniž by si byli vědomi, že jejich počínání druhé obtěžuje, český spam je zasílán spíše z nedostatku znalostí.

Právní regulace spamu

Novela zákona č. 40/1995 Sb. O regulaci reklamy
§ 2, bod 1, písm. e) Zakazuje se … šíření nevyžádané reklamy, pokud vede k výdajům adresáta nebo pokud adresáta obtěžuje.

- Orgánem dozoru jsou okresní živnostenské úřady,
- Sancí za porušení zákona je pokuta v max. výši 2 mil. korun, a to i opakovaně,
- Zákon explicitně hovoří o odpovědnosti „zadavatele, zpracovatele nebo šiřitele".
- Zákon nepožaduje „hromadnost", takže mimo zákon se ocitnou i různá jednorázová oslovení e-mailovou formou.

Zákon O ochraně osobních údajů č. 101/2000 Sb.)

- První problém – prokázat, že elektron. poštovní adresy jsou osbními údaji ve smyslu toho zákona.
- Druhý a největší problém – právní postihování spammerů obtížné kvůli jejich anonymitě.

Další možností je návrh zákona O (některých) službách informační společnosti,

Spam a EU

ES schválilo dokument *Communications Data Protection Directive*, který ošetřuje ochranu údajů mimo jiné také na Internetu. Každý oslovený recipient musí se zasíláním reklamy předem souhlasit, EU se přiklonila k modelu *opt-in*[5].

Mgr. Čermák Marek – Spam (pdf), Brno 2003

[5] Tedy na zásadě, že první iniciativa musí být na straně příjemce, a nikoli na straně rozesilatele. Musí to být příjemce, neboli potenciální zákazník, kdo projeví přání být o něčem informován. Aby takové přání projevil, musí k tomu mít motivaci. Důležitý je také způsob, jakým příjemce svůj zájem projeví - ten by měl být otevřený a korektní, měl by zájemci na rovinu a srozumitelně říkat, co se mu nabízí a za jakých podmínek (a ne aby šlo o "nachytání" na něco úplně jiného, s tím že to podstatné je skryto někde v právních kličkách psaných nejdrobnějším písmem někde pod čarou).

Literatura

Webopedia – Online Computer Dictionary for Computer and Internet Terms and Definitions (http://www.webopedia.com)

History of the Internet (http://www.nic.funet.fi/index/FUNET/history/internet/en/)

Internet Society (http://www.isoc.org)

Vladimír Vrabec Vladimír - Vítězná cesta TCP/IP (http://www.lupa.cz/clanek.php3?show=2467)

Bezpečnost na Internetu (Matyska L., ÚVT, a FI MU – pdf na www.fi.muni.cz)

Peterka Jiří – Internet a bezpečnost (Ekonomický poradce podnikatele č. 11/97) (http://www.earchiv.cz/a97/a711p200.php3)

Hacking FAQ and Information (http://www.btinternet.com/~shawweb/george/hacks/info.html)

Mgr. Čermák Marek – Spam (pdf), Brno 2003

Stria Jan – Bezpečnost internetového bankingu (2001) (http://www.seminarky.cz)

Počítačová kriminalita – Ontl L. (Hradec Králové, 2000) (http://www.seminarky.cz)