Služby sítě: e-mail

Elektronická pošta (nebo také e-mail, mail) je způsob odesílání, doručování a přijímání zpráv přes elektronické komunikační systémy. Termín e-mail se používá jak pro internetový systém elektronické pošty založený na protokolu SMTP, tak i pro intranetové systémy, které dovolují posílat si vzájemně zprávy uživatelům uvnitř jedné společnosti nebo organizace. K širokému rozšíření e-mailu přispěl zejména internet.

Historie

Elektronická pošta vznikla v roce 1965 jako způsob komunikace více uživatelů mainframového počítače se sdílením času (komunikace mezi více uživateli pracujícími současně na jednom počítači interaktivním nebo téměř interaktivním způsobem). Přesto je přesná historie nejasná.

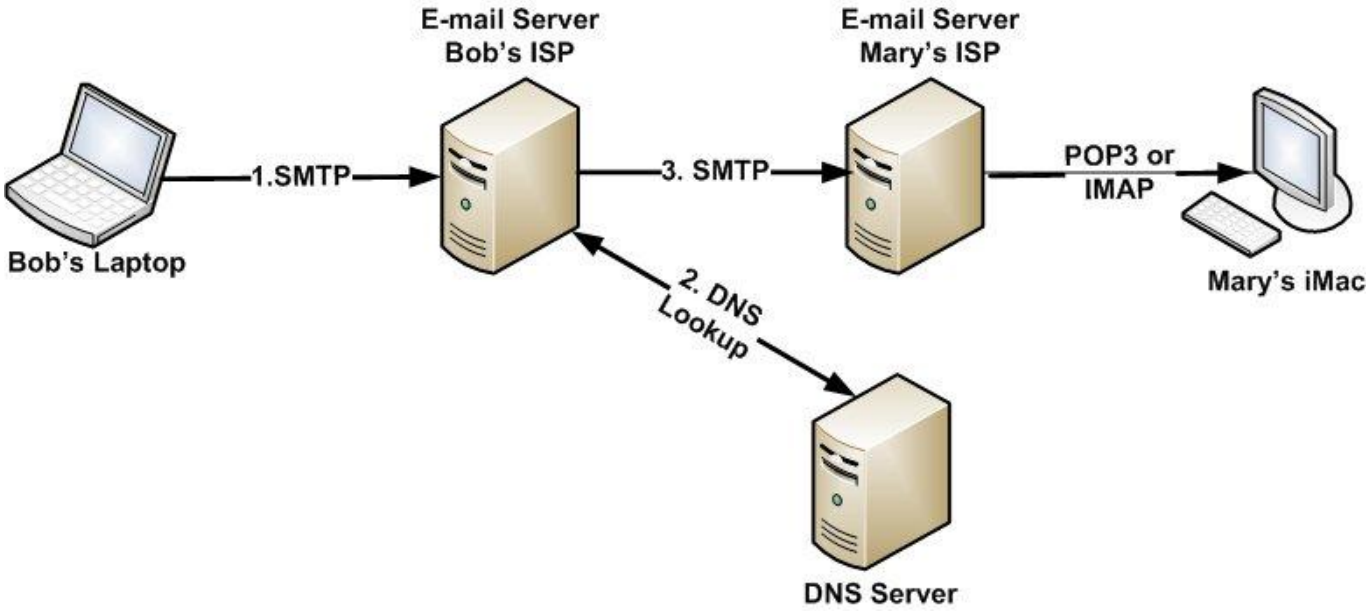
E-mail se rychle rozšířil a stal se síťovým e-mailem, což umožňovalo uživatelem posílání zpráv mezi různými počítači. Raná historie síťového e-mailu je taktéž nejasná.

Počítačová síť ARPANET (Advanced Research Projects Agency Network) byla důležitá v dalším vývoji elektronické pošty. Existuje zpráva, která poukazuje na experimenty s přenosem e-mailů mezi systémy krátce po vzniku ARPANETu v roce 1969. ARPANET významně zvýšil popularitu e-mailu, a ten se zároveň stal trhákem jako aplikace v rámci ARPANETu.

Ray Tomlinson začal v roce 1971 používat znak @ na oddělení jména uživatele od názvu stroje.

V té době nebyly všechny počítače nebo sítě navzájem síťově propojené, e-mailové adresy musely obsahovat „cestu“ pro zprávu, tj.trasu mezi počítačem odesílatele a příjemce. Tímto způsobem bylo možné posílat e-maily mezi více sítěmi. Cestu specifikovala tzv. „bang path“ adresa, která již specifikovala skoky (hops) mezi lokacemi, které byly považované za dostupné adresátovi. Nazývala sa tak, protože obsahovala pro každý skok znak „bang“, tj. „!“. Takže například cesta „...!bigsite!foovax!barbox!ja“ oznamuje, že pošta se má směrovat stroji „bigsite“ (předpokládaná dobře známá lokace přístupná každému) a odtud přes stroj „foovax“ uživatelskému účtu na stroji „barbox“.

Popis fungování



Zdroj: http://en.flossmanuals.net/thunderbird/how-email-works/

Protokoly

Mezi počítači na internetu se vyměňují zprávy pomocí protokolu SMTP a softwaru typu MTA jako např. Sendmail.

Uživatelé mívají na svém počítači nainstalován program, který se nazývá e-mailový klient. Ten stahuje zprávy z poštovního serveru použitím protokolů POP nebo IMAP, avšak v prostředí velkých společností se stále vyskytuje použití některého komerčního protokolu jako např. Lotus Notes nebo Microsoft Exchange Server.

Protokol SMTP

SMTP (Simple Mail Transfer Protocol) je internetový protokol určený pro přenos zpráv elektronické pošty (e-mailů) mezi přepravci elektronické pošty (MTA). Protokol zajišťuje doručení pošty pomocí přímého spojení mezi odesílatelem a adresátem. Zpráva je doručena do tzv. poštovní schránky adresáta, ke které potom může uživatel kdykoli (off-line) přistupovat (vybírat zprávy). SMTP funguje nad protokolem TCP, používá port TCP/25.

Protokol POP3

POP (Post Office Protocol) je internetový protokol, který se používá pro stahování emailových zpráv ze vzdáleného serveru na klienta. Jedná se o aplikační protokol pracující přes TCP/IP připojení. V současnosti je používána zejména třetí verze (POP3), která byla standardizována v roce 1996 v RFC 1939.

Protokol IMAP

IMAP (Internet Message Access Protocol) je internetový protokol pro vzdálený přístup k e-mailové schránce prostřednictvím e-mailového klienta. IMAP nabízí oproti jednodušší alternativě POP3 pokročilé možnosti vzdálené správy (práce se složkami a přesouvání zpráv mezi nimi, prohledávání na straně serveru a podobně) a práci v tzv. on-line i off-line režimu. V současné době se používá protokol IMAP4 (IMAP version 4 revision 1 - IMAP4rev1), který je definován v RFC 3501.

Typy programů podílejících se na doručování e-mailů

Doručování elektronické pošty po Internetu se účastní čtyři druhy programů:

- MUA - Mail User Agent, poštovní klient, který zpracovává zprávy u uživatele
- MSA - Mail Submission Agent, program, který obvykle předává poštu MTA (od MUA)
- MTA - Mail Transfer Agent, server, který se stará o doručování zprávy na cílový systém adresáta
- MDA - Mail Delivery Agent, program pro lokální doručování, který umísťuje zprávy do uživatelských schránek, případně je může přímo automaticky zpracovávat (ukládat přílohy, odpovídat, spouštět různé aplikace pro zpracování apod.)

MUA

MUA (Mail User Agent, také poštovní nebo e-mailový klient) je počítačový program, který slouží k přijímání, odesílání a správě elektronické pošty (e-mailů). Poštu nejčastěji ukládá na lokální disk a zprávy a další informace si se serverem poskytovatele emailové schránky vyměňuje pomocí internetových protokolů.

Mezi e-mailové klienty patří například Microsoft Outlook, Mozilla Thunderbird, The Bat!, Eudora.

Webmail

Webmail je v webová aplikace, která umožňuje uživatelům přistupovat k jejich e-mailovým schránkám prostřednictvím webového prohlížeče. Webmail je alternativa ke klasickým aplikacím e-mailových klientů. Webmail poskytují téměř všechny internetové portály a poskytovatelé webových služeb (např. Gmail od Googlu, Hotmail od Microsoftu, Seznam.cz, Centrum.cz, atd.).

MSA

MSA (Mail submission agent) je v informatice označení programu, který přijímá elektronickou poštu od MUA. MSA obvykle sám poštu nedoručuje, ale předává ji MTA, který zajistí její doručení příjemci. MTA předává MSA elektronickou poštu pomocí zjednodušené varianty SMTP protokolu, kterou popisuje RFC 4409. Naslouchá na tradičním síťovém portu číslo 25 nebo na portu 587. Funkci MSA často vykonává plnohodnotný MTA, ale existují i speciálně navržené MSA, které plně funkční MTA nemohou nahradit.

MTA

MTA (Mail Transfer Agent) je počítačový program, který přenáší elektronickou poštu z jednoho počítače na druhý. MTA přijímá zprávy z jiného MTA pomocí mail submission agenta (MSA), který

dostane zprávu od MUA, nebo přímo od MUA, MTA pak tedy působí jako MSA. MTA pracuje za scénou, mezitím co uživatel obvykle vzájemně komunikuje s MUA.

Mezi mail servery patří například Sendmail, Postfix, Microsoft Exchange Server.

MDA

MDA (Mail Delivery Agent) je počítačový program, který doručuje zprávy elektronické pošty do jednotlivých poštovních schránek uživatelů poté, co přepravce pošty (MTA) rozhodne, že jsou přijaty a patří místnímu uživateli. MDA nemusí být nutně součástí MTA, přestože obě funkce jsou implementovány stejným programem nebo programem pocházejícím ze stejného zdroje. Některé MTA umožňují správci systému zvolit nejvýhodnější MDA pro jeho konfiguraci.

Na unixových systémech patří mezi nejpopulárnější MDA programy procmail a maildrop.

Kódování obsahu e-mailu

Pro e-mail je definován přenos 7bitové ASCII informace. Přesto je většina e-mailových přenosů 8bitových, kde ale nelze zaručit bezproblémovost. Z toho důvodu byla elektronická pošta rozšířena o standard MIME (Multipurpose Internet Mail Extensions), aby bylo umožněno kódování vkládaných HTML a binárních příloh, obrázků, zvuků a videí.

Obsah e-mailové zprávy

Internetové e-mailové zprávy se skládají ze dvou hlavních částí:

- Hlavička – předmět zprávy, odesílatel, příjemce a jiné informace o e-mailu
- Tělo – samotná zpráva

K e-mailu je možné přikládat přílohy (obrázky, textové dokumenty a jiné soubory). Bez problémů bývá doručování menších souborů typu dokumentu. Pokud však je ke zprávě přiložen velký soubor nebo příliš mnoho souborů nebo soubor typu programu, který by mohl být infikován virem nebo červem, mnohdy taková zpráva neprojde ochrannými filtry na doručovací cestě.

Hlavička

Hlavičky e-mailu obvykle obsahují alespoň 4 pole:

- Od (From): e-mailová adresa (popř. i jméno) odesílatele zprávy (zpravidla vyplňuje program automaticky)
- Komu (To): e-mailová adresa (popř. i jméno) příjemce zprávy, adresátů může být více současně (vyplňuje odesílatel)
- Předmět (Subject): stručný popis obsahu zprávy (vyplňuje odesílatel, nepovinně)
- Datum (Date): místní datum a čas odeslání zprávy (vyplňuje program automaticky)

Pole „Od“ nemusí obsahovat adresu skutečného odesílatele. Je velmi jednoduché to zfalšovat a zpráva

potom vypadá, že přišla z uvedené adresy. Je možné e-mail digitálně podepsat, aby bylo jisté, od koho zpráva pochází.

Šifrování

Šifrování je proces, při kterém se čitelná nezabezpečená data převádí na nečitelná data šifrovaná, které je schopen rozšifrovat pouze majitel dešifrovacího klíče. U emailu se většinou používá princip asymetrického šifrování, které využívá klíče dva (pro šifrování a dešifrování). První klíč je veřejný a uložený na volně přístupném serveru. Odesílatel emailu ho použije k zašifrování své zprávy, kterou odešle. Poté příjemce zašifrovanou zprávu dešifruje svým druhým „soukromým“ klíčem. Opačný postup se může použít pro vytvoření digitálního podpisu, který potvzuje identitu odesílatele.

Ověřování

Protokol SMTP sám o sobě neposkytuje ověření, zda email skutečně pochází ze zdroje udaného v hlavičce, což je samozřejmě bezpečnostní problém. Odesilatel by mohl hlavičky zfalšovat a podvrhnout email pod cizím jménem. Existují ale validační řešení, které toto řeší. Pokud provozujeme vlastní email server, je důležité tyto systémy nastavit, aby nedocházelo k označování emailů jako spam.

- **DKIM** (DomainKeys Identified Mail) - e-mail je digitálně podepsán, veřejný klíč je uložen v DNS TXT záznamu
- **SPF** (Sender Policy Framework) - ověřuje jen IP adresu odesilatele, nastaven opět pomocí DNS TXT
- **DMARC** (Domain-based Message Authentication, Reporting and Conformance) - vychází z předchozích dvou mechanizmů, umožňuje přesněji nastavovat podmínky a zasílá pravidelné reporty

Nežádoucí zprávy

V elektronické poště se objevují čtyři typy nežádoucích zpráv. Spam, hoax, phishingové zprávy a e-mailový červi.

Spam

Spam je nevyžádaná reklamní pošta. Nízké náklady na odeslání zprávy umožňují spammerům odeslat stovky miliónů elektronických zpráv denně pomocí laciného internetového připojení. Stovky aktivních spammerů způsobují přetížení počítačů v internetu, které takto dostávají desítky či stovky nevyžádaných e-mailů denně.

Hoax

Hoax je zjednodušeně řečeno klamná zpráva. V elektronické komunikaci je hoax nevyžádaná e-

mailová zpráva, která uživatele varuje před nějakým virem, prosí o pomoc, informuje o nebezpečí, snaží se ho pobavit apod. Hoax většinou obsahuje i výzvu žádající další rozeslání hoaxu mezi přátele, příp. na co největší množství dalších adres, proto se někdy označuje také jako řetězový e-mail.

Phishing

Phishing je podvodná technika používaná na Internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.) v elektronické komunikaci. K nalákání důvěřivé veřejnosti komunikace předstírá, že pochází z populárních sociálních sítí, aukčních webů, on-line platebních portálů, úřadů státní správy nebo od IT administrátorů.

Principem phishingu je typicky rozesílání e-mailových zpráv, které často vyzývají adresáta k zadání osobních údajů na falešnou stránku, jejíž podoba je takřka identická s tou oficiální. Stránka může například napodobovat přihlašovací okno internetového bankovnictví. Uživatel do něj zadá své přihlašovací jméno a heslo. Tím tyto údaje prozradí útočníkům, kteří jsou poté schopni mu z účtu vykrást peníze.

Příklad phishingové zprávy

E-mailový červ

E-mailoví červi využívají ke svému šíření elektronické pošty. Poté, co infikují nový počítač, se začnou rozesílat na e-mailové adresy, které získají buď z e-mailového adresáře oběti počítače, nebo prohledáváním obsahu uložených souborů a extrahováním řetězců, které vyhovují tvaru e-mailové adresy. Zvláštním případem jsou sítě botnet, složené z počítačů infikovaných k tomu uzpůsobeným červem, kdy infikované počítače na příkaz autora infekce zasílají hromadně spam, nebo uskutečňují útoky typu DDoS na jiné počítače.

Obsah infikované zprávy zaslané e-mailovým červem obvykle obsahuje vlastní škodlivý program jako přílohu, případně odkazuje na webové stránky, které jsou schopny infikovat počítač příjemce.

Obrana

Způsobů jak se bránit před těmito typy e-mailů je více.

První možnost je zabránit tomu, aby se vaše e-mailová adresa nedostala na seznam e-mailových adres, na které se tyto e-maily posílají. Tomu se dá zabránit například tak, že svoji e-mailovou adresu nebudete zveřejňovat na webových stránkách ve formátu, v jakém ji rozpoznají roboti, kteří prohlížejí webové stránky a hledají e-mailové adresy (například panx „zavináč“ seznam.cz místo panx@seznam.cz). Další možnost je neuvádět svoji e-mailovou adresu na webových stránkách, kde nepotvrdíte souhlas se zasíláním e-mailů.

Další možnost je používání antivirové ochrany a spamových filtrů, které tyto e-maily rozpoznají a blokují je.