Správa serverů a počítačových sítí

2020/2021

Přednáška 7
(ver. 2021-03-30-01)

Poštovní služby

- Teorie mailových služeb
  - MUA, MTA, MDA
  - SMTP, IMAP, POP
- Odesílání a transport pošty
  - Postfix, Sendmail, Qmail, Exchange
- Doručování pošty
  - Courier, Cyrus, UW, ipop, Exchange
- Antispam a Antivir
  - Clamav, AVG, Nod32, ESET
  - Spamassassin

1. Teorie mailových služeb

- Elektronická pošta, druhý nejpoužívanější systém internetu
- Email je jako DNS decentralizované
- Mailové služby jsou úzce vázané na DNS
- Tři druhy programů
  - MUA – Mail User Agent, zpracování zpráv u uživatele
  - MTA – Mail Transport Agent, doručování pošty cílovým adresátům
  - MDA – Mail Delivery Agent, lokální doručování do koncových schránek

1.1. MUA

- Emailový klient, stará se o stahování a odesílání pošty na straně klienta
- Ovládá protokoly pro stahování i odesílaní pošty, komunikuje na více portech
- Ne každý klient umí POP i IMAP, stejně jako šifrování
- Dostupné pro všechny operační systémy

1.1 Příklady MUA

- GUI aplikace
  - Outlook, Outlook Express
  - Mozilla Thunderbird
  - Evolution, Kmail
- Konzolové aplikace
  - Mutt, Pine
  - Telnet, Openssl
- Webové aplikace
  - Horde, SquirrelMail
  - Gmail, Yahoo, Seznam

1.2 MTA

- Emailový server
- Komunikuje na portu TCP/25 nebo TCP/465 nebo TCP/587
- Přijímá maily od MUA a předává je dalším MTA či MDA na doručení
- Každý server umí základní funkce MDA
- Nejdůležitější a nejcitlivější prvek mailových služeb
- Rozhoduje na základě MX a A záznamů o doručování pošty

1.2 Příklady MTA

- Dostupné na všech operačních systémech
- Unix
  - Sendmail,Qmail
  - Postfix, Exim
  - Kerio Mailserver
- MS Windows
  - MS Exchange
  - Kerio Mailserver
  - HmailServer
- Cloud
  - Microsoft Office 365
  - Gmail

1.3 MDA

- Program doručující poštu do schránek
- Základní variantu obsahuje každý MTA
- Specializované programy mohou umět více
- Pro Unix například:
  - Procmail
  - maildrop
- Síťová varianta MDA je LMTP
  - Local Mail Transport Protocol
  - Používá se většinou na doručování do složitějších systémů jako Cyrus

1.3 MDA

- Kromě doručování probíhá často rozklad do více schránek
- Jedno z míst, kde se často nasazují přídavné filtry jako antispam či antivir
- Dnes filtraci a složitější filtrování zvládají i jednotliví klienti - MUA

1.4 Stahování pošty

- Klient stahuje poštu ze serveru
- Jednodušší protokol POP3
  - Umí stáhnout jen celé maily, umí nechat kopii na serveru
- Nabízející více možností IMAP
  - Umí stahovat jen hlavičky
  - Umí filtrovat už při stahování
  - Kompletně pracuje s mailovou schránkou
- Účet je vždy zabezpečen jménem a heslem
- Používají se protokoly:
  - POP3/S TCP 110 / TCP 995
  - IMAP/S TCP 143, případně 220 / TCP 993
  - MAPI RPC
  - HTTPS TCP 443

1.4 Stahování pošty

- Je vhodné používat šifrované protokoly, neboť hesla se posílají nešifrovaná
- Imap si na serveru indexuje stav schránek, při migraci může dojít k opětovnému stažení
- Ne každý klient umí plně oba protokoly
- Kromě klasických programů se používají ještě další jako fechtmail či offlineimap
- Se stahováním pošty problém nebývá

1.5 Doručování pošty

- Klient – MUA -odešle zprávu na mailovou ad-resu
  - Uzivatel @ domena.cz
  - Zprávu předá na definovaný SMTP server
- Server – MTA – zprávu převezme a zjišťuje zde je určena pro něj, pokud ano ověří zda existuje záznam kam mail uložit:
  - Virtuální email
  - Alias
  - Uživatel
- Pokud ano, předá jej na MDA k doručení

1.5 Doručování pošty

- Server – MTA – zprávu převezme a snaží se jí předat na další server podle :
  - MX záznamu, těch může být více a berou se sestupně podle priorit
  - A záznamu, pokud není nalezen MX bere se, že doména je název stroje
- Pokud se zpráva nedá doručit, MTA je vrací odesílateli, případně ji po časovém limitu vyřadí z fronty

1.6 Problémy s doručováním pošty

- Základní problém je DNS, nesprávně nastavené MX záznamy
- Špatná konfigurace MTA, nejsou správně definované lokální domény
- Špatná konfigurace doručování MDA
- Blokování mailů programy na ochranu před:
  - Spamem
  - Viry

2. Ochrana pošty

- V dřívější době nebylo řešeno
- V rámci SMTP není s ochranou počítáno
- Problémy vnikají dvojího druhu:
  - Viry šířené převážně na MS Windows
    - Vir je možné snadno detekovat
    - Emaily s virem se mohou mazat
  - Spamy:
    - Snaha o znepřístupnění mailů
    - Šíření reklamních informací
    - Šíření poplašných zpráv
    - Řetězová dopisy
    - Co je pro jednoho spam pro druhého není
    - Často kombinované s viry

1.6 SMTP Relay

- Ošetřuje odcházející a průchozí poštu
- Open SMTP Relay
  - Umožní odeslat libovolný mail komukoliv
  - Když je detekována
    - Začnou jí útočníci používat - trafic, zátěž
    - Je nahlášena na blacklistech – nedochází pošta
- Možnosti ochrany:
  - Odesílání s heslem
  - POP-before-SMTP
  - Akceptace jen nadefinovaných domén
  - Akceptace požadavků jen z definované sítě

1.7 Antispam

- Ošetřuje příchozí poštu
- Kombinuje několik metod:
  - Kontroluje black-listy na domény, emaily, servery
  - Analyzuje obsah mailu a strukturu mailu
  - Učí se na základě heuristik – bayesovské filtry
  - Reverzy a adresy odesilatele
- Většinou ve formě průchozího filtru
  - Přidává hlavičky, nebo mění subjekty
  - Není vhodné rovnou zahazovat
  - Většinou se filtruje do extra schránek s omezenou dobou úschovy
- Klasický představitel : spamassassin

1.8 Antivir

- Viry prochází všemi operačními systémy, ale ne ve všech škodí
- Vir sám o sobě běžně emailovému systému nevadí
- Škodí až na stroji uživatele
- Škodí tím, že se cyklicky rozesílá, vede k zpožďování pošty a přetěžování serverů
- Viry je možné okamžitě izolovat či mazat

1.9 Black a White listy

- Seznamy zakázaných a povolených adres či serverů
- White-listy bývají klasicky na straně serverů, definují zákazníky, jejichž pošta musí dojít
- Black listy jsou jak na straně serverů tak u třetích stran jako SpamCop,SpamLab, CBL
- Do lokálních black-listů přidává správce

1.9 Black listy

- Internetové blacklisty jsou velmi kontroverzní
- Nahlásit váš může kdokoliv i křivě
- Používají se jako součást antispamových systému s nižší váhou
- Ne všechny mailové servery správně uvedou důvod odmítnutí
- Různé způsoby odmazání
  - Na základě žádosti
  - Po určité době
  - Na základě potvrzení mail na postmastera

2. Greylisting

- Filtruje na základě IP, odesílatele a příjemce
- Funguje na straně serveru
- Dočasně odmítá emaily s informací o čase kdy se má klient pokusit poslat znovu
- Udržuje si DB požadavků
- Je možné jej kompletně smazat bez nutnosti kontaktovat třetí stranu
- Účinný proti robotům a pokud není použit zá-ložní MX

2.1 Zabezpečení

- Podepisovaní emailů GPG, S/MIME
  - Zprávu podepisuje autor
  - Je vázané na konkrétní adresu
  - Privátní / veřejný klíč
  - Možnost šifrovat pro více příjemců
- SPF
  - Definice seznamu povolených odesílacích serverů
  - Vázané na DNS – nutnost vytvořit TXT záznam
    - x.y. IN TXT "v=spf1 ip4:192.0.2.0/24 ip4:198.51.100.123 a -all"
- DKIM
  - Podepisovaní na serveru, příslušnost emailu k doméně
  - Vázané na DNS – nutnost vytvořit záznam
    - default._domainkey TXT IN ….

3. Dostupné implementace

- MS Windows
  - MS ExChange
  - KerioMailserver
  - HmailServer
- Linux
  - Sendmail
  - Qmail
  - Postfix
  - Exim, Nullmailer
- Cloud
  - Gmail
  - Office 365 + kombinace s on-premise