Bezpečnost síťových aplikací

2019/2020

Př 7

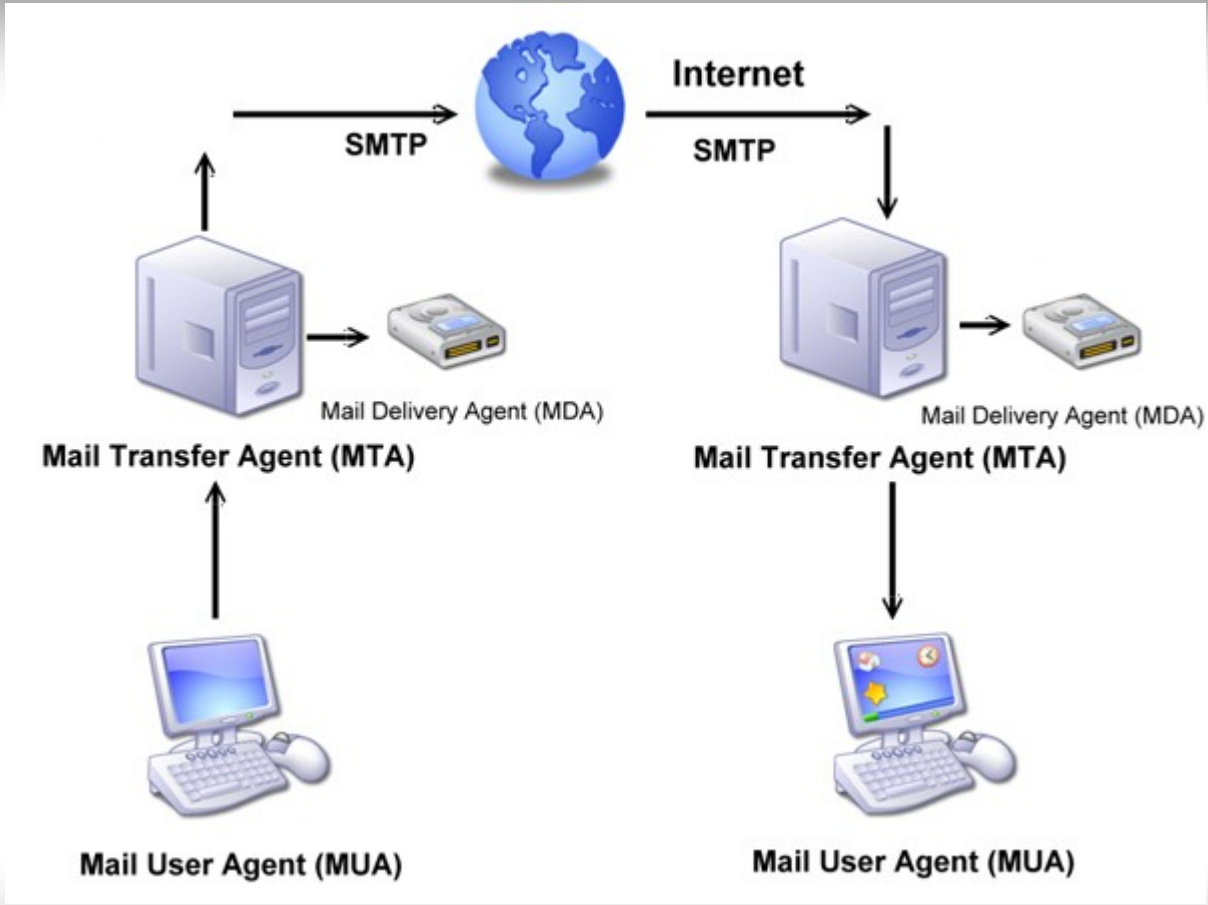
Mailové služby

- Přístupové údaje / Obsah mailů
  - Šifrovaná spojení SSL, virtuální uživatelé, GnuPG
- Zneužití SMTP serverů
  - OpenRelay,PopBeforeSMTP, SMTP-Auth, TLS
- Viry / Spamy
  - Clamav, spamassassin
- Podvržené email
  - SPF, Dkim, SRS, DMARC

Mail - opakování

- MUA -> MTA -> MDA
  - Outlook -> Postfix → maildir
- Decentralizované, vázané na DNS MX/A
- Nepotvrzovaná služba
- Stahování
  - POP3/POP3S/IMAP/IMAPS/HTTPS/MAPI
- Odesílání
  - SMTP

Směrování mailů



Přístupové údaje klienta

- Zneužití:
  - Zcizení obsahu
  - Šíření spamu/virů
  - Přístup na server
- Možnost uhádnutí hesla → min. složitost
- Možnost odposlechnutí hesla → SSL/TLS
- Odposlech/podrvžení obsahu → GnuPG
- Napadení serveru → virtuální uživatele

SMTP servery

- Zneužívání k šíření virů/spamů
- DOS/DDOS
- Změna směrování
  - Vytváření kopií, přeposílání, modifikace obsahu
  - Problém WWW konfigurátorů
  - Kompromitace DNS

SMTP - šíření virů/spamů

- Bez přihlášení – Open Relay
  - http://mxtoolbox.com/diagnostic.aspx
  - Vždy nutno zakázat
- S přihlášením
  - Odhadnutí/odposlech/vir na klientovy
  - Snadno identifikujeme viníka
- Servery se dostávají na blacklisty
  - Problém odstranění z blacklistu
  - BARRACUDA, CBL, SPAMCOP, ...

SMTP Auth

- Omezení přístupu jen na známé sítě
- PopBeforeSMTP
  - Ověření na základě stažení mailu
- SMTP-Auth
  - Plain, Login, GSSAPI, MD5...
  - Nutnost šifrování
  - Historicky port 587

SMTP - BlackListy

- Lokální
  - Řeší si administrátor sám
- Specializované
    - http://mxtoolbox.com/SuperTool.aspx
    - Nahlásit může kdokoliv
    - Problém deaktivace → opakovný poplatek
- Řešení v podobě rotace IP adres

SMTP - Greylist

- Dočasné odmítnutí
- Zaznamenám si čas, Ip a cíl a čekám
- Problemémy
  - Sekundární mailservery
  - MS Exchange
- Účinná ochrana před roboty

Viry a email

- Dnes nejčastější cesta šíření virů
- Vir má proti spamu výhodu
  - "jde bezpečně poznat"
  - X-Virus-Scanned: amavisd-new at icantinternet.org
- S mailem pracují téměř všechny dnešní antiviry

Spam

- Nevyžádaná pošta, až 80% provozu
- Není možné jednoznačně detekovat
- Bayer filtr, signatury, SPF, PTR, DKIM,...

  X-Spam-Flag: YES

  X-Spam-Score: 1000.907

  X-Spam-Status: Yes, score=1000.907 required=6.2 tests=[ALL_TRUSTED=-1,FH_FROMEML_NOTLD=0.18, GTUBE=1000, MISSING_HEADERS=1.207

  – Black/White listy, spam / ham složky
- Spamassassin

Podvržení email

- Snaha doručit nevyžádaný obsah
- Vydávam se za známého → otevřít mail
- Využívá předchozí mailové komunikace

SPF - Sender Policy Framework

- Podvržení uživatele - důvěryhodnost
- Benefit při identifikace spamu
- Umístění do TXT záznamu DNS

  v=spf1 a mx -all

  v=spf – verze

  a mx a:mail.zcu.cz

  -all = NE, +all = ANO, ~all = SOFT

  ?all = neutral

SRS - Sender Rewriting Scheme

- Umožňuje přeposílání emailu s SPF
- Běžně by docházelo k blokaci
- Instaluje se jako doplněk SMTP serveru
- V podstatě jen přepisuje údaje v hlavičkách

DKIM - DomainKeys Identified Mail

- Ověření původu e-mailu
- Podposy emailů a možnost ověření pravosti **ADSP**
- Konfigurace opět přes DNS
  - default._domainkey IN TXT "v=DKIM1; g=*; k=rsa; p=MIGfMA0GCSqG.....

ADSP - Author Domain Signing Practices

- Navazuje na DKIM
- Definuje vztah mezi odesilatelem a DKIM
- Hleda DKIM ze stejné domény jako From
- _adsp._domainkey TXT "dkim=discardable"
- Dkim= unknown | all | discardables

DMARC

- Domain-based Message Authentication, Reporting and Conformance
- Snaží se ověřit From: z SPF a DKIM
- Reportuje výsledky hodnocení
- Pokud SPF či DKIM sedí na From prohlásí email za platný
- Dva režimy strict pro SPF I DKIM a related pro SPF nebo DKIM

DMARC

- Nelze použít pro více příjemců
- v=DMARC1; p=reject; sp=none; pct=100; rua=mailto:dmarc@kiv.zcu.cz;
- Chyba se odesílá ihned
- Agregované hlašení pokud je povolené
-