DUM č. 15 v sadě

36. Inf-12 Počítačové sítě

Autor: Lukáš Rýdlo

Datum: 06.05.2014

Ročník: 3AV, 3AF

Anotace DUMu: e-mail, smtp, pop3, imap, hoax, phishing, spam

evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Počítačové sítě
Služba e-mail

E-mail

- jedna z historicky nejstarších služeb: 1965
  - původně komunikace uživatelů na sálových počítačích
- od 70. let použití znaku @ pro oddělení jména uživatele a stroje
- elektronická pošta – zasílání zpráv do schránky
- liší se od Instant Messagingu, kde se komunikuje v reálném čase
- e-mail je textový soubor, který putuje mezi různými servery
- technologie klient-server (s více servery)

Kdo komunikuje?

- MUA = Mail User Agent
  - klient (program na uživatelově PC/mobilu)
  - odesílá zprávu na odesílací server nebo mail přijímá/čte ze schránky na cílovém serveru
  - např. MS Outlook, Thunderbird apod., dnes většinou webový server s e-mailovým rozhraním
- MTA = Mail Transfer Agent
  - server (program na serveru)
  - přijímá novou zprávu od MUA, přeposílá cílovému stroji
- MDA = Mail Delivery Agent
  - server (program na serveru)
  - cílový stroj, který ukládá zprávy do schránky a umožňuje MUA zprávy číst

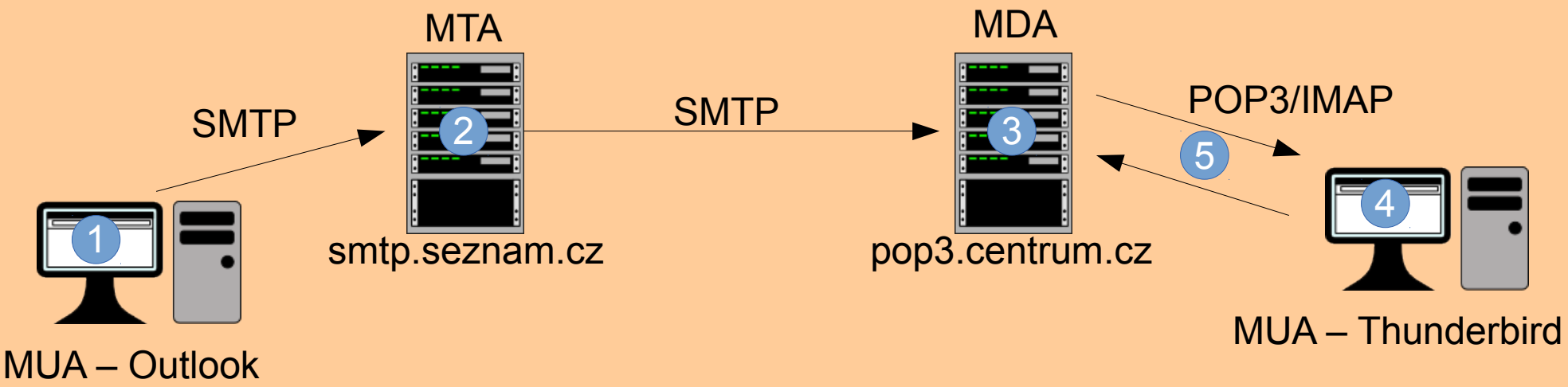
Jak komunikuje?

- SMTP = Simple mail transfer protocol
  - protokol umožňující posílání zprávy
  - slouží pro komunikaci odesílacího MUA s MTA a mezi MTA navzájem a mezi MTA a MDA
- POP3 = Post Office Protocol
  - protokol umožňuje stahovat zprávy z MDA do MUA
  - starý, umožňuje stahovat jen celé zprávy (nelze stáhnout jen „hlavičky“ – předmět, odesílatele, …)
  - standardně stáhne zprávy do PC (MUA) a na serveru je smaže
    - tzn. zpráva zůstává na jednom PC nikoli na MDA
  - dnes nevýhodný, zcela nevhodný pro mobily
  - existuje POP3S šifrovaná verze, jinak je komunikace nešifrovaná

Jak komunikuje? (pokračování)

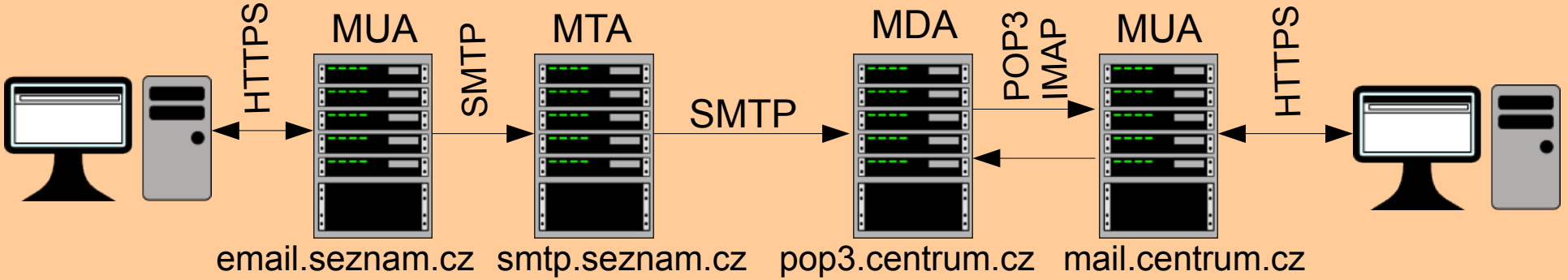
- IMAP = Internet Message Access Protocol
  - umožňuje číst MUA zprávy z MDA
  - novější a lepší varianta POP3
  - oproti POP3 umožňuje stáhnout nejprve hlavičky a teprve později text zprávy a přílohy
    - výhoda: pokud poznám spam podle předmětu/odesílatele, nemusím jej stahovat, ale rovnou jej smažu
  - umožňuje číst zprávy ze serveru více různým zařízením online
    - zprávy se ponechají na serveru, na zařízení se stahuje kopie, jeli-to potřeba
    - zprávy zůstávají standardně na MDA
  - existuje IMAPS šifrovaná verze, jinak je komunikace nešifrovaná

Schéma komunikace



1) Odesílatel napíše v MUA (třeba Outlook) e-mail a zvolí odeslat.
2) MUA se zkontaktuje s MTA pomocí protokolu SMTP a zprávu převezme (je odeslaná).
3) MTA se dále kontaktuje s dalšími MTA a nakonec s MDA, vše pomocí SMTP.
4) Adresát se rozhodne zkontrolovat poštu, spustí MUA.
5) MUA adresáta ověří obsah schránky na MDA přes POP3 nebo IMAP a požadované zprávy stáhne (zobrazí).

Schéma komunikace přes web



- V roli MUA vystupuje webový server.
- Odesílatel se přes HTTPS připojí na webovou stránku a napíše zprávu, kterou skript ve webové stránce přesá přes SMTP příslušnému MTA k odeslání.
- MTA a MDA mezi sebou komunikují jako obvykle.
- Příjemce se přes HTTPS přihlásí do webového rozhraní, webový server pomocí POP3 nebo IMAP stáhne zprávy, vytvoří příslušnou webovou stránku a zobrazí uživateli.

Jak e-mail vypadá ve skutečnosti?

- Je to obyčejný textový soubor, kódovaný v ASCII s přílohami zakódovanými pomocí Base64 kódování.
- Některé servery kódují i v UTF-8.
- Odesílatel, příjemce, předmět, datum a další data jsou v tzv. hlavičce, pak následuje „tělo“ zprávy a přílohy.
- Textovou podobu lze získat např. na Gmailu volbou „zobrazit originál“.

Příklad e-mailu

Delivered-To: user@server.cz
Received: by 10.194.79.133 with SMTP id j5csp119021wjx;
Mon, 5 May 2013 04:34:29 -0700 (PDT)
X-Received: by 10.14.32.136 with SMTP id o8mr4279107eea.35.1399289668836;
Mon, 05 May 2013 04:34:28 -0700 (PDT)
Return-Path: <me@mail.cz>
To: <user@server.cz>
Subject: =?utf-8?q?Testovac=C3=AD_zpr=C3=A1va?=
Received: from 195.113.164.178 (X-Forwarded-For: 195.113.164.178)
by mail1007.mail.cz (mail.cz multimail) with HTTP
Date: Mon, 05 May 2013 13:34:28 +0200
From: <me@mail.cz>
Cc: =?utf-8?q?l=2Eme?= <me@mail.cz>
X-Mailer: My Email 5.3
X-Priority: 3
X-Original-From: me@mail.cz
MIME-Version: 1.0
Message-Id: <20140505133428.77B3E21E@mail.cz>
X-Maser: Georgo
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 8bit

Ahoj,
Ĺ˘Ă-lenÄ› Ĺľluĺ„ouÄŤkĂ˝ kĹŻĹ‍ ĂşpÄ›l ÄŹĂ˘belskÄ© Ăłdy...

Na co si dát pozor…

- Nepište VELKÝMI PÍSMENY (křik).
- Používejte rozumný předmět (Místo „Pomoc!!!“ raději „Potřebuji poradit s úkolem do matiky.“).
- Používejte pole „kopie“ (Cc) a „skrytá kopie“ (Bcc).
  - Hromadná přání odesílejte bez vyplněného odesílatele, všechny adresy patří do Bcc.
- Nerozesílejte a nečtěte smap, hoax a phishing.
- „Zaručené zprávy“ si vždy ověřujte.

SPAM

- Nevyžádaná (reklamní) pošta.
- Obtěžuje, zdržuje od práce, zbytečně plní schránku.
- Obrana?
  - nenechávat nikde volně napsanou svou adresu (různé weby)
  - mít zvlášť osobní schránku a schránku pro různé registrace na webech, e-shopech apod.
  - používat filtry
    - lze filtrovat podle předmětu, odesílatele apod.
    - Úkol: vytvořte ve své schránce filtr na mazání zpráv odeslaných ze serveru reklama.cz
  - nahlásit spam na ÚOOÚ: http://www.uoou.cz/stiznost.asp#obalhlava

HOAX

- poplašná, obvykle nepravdivá, řetězově se šířící zpráva
- Příklady:

Dobrý den
Hledají se vážní zájemci o štěňata Golden Retriver.
Narodilo se jich tolik, že nejspíš budou uspány.
V případě zájmu budou štěňata předána zdarma.
Pokud máte zájem,volejte 515123456.
V případě,že se nedovoláte, volejte 736 123 456.

Vznik: listopad 2003

Vznik: září 2010

SKANDÁL:mlékárenské společnosti mohou ze zákona prošlé mléko až pětkrát přepasterizovat a uvést znovu do prodeje,

Je nutno velmi dobře prohlédnout tetrapack, jestliže najdete 12 45 - tj. chybí 3 - pak se jedná o mléko, jež třikrát prošlo a bylo třikrát přepasterizované. A ovšem v krabici je každé balení jiné.

De facto pijeme špinavou vodu!

HOAX – prokračování

- Jak ho poznáme?
  - Obsahuje kontroverzní informace s odkazem na neexistující osobnost nebo instituci.
  - Žádá další šíření, apeluje na city (nikoli rozum).
  - Ověříme si informaci, nejlépe na www.hoax.cz.
- Čím škodí?
  - panika, hloupé chování, davová manipulace
  - obtěžování lidí na přiloženém telefonu/e-mailu
- Proč to lidé vymýšlejí a šíří?
  - Př.: Otec rozeslal žádost o krevní transfuzi pro svého syna. Nemocnice sama ji během pár hodin obstarala. E-mail ale koluje několik let po propuštění pacienta a nemocnice si kvůli množství telefonátů musela změnit telefonní číslo…

Phishing

- „rybaření“ – snaha „ulovit“ naivního uživatele
- e-mail požaduje zaslání hesla, kopie kreditní karty, občanského průkazu a podobně
- snaha vylákat osobní údaje ke spamování nebo krádeži
- Jak se pozná?
  - často špatná čeština
  - hrozí zrušením účtu, ztrátou peněz apod.
  - požaduje zaslání nebo vyplnění údajů na podvodné stránce
  - podvodná stránka může vypadat velice podobně jako originální

Phishing – příklad

Vážený kliente / klientko,

Jelikož využíváte služeb naší banky, tzn. osobní účet v České spořitelně, ke kterému máte vedenou platební kartu VISA a v poslední době jsme zaznamenali na Vašem běžném účtě podezřelé platební transakce, je potřeba aktualizovat data Vaši kreditní karty, v opačném případě bude Vaše kreditní karta zablokovaná a Váš účet pozastaven na dobu neurčitou. Chceme pouze ověřit, že transakce na Vašem účtě opravdu provádíte Vy jako disponent/ka účtu a ne někdo jiný.

Pošlete nám prosím níže vyplněné parametry:

Jméno a přijmení:_____

Rodné číslo:_____/_____

Místo trvalého bydliště:_____

Telefonní číslo: +420_____

Číslo platební karty: _____

Platnost karty od a do: _____/_____

CVC kód (poslední tři čísla na zadní straně)__

Zdroje

- http://en.kioskea.net/contents/116-how-email-works-mta-mda-m
- http://www.hoax.cz